HAESE MATHEMATICS

Specialists in mathematics publishing

Mathematics

for the international student

Mathematics HL (Option): Discrete Mathematics

HL Topic 10

FM Topic 6

Catherine Quinn
Peter Blythe
Chris Sangwin
Robert Haese
Michael Haese

for use with
IB Diploma
Programme

MATHEMATICS FOR THE INTERNATIONAL STUDENT
Mathematics HL (Option): Discrete Mathematics

Catherine Quinn	B.Sc.(Hons), Grad.Dip.Ed., Ph.D.
Peter Blythe	B.Sc.
Chris Sangwin	M.A., M.Sc., Ph.D.
Robert Haese	B.Sc.
Michael Haese	B.Sc.(Hons.), Ph.D.

Haese Mathematics
152 Richmond Road, Marleston, SA 5033, AUSTRALIA
Telephone: +61 8 8210 4666, Fax: +61 8 8354 1238
Email: info@haesemathematics.com.au
Web: www.haesemathematics.com.au

National Library of Australia Card Number & ISBN 978-1-921972-34-8

Published by Haese Mathematics.
152 Richmond Road, Marleston, SA 5033, AUSTRALIA

First Edition 2014

Artwork by Brian Houston.

Cover design by Piotr Poturaj.

Typeset in Australia by Deanne Gallasch. Typeset in Times Roman 10.

Computer software by Tim Lee.

Production work by Anna Rijken and Mark Humphries.

Printed in China by Prolong Press Limited.

The textbook and its accompanying CD have been developed independently of the International Baccalaureate Organization (IBO). The textbook and CD are in no way connected with, or endorsed by, the IBO.

Acknowledgements: While every attempt has been made to trace and acknowledge copyright, the authors and publishers apologise for any accidental infringement where copyright has proved untraceable. They would be pleased to come to a suitable agreement with the rightful owner.

Disclaimer: All the internet addresses (URLs) given in this book were valid at the time of printing. While the authors and publisher regret any inconvenience that changes of address may cause readers, no responsibility for any such changes can be accepted by either the authors or the publisher.

FOREWORD

Mathematics HL (Option): Discrete Mathematics has been written as a companion book to the Mathematics HL (Core) textbook. Together, they aim to provide students and teachers with appropriate coverage of the two-year Mathematics HL Course, to be first examined in 2014.

This book covers all sub-topics set out in Mathematics HL Option Topic 10 and Further Mathematics HL Topic 6, Discrete Mathematics.

The aim of this topic is to introduce students to the basic concepts, techniques and main results in number theory and graph theory.

Detailed explanations and key facts are highlighted throughout the text. Each sub-topic contains numerous Worked Examples, highlighting each step necessary to reach the answer for that example.

Theory of Knowledge is a core requirement in the International Baccalaureate Diploma Programme, whereby students are encouraged to think critically and challenge the assumptions of knowledge. Discussion topics for Theory of Knowledge have been included on pages 140 and 160. These aim to help students discover and express their views on knowledge issues.

The accompanying student CD includes a PDF of the full text and access to specially designed software and printable pages.

Graphics calculator instructions for Casio fx-9860G Plus, Casio fx-CG20, TI-84 Plus and TI-*n*spire are available from icons in the book.

Fully worked solutions are provided at the back of the text, however students are encouraged to attempt each question before referring to the solution.

It is not our intention to define the course. Teachers are encouraged to use other resources. We have developed this book independently of the International Baccalaureate Organization (IBO) in consultation with experienced teachers of IB Mathematics. The text is not endorsed by the IBO.

In this changing world of mathematics education, we believe that the contextual approach shown in this book, with associated use of technology, will enhance the students understanding, knowledge and appreciation of mathematics and its universal applications.

We welcome your feedback.

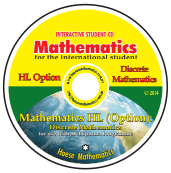
Email: *info@haesemathematics.com.au*
Web: *www.haesemathematics.com.au*

CTQ PJB CS
RCH PMH

ACKNOWLEDGEMENTS

The authors and publishers would like to thank all those teachers who offered advice and encouragement on this book.

USING THE INTERACTIVE STUDENT CD



The interactive CD is ideal for independent study.

Students can revisit concepts taught in class and undertake their own revision and practice. The CD also has the text of the book, allowing students to leave the textbook at school and keep the CD at home.

By clicking on the relevant icon, a range of interactive features can be accessed:

- Graphics calculator instructions for the **Casio fx-9860G Plus**, **Casio fx-CG20**, **TI-84 Plus** and the **TI-$n$spire**
- Interactive links to software
- Printable pages

INTERACTIVE LINK

GRAPHICS CALCULATOR INSTRUCTIONS

TABLE OF CONTENTS

SYMBOLS AND NOTATION USED IN THIS BOOK

$\approx$	is approximately equal to
$>$	is greater than
$\geqslant$	is greater than or equal to
$<$	is less than
$\leqslant$	is less than or equal to
$\{......\}$	the set of all elements ......
$\{x_1,\ x_2,\ ....\}$	the set with elements $x_1,\ x_2,\ ....$
$\in$	is an element of
$\notin$	is not an element of
$\mathbb{N}$	the set of all natural numbers $\{0,\ 1,\ 2,\ 3,\ ....\}$
$\mathbb{Z}$	the set of integers $\{0,\ \pm1,\ \pm2,\ \pm3,\ ....\}$
$\mathbb{Z}^+$	the set of positive integers $\{1,\ 2,\ 3,\ ....\}$
$\mathbb{R}$	the set of real numbers
$\cup$	union
$\cap$	intersection
$\mathbb{Z}_m$	the set of equivalence classes $\{0,\ 1,\ 2,\ ....,\ m-1\}$ of integers modulo m
$\Rightarrow$	implies that
$\not\Rightarrow$	does not imply that
$\Leftrightarrow$	if and only if
$f(x)$	the image of x under the function f
$\sum\limits_{i=1}^{n} u_i$	$u_1 + u_2 + u_3 + ... + u_n$
$a \mid b$	a divides b
$\gcd(a,\ b)$	the greatest common divisor of a and b
$\operatorname{lcm}(a,\ b)$	the least common multiple of a and b
$a \equiv b (\operatorname{mod} m)$	a is congruent to b modulo m
sin, cos, tan	the circular functions
arcsin, arccos, arctan	the inverse circular functions
cis θ	$\cos\theta + i\sin\theta$
$n!$	$n \times (n-1) \times (n-2) \times .... \times 3 \times 2 \times 1$
$\binom{n}{r}$	$\dfrac{n!}{r!(n-r)!}$

$(a_k....a_2a_1a_0)$	digital form of the integer $a_k10^k + ... + a_210^2 + a_110 + a_0$
$(a_k....a_2a_1a_0)_n$	digital form of the integer $a_kn^k + ... + a_2n^2 + a_1n + a_0$
P_n	a proposition defined for some n
f_n	the nth term of the Fibonacci sequence
deg(A)	the degree of vertex A
G'	the complement of graph G
K_n	the complete graph on n vertices
$K_{m,\, n}$	the complete bipartite graph with m vertices in one set and n in the other
C_n	the cycle graph on n vertices
W_n	the wheel graph on n vertices
deg(F)	the degree of face F
wt(T)	the weight of tree T
wt(VW)	the weight of edge VW

Number theory 1

Contents:

INTRODUCTION TO NUMBER THEORY

You might think that integers are the simplest of mathematical objects. However, their properties lead to some very deep and satisfying mathematics. The study of the properties of integers is called **number theory**.

In this course we will study:

- *techniques of proof*
- *applications of algorithms*, which are methods of mathematical reasoning and solution
- a development of the number system with *modular arithmetic*
- the use and proof of important theorems.

SETS OF INTEGERS

The set of all **integers** is $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \pm4, \pm5, ...\}$.

The set of all **positive integers** is $\mathbb{Z}^+ = \{1, 2, 3, 4, 5, ...\}$.

The set of **natural numbers** is $\mathbb{N} = \{0, 1, 2, 3, ...\} = \mathbb{Z}^+ \cup \{0\}$.

NOTATION

$\in$ reads *is in* or *is an element of* or *is a member of*

$\Rightarrow$ reads *implies*

$\Leftrightarrow$ reads *if and only if*

$a \mid b$ reads *a divides b* or *a is a factor of b* $\{a \mid b \Rightarrow b = na$ for some $n \in \mathbb{Z}\}$.

$\gcd(a, b)$ reads *the greatest common divisor of a and b*, which is the highest common factor of a and b

$\text{lcm}(a, b)$ reads *the least common multiple of a and b*.

$(a_k....a_2a_1a_0)$ is the digital form of the integer $a_k10^k + ... + a_210^2 + a_110 + a_0$

$(a_k....a_2a_1a_0)_n$ is the digital form of the integer $a_kn^k + ... + a_2n^2 + a_1n + a_0$

If the digits are all known then we leave off the brackets.

For example, $101\,101_2 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$.

PRIME AND COMPOSITE INTEGERS

A positive integer p is **prime** if $p > 1$ and the only factors of p are 1 and p itself.

If a positive integer m, $m > 1$, is not prime, it is called **composite**.

The integer 1 is neither prime nor composite.

For example:

- 2, 3, 5, 7, 11 are prime numbers.
- 1, 4, 6, 9 are not prime numbers. In particular, $4 = 2 \times 2$, $6 = 2 \times 3$, and $9 = 3 \times 3$ are examples of composite numbers.

OPENING PROBLEMS

In this course we will address problems like the ones in the following exercise. Do not be discouraged if you cannot solve some of these problems yet.

1 Consider the integers of the form $2^n - 1$, $n \in \mathbb{Z}^+$, $n \geqslant 2$. Are all integers of this form prime numbers?

2 Consider the integers of the form $2^p - 1$, where p is prime. Are all integers of this form prime numbers?

3 Find a list of:

a five consecutive non-prime integers **b** six consecutive non-prime integers.

4 Prove that it is not possible to find integers x and y such that $6x + 3y = 83$.

5 Prove that a perfect square always:

a has an odd number of factors

b is the product of an even number of primes (counting repetitions).

6 Without using division, determine whether $14\,975\,028\,526\,824$ is divisible by 36.

7 Show that the equation $2x + 4y = 62$ has an infinite number of solutions such that x and y are integers.

8 Are there infinitely many prime numbers? Can you prove your assertion?

9 A **rational number** is a number which can be written in the form $\frac{p}{q}$ where p and q are integers and $q \neq 0$. Prove that $\sqrt{2}$ is not rational.

Hint: Start by assuming that $\sqrt{2}$ is rational. You may find **5b** above useful.

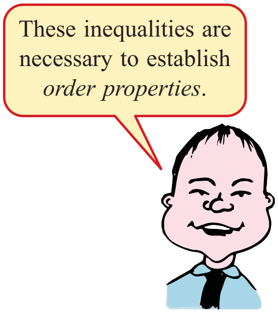
10 Is 5041 a prime number?

AXIOMS

An **axiom** is a foundation statement which is stipulated to be true for the purpose of developing further theory.

For example, we define the inequalities:

$$a > b \Leftrightarrow a - b > 0$$
$$a < b \Leftrightarrow b - a > 0$$


These inequalities are necessary to establish *order properties*.

The **order axiom** is:

If $a > 0$ and $b > 0$ then $a + b > 0$ and $ab > 0$.

Using the order axiom, the following results can be proven:

- If $a < b$ and $b < c$, then $a < c$. (transitivity)
- If $a < b$ then $a + c < b + c$ and $a - c < b - c$.
- If $a < b$ and $c > 0$, then $ac < bc$.
- If $a < b$ and $c < 0$, then $ac > bc$.

Proof:

$$\begin{aligned} & a < b \Rightarrow b - a > 0 \\ \text{and } & c < 0 \Rightarrow -c > 0 \\ \therefore\ & -c(b-a) > 0 \qquad \{\text{order axiom}\} \\ \therefore\ & -bc + ac > 0 \\ \therefore\ & ac > bc \end{aligned}$$

AXIOMS FOR INTEGERS

- If $a, b \in \mathbb{Z}$ then $a+b$, $a-b$, and $ab \in \mathbb{Z}$.
- If $a \in \mathbb{Z}$ then there does not exist $x \in \mathbb{Z}$ such that $a < x < a+1$.
- If $a, b \in \mathbb{Z}$ and $ab = 1$, then either $a = b = 1$ or $a = b = -1$.
- If $a, b \in \mathbb{Z}$ then either $a < b$, $a = b$, or $a > b$.

WELL ORDERED PRINCIPLE (WOP)

A set S is **well ordered** $\Leftrightarrow$ every non-empty subset of S contains a *least* element.

$\mathbb{Z}^+ = \{1, 2, 3, ...\}$ is well ordered since any subset of $\mathbb{Z}^+$ will contain a distinct element of lowest value.

$\mathbb{Z} = \{...., -2, -1, 0, 1, 2, 3, ...\}$ is not well ordered, since for example the set $\mathbb{Z}$ itself does not have a least element.

$\mathbb{R}$ is not well ordered, since any open subset of $\mathbb{R}$ does not contain a least element.

$\mathbb{N} = \{0, 1, 2, ...\}$ is well ordered.

A MATHEMATICAL INDUCTION

The Well Ordered Principle (WOP) for $\mathbb{Z}^+$ is that every non-empty subset of $\mathbb{Z}^+$ contains a least (lowest value) element.

This property of the set of positive integers is necessary for the validity of **proof by induction**.

From the HL Core course, the **Principle of Mathematical Induction (PMI)** in its weak form is:

> Suppose P_n is a proposition defined for all n in $\mathbb{Z}^+$. If
>
> - P_1 is true and
> - the truth of $P_k \Rightarrow$ the truth of P_{k+1} (called the **inductive step**)
>
> then P_n is true for all $n \in \mathbb{Z}^+$.

Theorem 1:

> The proof by the Principle of Mathematical Induction is a valid method of mathematical proof.

Proof (by contradiction):

Suppose that P_1 is true and the truth of $P_k \Rightarrow$ the truth of P_{k+1}, but the conclusion P_n is not true for every $n \in \mathbb{Z}^+$

$\Rightarrow$ there exists at least one positive integer for which P_n is false

$\Rightarrow$ the set S of positive integers for which P_n is false, is non-empty

$\Rightarrow$ S has a least element, k say, where P_k is false. {WOP} .... $(*)$

But P_1 is true, so $k > 1$

$\Rightarrow k - 1 > 0$

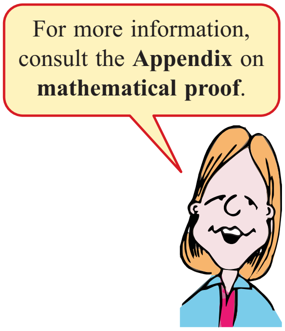
$\Rightarrow 0 < k - 1 < k$ {axioms}

Now since $k - 1 < k$, $k - 1$ is not in S {as k is the least element of S}.

This implies that P_{k-1} is true {from $*$}.

But P_{k-1} true $\Rightarrow P_k$ true, hence P_k is true which contradicts $*$.

So, our supposition is false.


For more information, consult the **Appendix** on **mathematical proof**.

Mathematical induction is used in many number theoretic proofs, especially for establishing divisibility, and in later work on recurrence relations.

Example 1

Use the Principle of Mathematical Induction to prove that $10^{n+1} + 3 \times 10^n + 5$ is divisible by 9 for all $n \in \mathbb{Z}^+$.

Proof: (By the Principle of Mathematical Induction)

P_n is that "$10^{n+1} + 3 \times 10^n + 5$ is divisible by 9" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $10^2 + 3 \times 10^1 + 5 = 135 = 15 \times 9$ which is divisible by 9

$\therefore$ P_1 is true.

(2) If P_k is true, then $10^{k+1} + 3 \times 10^k + 5 = 9A$ for some $A \in \mathbb{Z}$ .... $(*)$

$$\begin{aligned}\therefore\quad & 10^{[k+1]+1} + 3 \times 10^{[k+1]} + 5\\ &= 10 \times 10^{k+1} + 30 \times 10^k + 5\\ &= 10(9A - 3 \times 10^k - 5) + 30 \times 10^k + 5 \qquad \{\text{using } *\}\\ &= 90A - 30 \times 10^k - 50 + 30 \times 10^k + 5\\ &= 90A - 45\\ &= 9(10A - 5) \quad \text{where } 10A - 5 \in \mathbb{Z} \text{ since } A \in \mathbb{Z}\end{aligned}$$

$\therefore$ $10^{[k+1]+1} + 3 \times 10^{[k+1]} + 5$ is divisible by 9

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

Example 2

Use the Principle of Mathematical Induction to prove that $5^n \geqslant 8n^2 - 4n + 1$ for all $n \in \mathbb{Z}^+$.

Proof: (By the Principle of Mathematical Induction)

P_n is that "$5^n \geqslant 8n^2 - 4n + 1$" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, LHS $= 5^1 = 5$ and RHS $= 8 \times 1 - 4 \times 1 + 1 = 5$

$\therefore$ P_1 is true.

(2) If P_k is true, then $5^k \geqslant 8k^2 - 4k + 1$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & 5^{[k+1]} - 8[k+1]^2 + 4[k+1] - 1\\ &= 5 \times 5^k - 8(k^2 + 2k + 1) + 4k + 4 - 1\\ &= 5 \times 5^k - 8k^2 - 16k - 8 + 4k + 4 - 1\\ &= 5 \times 5^k - 8k^2 - 12k - 5\\ &\geqslant 5(8k^2 - 4k + 1) - 8k^2 - 12k - 5 \qquad \{\text{using } *\}\\ &\geqslant 32k^2 - 32k\\ &\geqslant 32k(k-1)\\ &\geqslant 0 \quad \text{since } k \geqslant 1\end{aligned}$$

$\therefore$ $5^{[k+1]} \geqslant 8[k+1]^2 - 4[k+1] + 1$

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

EXERCISE 1A.1

1 Use the Principle of Mathematical Induction to prove that:

a $3^n > 7n$ for $n \geqslant 3,\ n \in \mathbb{Z}^+$

b $n^n > n!$ for $n \geqslant 2,\ n \in \mathbb{Z}^+$

c $3^n < n!$ for $n \geqslant 7,\ n \in \mathbb{Z}^+$.

2 Use the Principle of Mathematical Induction to prove that:

a $n^3 - 4n$ is divisible by 3 for all $n \geqslant 3,\ n \in \mathbb{Z}^+$

b $5^{n+1} + 2(3^n) + 1$ is divisible by 8 for all $n \in \mathbb{Z}^+$

c $73 \mid (8^{n+2} + 9^{2n+1})$ for all $n \in \mathbb{Z}^+$.

3 The nth repunit is the integer consisting of n "1"s.
For example, the third repunit is the number 111.

a Prove that the nth repunit is $\dfrac{10^n - 1}{9}$ for all $n \in \mathbb{Z}^+$.

b Ali claimed that all repunits other than the second, are composite. Can you prove or disprove Ali's claim?

c Tara made a weaker statement. She claimed that if a repunit is prime, then it must have a prime number of digits. Can you prove or disprove Tara's claim?

d Joachim made a stronger claim than Tara. He said that all repunits with a prime number of digits must themselves be prime. Can you prove or disprove Joachim's claim?

4 Use the Principle of Mathematical Induction to prove that $3^n \geqslant 5n^2 - 6n$ for all $n \geqslant 3,\ n \in \mathbb{Z}^+$.

STRONG INDUCTION (THE SECOND FORM OF MATHEMATICAL INDUCTION)

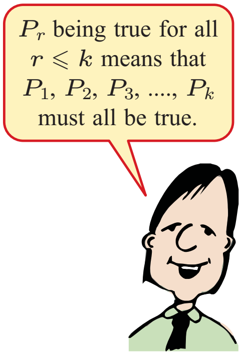
Strong induction is so-called because its inductive step appears to require more conditions than in the first (weak) form. It states that:

> If P_1 is true, and if P_r being true for all $r \leqslant k \Rightarrow P_{k+1}$ is true, then P_n is true for all $n \in \mathbb{Z}^+$.

This form of inductive proof is in fact logically equivalent to the weak form!

The proof of the **Unique Prime Factorisation Theorem** depends on it.

P_r being true for all $r \leqslant k$ means that P_1, P_2, P_3, ..., P_k must all be true.



THE FIBONACCI SEQUENCE

An area of Mathematics where proof by Strong Induction is used is that of **recurrence relations**.

An example is the **Fibonacci sequence** of numbers: 1, 1, 2, 3, 5, 8, 13, 21, 34, ...

Leonardo of Pisa (Fibonacci) (c. 1180 - 1228) introduced the sequence to Europe along with the Arabic notation for numerals, in his book "*Liber Abaci*". It is posed as the rabbits problem which you could source on the internet or in the library.

Many results about the Fibonacci sequence have been proven, but others are still to be proved. The magazine “The Fibonacci Quarterly” deals solely with newly discovered properties of the sequence. A number of proofs require **strong induction** for proof. Many sites could be visited including:

http://mathworld.wolfram.com/FibonacciNumber.html

The Fibonacci sequence can be defined as:

$$f_1 = 1, \quad f_2 = 1, \quad \text{and} \quad f_{n+2} = f_{n+1} + f_n \quad \text{for all} \quad n \geqslant 1.$$

This is an example of a recurrence relation as we specify the initial value(s) and then give a rule for generating all subsequent terms.

Example 3

A sequence is defined recursively by $a_{n+1} = \dfrac{a_n{}^2}{a_{n-1}}$ for all integers $n \geqslant 2$ with $a_1 = 1$ and $a_2 = 2$.

a Find a_3, a_4, a_5, and a_6.

b Hence, postulate a closed form solution for a_n.

c Prove your postulate is true using Mathematical Induction.

A **closed form** solution is a solution given as an explicit function of n.

a

$$a_3 = \frac{a_2{}^2}{a_1} = \frac{2^2}{1} = 4$$

$$a_4 = \frac{a_3{}^2}{a_2} = \frac{4^2}{2} = 8$$

$$a_5 = \frac{a_4{}^2}{a_3} = \frac{8^2}{4} = 16$$

$$a_6 = \frac{a_5{}^2}{a_4} = \frac{16^2}{8} = 32$$

b

$a_1 = 1 = 2^0$

$a_2 = 2 = 2^1$

$a_3 = 4 = 2^2$

$a_4 = 8 = 2^3$

$a_5 = 16 = 2^4$

$a_6 = 32 = 2^5$

We postulate that $a_n = 2^{n-1}$.

c **Proof:** (By the Principle of Mathematical Induction (strong form).)

P_n is that “if $a_1 = 1$, $a_2 = 2$, and $a_{n+1} = \dfrac{a_n{}^2}{a_{n-1}}$ for all integers $n \geqslant 2$, then $a_n = 2^{n-1}$”.

(1) If $n = 1$, $2^{1-1} = 2^0 = 1 = a_1$ $\quad\therefore\quad P_1$ is true.

(2) Assume that $a_r = 2^{r-1}$ is true for all $r \leqslant k$

$\therefore \quad a_r = 2^{r-1}$ for $r = 1, 2, 3, 4, ..., k$ .... $(*)$

$$\text{Now} \quad a_{k+1} = \frac{a_k{}^2}{a_{k-1}} = \frac{(2^{k-1})^2}{2^{k-2}} \qquad \{\text{using } *\}$$

$$= \frac{2^{2k-2}}{2^{k-2}}$$

$$= 2^k$$

$$= 2^{(k+1)-1} \quad \text{which has the required form.}$$

Thus P_1 is true, and the assumed result for $r = 1, 2, 3, 4, ..., k \Rightarrow$ the same result for $r = k + 1$.

$\therefore \quad P_n$ is true for all $n \in \mathbb{Z}^+$.

EXERCISE 1A.2

1 If a sequence is defined by $a_1 = 1$, $a_2 = 2$, and $a_{n+2} = a_{n+1} + a_n$, prove that $a_n \leqslant \left(\frac{5}{3}\right)^n$ for all $n \in \mathbb{Z}^+$.

2 If $b_1 = b_2 = 1$ and $b_n = 2b_{n-1} + b_{n-2}$ for all $n \geqslant 3$, prove that b_n is odd for $n \in \mathbb{Z}^+$.

The remaining questions all involve the Fibonacci sequence, f_n.

3 Evaluate $\sum\limits_{k=1}^{n} f_k$ for $n = 1, 2, 3, 4, 5, 6$, and 7. Hence express $\sum\limits_{k=1}^{n} f_k$ in terms of another Fibonacci number. Prove your postulate true by induction.

4 We can use inequalities to *bound* the Fibonacci numbers and tell us something about how they grow 'exponentially'.

a Prove that $\left(\frac{3}{2}\right)^{n-2} < f_n \leqslant 2^{n-2}$ for all $n \in \mathbb{Z}^+$, $n \geqslant 3$.

b Prove that $\left(\dfrac{1+\sqrt{5}}{2}\right)^{n-2} < f_n$ for all $n \in \mathbb{Z}^+$. This leads to a closed form for f_n known as **Binet's formula**.

5 Rearranging $f_{n+2} = f_{n+1} + f_n$ to $f_n = f_{n+2} - f_{n+1}$ enables us to prove question **3** directly. Show how this can be done.

6 Postulate and prove a result for $\sum\limits_{k=1}^{n} f_{2k-1}$ in terms of other Fibonacci numbers.

7 Postulate and prove a result for $\sum\limits_{k=1}^{n} {f_k}^2$ in terms of other Fibonacci numbers by expressing the result of this sum as a product of two factors, each of which can be expressed in terms of a Fibonacci number.

8 Prove that $f_{n+1} \times f_{n-1} - (f_n)^2 = (-1)^n$ for all $n \in \mathbb{Z}^+$, $n \geqslant 2$.

9 Postulate and prove a result for $\sum\limits_{k=1}^{n} f_{2k}$ in terms of other Fibonacci numbers.

10 Postulate and prove a result for $\sum\limits_{k=1}^{2n-1} (f_k \times f_{k+1})$ in terms of the square of another Fibonacci number.

11 Prove that $f_n \times f_{n-1} = (f_n)^2 - (f_{n-1})^2 + (-1)^n$ for all $n \geqslant 2$.
Hence show that consecutive Fibonacci numbers have no common factor besides 1.

12 **a** Prove by induction that $a_n = \dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \dfrac{1}{\sqrt{5}}\left(\dfrac{1-\sqrt{5}}{2}\right)^n$, $n \in \mathbb{Z}^+$, is a closed form solution to the Fibonacci recurrence relation.

b Which form of induction was required in **a**?

13 Prove that f_{4n} is a multiple of 3 for all $n \in \mathbb{Z}^+$.

14 An alternative definition of the Fibonacci sequence includes an initial term $f_0 = 0$. In this case we have $f_0 = 0$, $f_1 = 1$, $f_{n+1} = f_n + f_{n-1}$ for all $n \geqslant 1$.

a Find f_0, f_5, and f_{10}.

b Prove that every Fibonacci number f_{5t} is a multiple of 5.

B RECURRENCE RELATIONS

We have seen that the Fibonacci sequence is an example of a recurrence relation, where we specify an initial term, and generate subsequent terms using a rule which involves the previous terms.

In this section we examine methods to solve problems involving a *recursive* or *iterative* calculation. These occur in certain counting problems, and in problems involving population growth, compound interest, and debt repayment.

In the HL Core course we defined:

A **sequence** $\{a_n\}$ is a list of numbers a_n, $n = 0, 1, 2, ...$ called **terms**, in a definite order.

Depending on the theory being studied, the first term of a sequence may be denoted a_0 or a_1, which means the terms of the sequence are indexed either by $\mathbb{N}$ or $\mathbb{Z}^+$. This is a matter of convenience, and we choose $\mathbb{N}$ or $\mathbb{Z}^+$ depending on the context of the problem.

In this section we mostly use $\mathbb{N}$, and indeed we assume $n \in \mathbb{N}$ unless otherwise specified.

For example:

- Consider the sequence $0!, 1!, 2!, 3!, ...$ defined by the closed form solution $a_n = n!$, $n \in \mathbb{N}$.

  Notice that
  $$\begin{aligned} a_0 &= 0! = 1 \\ a_1 &= 1! = 1 = 1 \times a_0 \\ a_2 &= 2! = 2 = 2 \times a_1 \\ a_3 &= 3! = 6 = 3 \times a_2 \\ a_4 &= 4! = 24 = 4 \times a_3 \\ &\vdots \\ a_n &= na_{n-1} \quad \text{for all } n \in \mathbb{N},\ n \geqslant 1. \end{aligned}$$

  This is a **recursive definition** which gives us:
  $$\begin{aligned} a_{n-1} &= (n-1)a_{n-2}, \quad \text{for } n \geqslant 2 \\ a_{n-2} &= (n-2)a_{n-3}, \quad \text{for } n \geqslant 3 \\ a_{n-3} &= (n-3)a_{n-4}, \quad \text{for } n \geqslant 4 \\ &\vdots \\ a_{n-k} &= (n-k)a_{n-k-1}, \quad \text{for } n \geqslant k \geqslant 1. \\ &\vdots \end{aligned}$$
  and so on, by recursion.

  The **relation** $a_n = na_{n-1}$, $n \in \mathbb{N}$, $n \geqslant 1$, together with the **initial condition** $a_0 = 1$ defines the sequence uniquely, since
  $$\begin{aligned} a_n &= na_{n-1} \quad \text{for } n \geqslant 1 \\ &= n[(n-1)a_{n-2}] && \{\text{by recursion}\} \\ &= n(n-1)[(n-2)a_{n-3}] && \{\text{by recursion}\} \\ &\vdots \\ &= n(n-1)(n-2)\,....\times 2 \times 1 \times a_0 \\ &= n! && \{\text{since } a_0 = 1\} \end{aligned}$$

  The form $a_0 = 1$, $a_n = na_{n-1}$, $n \geqslant 1$ is called a **recurrence relation** for this sequence.

- The Fibonacci sequence can be defined by the recurrence relation $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$, $n \geqslant 2$, which gives the values 0, 1, 1, 2, 3, 5, 8, 13, 21, ...
  In **Exercise 1A.2** question **12**, strong induction was used to prove that
  $$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n, \quad n \in \mathbb{N}$$
  is the closed form solution for the Fibonacci sequence. The two definitions, closed form and recursive, are both useful.
  From the recursive definition it is easy to observe that all terms in the Fibonacci sequence are integers; this is not obvious from the closed form solution. However, if we wish to calculate an arbitrary term in the Fibonacci sequence, for example a_{100}, then the closed form solution is more useful than the recursive definition.

A **recurrence relation** for the sequence $\{a_n\}$, $n \in \mathbb{N}$, is an equation which relates the term a_n to some or all of the preceding terms in the sequence, together with *initial values* for the first few terms.

For a sequence $\{a_n\}$, $n \in \mathbb{N}$, a **recurrence relation of degree (or order)** $\boldsymbol{r}$ for the sequence is a relationship which defines the term a_n as a function of a_{n-r} and possibly also $a_{n-1}, a_{n-2}, ..., a_{n-r+1}$, and n. Hence $a_n = f(a_{n-1}, a_{n-2}, ..., a_{n-r}) + g(n)$, where f and g are functions, together with **initial values** for the first r terms $a_0, a_1, ..., a_{r-1}$, of the sequence.

- If $g(n) = 0$ for all $n \in \mathbb{N}$ then the recurrence relation is **homogeneous**; otherwise it is **inhomogeneous**.
- If $f(a_{n-1}, a_{n-2}, ..., a_{n-r}) = h_1(n)a_{n-1} + h_2(n)a_{n-2} + ... + h_r(n)a_{n-r}$ for some functions $h_1, h_2, ..., h_r$ of n, then the recurrence relation is **linear**, otherwise it is **non-linear**.
- If a recurrence relation is linear and each function $h_i(n)$, $i = 1, ..., r$, is a constant, then the recurrence relation is said to have **constant coefficients**.

For example:

- The Fibonacci sequence defined by $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$, $n \geqslant 2$ is a second-degree linear homogeneous recurrence relation with constant coefficients.
- $a_0 = -2$, $a_n = 5a_{n-1}$, $n \geqslant 1$ is a first-degree linear homogeneous recurrence relation with constant coefficients.
  The corresponding sequence is:
  $$\begin{aligned} a_0 &= -2 \\ a_1 &= 5 \times a_0 = 5 \times (-2) &&= -10 \\ a_2 &= 5 \times a_1 = 5 \times (5 \times -2) &= 5^2 \times (-2) &= -50 \\ a_3 &= 5 \times a_2 = 5 \times (5^2 \times -2) &= 5^3 \times (-2) &= -250 \\ &\vdots \end{aligned}$$
  This is a **geometric sequence** with closed form solution $a_n = 5^n \times -2$, $n \in \mathbb{N}$.
- $a_0 = 10$, $a_n = a_{n-1} - 7$, $n \geqslant 1$, is a first-degree linear inhomogeneous recurrence relation with constant coefficients.
  The corresponding sequence is:
  $$\begin{aligned} a_0 &= 10 \\ a_1 &= a_0 - 7 = 10 - 7 &&= 3 \\ a_2 &= a_1 - 7 = (10 - 7) - 7 &= 10 - 2 \times 7 &= -4 \\ a_3 &= a_2 - 7 = (10 - 2 \times 7) - 7 &= 10 - 3 \times 7 &= -11 \\ &\vdots \end{aligned}$$
  This is an **arithmetic sequence** with closed form solution $a_n = 10 - 7n$, $n \in \mathbb{N}$.

- $a_0 = 1,\ a_1 = 5,\ a_2 = -2,\ a_n = a_{n-1}^2 + a_{n-2}a_{n-3},\ n \geqslant 3,$ is a third-degree non-linear homogeneous recurrence relation.

  The corresponding sequence is: $$\begin{aligned} a_3 &= a_2^2 + a_1a_0 = (-2)^2 + 5 \times 1 &&= 9 \\ a_4 &= a_3^2 + a_2a_1 = 9^2 + (-2) \times 5 &&= 71 \\ a_5 &= a_4^2 + a_3a_2 = (71)^2 + 9 \times (-2) &&= 5023 \\ &\ \vdots \end{aligned}$$

- $a_0 = 1,\ a_n = a_{n-1} + n,\ n \geqslant 1$ is a first-degree linear inhomogeneous recurrence relation with constant coefficients.

  The corresponding sequence is: 1, 2, 4, 7, 11, 16, ...

- $a_0 = 0,\ a_n^2 = 1 + a_{n-1},\ n \geqslant 1$ is a first-degree non-linear inhomogeneous recurrence relation.

  This recurrence relation does not define a unique sequence, since at least two sequences can be found to satisfy the recurrence relation:

$$0,\ -1,\ 0,\ -1,\ 0,\ -1,\ 0,\ -1,\ \ldots. \quad \text{and} \quad 0,\ 1,\ \sqrt{2},\ \sqrt{1+\sqrt{2}},\ \sqrt{1+\sqrt{1+\sqrt{2}}},\ \ldots. .$$

This last example shows that not all recurrence relations define a unique sequence.

We state without proof the following result:

> Any linear homogeneous recurrence relation of degree r with constant coefficients $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots. + c_ra_{n-r}$ (where $c_r \neq 0$ since the recurrence relation is of degree r), together with **initial values** for the first r terms $a_0,\ a_1,\ a_2,\ \ldots.,\ a_{r-1},$ defines a *unique* solution sequence $\{a_n\},\ n \in \mathbb{N}$.

Example 4

For each sequence below:

i Find the first four terms of the sequence described by the given recurrence relation, and conjecture a closed form solution.

ii Use induction to prove your conjecture.

iii Hence calculate a_{100}.

a $a_0 = 2,\ a_n = a_{n-1} + 3,\ n \geqslant 1$

b $a_0 = 1,\ a_n = \left(\dfrac{n}{n+1}\right) a_{n-1},\ n \geqslant 1$

a **i** This is a first-degree linear inhomogeneous recurrence relation with constant coefficients.

$$\begin{aligned} a_0 &= 2 \\ a_1 &= a_0 + 3 = 2 + 3 = 5 \\ a_2 &= a_1 + 3 = (2+3) + 3 = 2 + 2 \times 3 = 8 \\ a_3 &= a_2 + 3 = (2 + 2 \times 3) + 3 = 2 + 3 \times 3 = 11 \end{aligned}$$

Conjecture: $a_n = 2 + 3n,\ n \in \mathbb{N}$

ii For $n = 0,\ a_0 = 2 + 3 \times 0 = 2$ ✓

If $a_k = 2 + 3k$

then $a_{k+1} = a_k + 3 = (2 + 3k) + 3 = 2 + 3(k+1)$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = 2 + 3n$ for all $n \in \mathbb{N}$.

iii $a_{100} = 2 + 3 \times 100 = 302$

b **i** This is a first-order linear homogeneous recurrence relation.

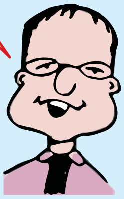
$$a_0 = 1$$

$$a_1 = \frac{1}{(1+1)}a_0 = \tfrac{1}{2} \times 1 = \tfrac{1}{2}$$

$$a_2 = \frac{2}{(2+1)}a_1 = \tfrac{2}{3} \times \tfrac{1}{2} = \tfrac{1}{3}$$

$$a_3 = \frac{3}{(3+1)}a_2 = \tfrac{3}{4} \times \tfrac{1}{3} = \tfrac{1}{4}$$

Conjecture: $a_n = \dfrac{1}{n+1}, \quad n \in \mathbb{N}.$



For first-degree recurrence relations we can use weak induction to prove a closed form solution.

ii For $n = 0, \ a_0 = \dfrac{1}{0+1} = 1$ ✓

If $a_k = \dfrac{1}{k+1}$

then $a_{k+1} = \dfrac{k+1}{(k+1)+1} \times a_k = \dfrac{(k+1)}{(k+2)} \times \dfrac{1}{(k+1)} = \dfrac{1}{k+2} = \dfrac{1}{(k+1)+1}$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = \dfrac{1}{n+1}$ for all $n \in \mathbb{N}$.

iii $a_{100} = \dfrac{1}{100+1} = \dfrac{1}{101}$

EXERCISE 1B.1

1 For each sequence below:

i Find the first five terms of each sequence described by the given recurrence relation, and conjecture a closed form solution.

ii Use induction to prove your conjecture.

a $a_n = a_{n-1} + 2, \ n \geqslant 1, \ a_0 = 12$

b $a_n = 3a_{n-1}, \ n \geqslant 1, \ a_0 = 10$

c $a_{n+1} = 3a_n, \ n \geqslant 1, \ a_1 = 10$

d $a_n = 2a_{n-1} + 10, \ n \geqslant 1, \ a_0 = 1$

e $a_n = a_{n-1} + k, \ n \geqslant 1, \ a_0 = 0,$ where k is a non-zero constant

f $a_n = ka_{n-1}, \ n \in \mathbb{Z}^+, \ a_0 = 1,$ where k is a non-zero constant

g $a_n = na_{n-1}, \ n \in \mathbb{Z}^+, \ n \geqslant 2, \ a_1 = 1$

h $x_{n+1} = x_n + (2n+3), \ n \in \mathbb{Z}^+, \ x_0 = 1$

2 Express each sequence as a recurrence relation and conjecture its closed form solution:

a 5, 7, 9, 11, ...

b 5, 6, 9, 14, 21, 30, ...

c 5, 10, 20, 40, 80, ...

d 2, 8, 24, 64, 160, ...

e 1, 1, 2, 3, 5, 8, 13, ...

3 For each sequence below:

i Find the first four terms of the sequence described by the recurrence relation, and conjecture a closed form solution.

ii Use induction to prove your conjecture.

iii Find a_{100}.

a $a_n = a_{n-1} + 2n - 1, \ n \in \mathbb{Z}^+, \ a_0 = 0$

b $a_n = a_{n-1} + 2n + 1, \ n \geqslant 1, \ a_0 = 1$

c $a_n = a_{n-1} + n, \ n \in \mathbb{Z}^+, \ a_0 = 0$

d $a_n = a_{n-1} + n + 1, \ n \in \mathbb{Z}^+, \ a_0 = 1$

e $a_n = a_{n-1} + n^3, \ n \in \mathbb{Z}^+, \ a_0 = 0$ **Hint:** Compare to the sequence in **c**.

f $a_n = (n+1)a_{n-1}, \ n \geqslant 1, \ a_0 = 1$

4 Consider the recurrence relation $a_0 = c$, $a_n = ra_{n-1}$, $n \in \mathbb{Z}^+$ where $r, c \in \mathbb{Z}$ are constants.

a Calculate the first four terms of the sequence.

b Hence state a closed form solution for the geometric sequence a_n, $n \in \mathbb{N}$.

5 Consider the recurrence relation $a_0 = c$, $a_n = a_{n-1} + b$, $n \in \mathbb{Z}^+$ where $c, b \in \mathbb{Z}$ are constants.

a Calculate the first four terms of the sequence.

b Hence state a closed form solution for the arithmetic sequence a_n, $n \in \mathbb{N}$.

6 Consider the recurrence relation $a_0 = c$, $a_n = ra_{n-1} + b$, $n \in \mathbb{Z}^+$ where $r, b, c \in \mathbb{Z}$ are constants and $r \neq 1$.

a Calculate the first five terms of the sequence.

b Derive the closed form solution $a_n = r^n c + b\left(\dfrac{r^n - 1}{r - 1}\right)$, $n \in \mathbb{N}$.

Example 5

Consider the recursive definition $a_n = 2a_{n-1} - a_{n-2}$, $n \geqslant 2$.

a Why is this an improperly defined recurrence relation?

b Show that $a_n = 3n$, $n \in \mathbb{N}$ is a closed form solution.

c Show that $a_n = 5$, $n \in \mathbb{N}$ is a closed form solution.

a Initial values for a_0 and a_1 are required to complete the definition of the recurrence relation.

b If $a_n = 3n$, $n \in \mathbb{N}$ then for $n \geqslant 2$, $a_{n-2} = 3(n-2)$
and $a_{n-1} = 3(n-1)$.

$$\begin{aligned}\therefore\quad 2a_{n-1} - a_{n-2} &= 2 \times 3(n-1) - 3(n-2)\\ &= 6n - 6 - 3n + 6\\ &= 3n\\ &= a_n\end{aligned}$$

$\therefore$ $a_n = 3n$, for $n \in \mathbb{N}$ is a closed form solution.

c If $a_n = 5$ for all $n \in \mathbb{N}$, then for $n \geqslant 2$, $2a_{n-1} - a_{n-2} = 2 \times 5 - 5 = 5 = a_n$.
Thus $a_n = 5$, $n \in \mathbb{N}$, is a closed form solution.

7 Consider the recursive definition $a_n = a_{n-1} + a_{n-2} - a_{n-3}$, $n \geqslant 3$.

a Is this a properly defined recurrence relation? Explain your answer.

b Show that $a_n = c$, $n \in \mathbb{N}$, $c \in \mathbb{R}$ is a closed form solution.

c Show that $a_n = cn + d$, $n \in \mathbb{N}$, $c, d \in \mathbb{R}$ is a closed form solution.

Example 6

Use the identity $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ to find a closed form solution for the recurrence relation:

$$a_0 = c \text{ (a constant)}, \quad a_n = a_{n-1} + n, \quad n \geqslant 1.$$

$$\begin{aligned}
a_0 &= c \\
a_1 &= a_0 + 1 = c + 1 \\
a_2 &= a_1 + 2 = (c+1) + 2 = c + 1 + 2 \\
a_3 &= a_2 + 3 = (c+1+2) + 3 = c + 1 + 2 + 3 \\
a_4 &= a_3 + 4 = (c+1+2+3) + 4 = c + 1 + 2 + 3 + 4 \\
&\vdots \\
a_n &= c + 1 + 2 + 3 + ... + (n-1) + n
\end{aligned}$$

$$\therefore \quad a_n = c + \sum_{i=1}^{n} i = c + \frac{n(n+1)}{2}, \quad n \in \mathbb{N}$$

8 Use the identity $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ to find a closed form solution for the recurrence relation:

$$a_0 = c \text{ (a constant)}, \quad a_n = a_{n-1} + n^2, \quad n \in \mathbb{Z}^+.$$

FIRST-DEGREE LINEAR RECURRENCE RELATIONS

A **first-degree linear recurrence relation** has the form

$$a_0 = c, \quad a_n = h(n)a_{n-1} + g(n), \quad n \geqslant 1$$

where $a_0 = c$ is a constant and $h(n)$, $g(n)$ are functions of n, $n \in \mathbb{N}$.

In the previous exercise, you should have found the following results:

Special cases	**Recurrence relation** for $n \in \mathbb{N}$	**Closed form solution** for $n \in \mathbb{N}$
$g(n) = 0$ **homogeneous** $h(n) = r$ **constant coefficients**	$a_0 = c, \quad a_n = ra_{n-1}, \quad n \geqslant 1$	Geometric sequence $a_n = r^n c$
$g(n) = b$, constant. **inhomogeneous** $h(n) = 1$ **constant coefficient** of 1	$a_0 = c, \quad a_n = a_{n-1} + b, \quad n \geqslant 1$	Arithmetic sequence $a_n = c + nb$
$g(n) = b$, constant. **inhomogeneous** $h(n) = r, \quad r \neq 1$ **constant coefficient** $r \neq 1$	$a_0 = c, \quad a_n = ra_{n-1} + b, \quad n \geqslant 1$	$a_n = r^n c + b\left(\frac{r^n - 1}{r - 1}\right)$ where $r \neq 1$.
$g(n)$ a function of n **inhomogeneous** $h(n) = 1$	$a_0 = c, \quad a_n = a_{n-1} + g(n)$	Can be found for certain forms of $g(n)$.

MODELLING WITH FIRST-DEGREE LINEAR RECURRENCE RELATIONS

Problems involving simple interest, compound interest, and debt repayment can often be formulated in terms of first-degree linear recurrence relations.

SINGLE DEPOSIT COMPOUNDED INVESTMENT

Example 7

Suppose €45 000 is invested at 7.5% p.a. with interest compounded at the end of each quarter. No withdrawals are made.

a Write a recurrence relation for a_n, the value of the investment after n compounding periods.

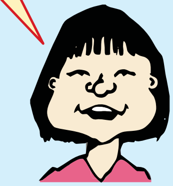
b Write down the closed form solution for a_n, $n \in \mathbb{N}$.

c Find the value of the investment after 3 years.

d What initial amount should be invested under the same conditions to obtain a value of €80 000 after $2\frac{1}{2}$ years?

a
$$a_n = \left(1 + \frac{0.075}{4}\right) a_{n-1}, \quad n \geqslant 1$$
$$\therefore \quad a_n = (1.018\,75)a_{n-1}, \quad n \geqslant 1$$
with $a_0 = 45\,000$

b
$$\begin{aligned} a_n &= 1.018\,75a_{n-1} \\ &= 1.018\,75(1.018\,75a_{n-2}) && \{\text{by recursion}\} \\ &= (1.018\,75)^2 a_{n-2} \\ &= (1.018\,75)^2(1.018\,75a_{n-3}) && \{\text{by recursion}\} \\ &= (1.018\,75)^3 a_{n-3} \\ &\;\vdots \\ &= (1.018\,75)^n a_0 \end{aligned}$$
$$\therefore \quad a_n = (1.018\,75)^n \times 45\,000, \quad n \in \mathbb{N}$$



For a recurrence relation to be properly defined, there must be appropriate initial conditions.

c A period of 3 years corresponds to $3 \times 4 = 12$ compounding periods.

Now $a_{12} = (1.018\,75)^{12} \times 45\,000$
$\approx$ €56 237.24

$\therefore$ the investment is worth $\approx$ €56 237.24 .

d $2\frac{1}{2}$ years corresponds to $2\frac{1}{2} \times 4 = 10$ compounding periods.

If $80\,000 = (1.018\,75)^{10} a_0$
then $a_0 \approx 66\,437.6$

$\therefore$ at least €66 438 must be invested.

CONSTANT AND REGULAR DEPOSIT COMPOUNDED INVESTMENT

Example 8

At the time when an employee joins a company, he has a savings account with \$500 balance. The savings account earns 10% p.a. interest compounded monthly. At the end of the month, the employee makes a salary sacrifice of \$500 which is deposited into the account.

Let a_n be the amount in the account n compounding periods after the account is opened.

a Calculate a_0, a_1, a_2, a_3, and a_4.

b For $n \geqslant 1$, write an equation for a_n in terms of a_{n-1}.

c Solve the resulting recurrence relation, that is state a closed form solution.

d What is the value of the investment after 5 years?

e How long does it take for the value of the investment to reach at least $50 000?

a $a_0 = 500$ {the account has $500 balance initially}

$$a_1 = \left(1 + \frac{0.1}{12}\right) 500 + 500$$

$$= \frac{121}{120} \times a_0 + 500 \approx 1004.17$$

$$a_2 = \frac{121}{120} \times a_1 + 500 \approx 1512.53$$

$$a_3 = \frac{121}{120} \times a_2 + 500 \approx 2025.14$$

b $a_n = \frac{121}{120} a_{n-1} + 500, \quad n \geqslant 1$

Be careful to not round $1 + \frac{0.1}{12} \approx 1.0083$ as your solution will lose accuracy.

c The recurrence relation is $a_0 = 500, \quad a_n = r a_{n-1} + 500, \quad n \geqslant 1$ where $r = \frac{121}{120}$.

Using the summary table, we could write
$$a_n = r^n 500 + 500\left(\frac{r^n - 1}{r-1}\right)$$
$$= 500(r^n + r^{n-1} + ... + r + 1)$$
$$= 500\left(\frac{r^{n+1} - 1}{r-1}\right)$$

Alternatively,
$$a_n = r a_{n-1} + 500$$
$$= r[r a_{n-2} + 500] + 500$$
$$= r^2 a_{n-2} + 500r + 500$$
$$\vdots$$
$$= r^n a_0 + 500[r^{n-1} + r^{n-2} + ... + r + 1]$$
$$= 500[r^n + ... + r^2 + r + 1]$$
$$= 500\left[\frac{r^{n+1} - 1}{r-1}\right]$$
$$= 500\left[\frac{\left(\frac{121}{120}\right)^{n+1} - 1}{\left(\frac{121}{120}\right) - 1}\right], \quad n \in \mathbb{N}$$

d $a_{60} = 500\left[\frac{\left(\frac{121}{120}\right)^{61} - 1}{\frac{121}{120} - 1}\right] \approx \$39\,541.19$

$\therefore$ after 5 years the investment is worth $\approx$ $39 541.19 .

e If $50\,000 = 500\left[\frac{\left(\frac{121}{120}\right)^{n+1} - 1}{\left(\frac{121}{120}\right) - 1}\right]$

then $n \approx 72.04$ {using technology}

$\therefore$ it will take at least 73 months, or 6 years and 1 month, to reach $50 000.

REPAYING A LOAN WITH CONSTANT AND REGULAR REPAYMENTS

Example 9

Josef borrows $12 000 to buy a car, with interest charged at 8% p.a. compounded monthly. Josef wishes to repay the loan in regular monthly repayments. The first repayment is due one month after the loan is taken out, after the first amount of interest is calculated and added to the loan.

Let a_n be the outstanding value of the loan after n months.

a Suppose Josef repays a regular monthly amount of $300.

i Calculate a_0, a_1, a_2, and a_3.

ii Write a_n in terms of a_{n-1}, $n \geqslant 1$, and state an appropriate initial condition for the recurrence relation.

iii Find a closed form solution for the recurrence relation.

iv What is the outstanding debt after 1 year?

v How long will it take Josef to repay the loan?

vi Calculate the total interest paid over the full term of the loan.

b Now suppose instead that Josef is prepared to take up to 5 years to repay the loan.

i Calculate the regular monthly repayment amount required to repay the loan over 5 years.

ii Calculate the total interest paid over the full term of the loan.

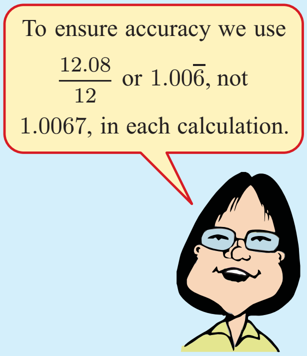
a **i** $a_0 = 12\,000$

$$a_1 = \left(1 + \frac{0.08}{12}\right) a_0 - 300$$

$$= \left(\frac{12.08}{12}\right) a_0 - 300 \approx 11\,780$$

$$a_2 = \left(\frac{12.08}{12}\right) a_1 - 300 \approx 11\,558.53$$

$$a_3 = \left(\frac{12.08}{12}\right) a_2 - 300 \approx 11\,335.6$$


To ensure accuracy we use $\frac{12.08}{12}$ or $1.00\overline{6}$, not 1.0067, in each calculation.

ii $a_0 = 12\,000$, $a_n = \left(\frac{12.08}{12}\right) a_{n-1} - 300$, $n \geqslant 1$

or $a_n = r a_{n-1} - 300$, $n \geqslant 1$ where $r = \frac{12.08}{12}$

iii

$$a_0 = 12\,000$$

$$a_1 = r(12\,000) - 300$$

$$a_2 = r[r 12\,000 - 300] - 300$$

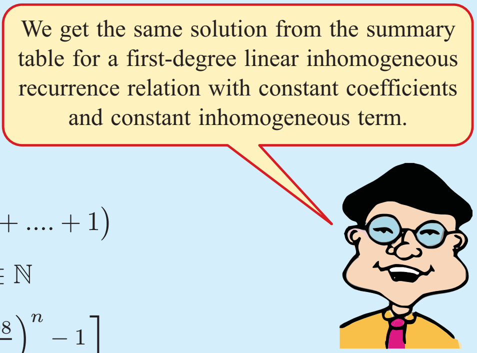
$$= r^2 12\,000 - r300 - 300$$

$$\vdots$$

$$a_n = r^n 12\,000 - 300\left(r^{n-1} + r^{n-2} + ... + 1\right)$$

$$\therefore\ a_n = r^n 12\,000 - 300\left[\frac{r^n - 1}{r - 1}\right], \quad n \in \mathbb{N}$$

$$\therefore\ a_n = \left(\frac{12.08}{12}\right)^n 12\,000 - 300\left[\frac{\left(\frac{12.08}{12}\right)^n - 1}{\left(\frac{12.08}{12}\right) - 1}\right], \quad n \in \mathbb{N}$$


We get the same solution from the summary table for a first-degree linear inhomogeneous recurrence relation with constant coefficients and constant inhomogeneous term.

iv One year corresponds to 12 monthly repayments. $a_{12} = 9261.02$

$\therefore$ the outstanding debt is about $9261.

v If $\left(\frac{12.08}{12}\right)^n 12\,000 - 300\left[\frac{\left(\frac{12.08}{12}\right)^n - 1}{\left(\frac{12.08}{12}\right) - 1}\right] = 0$

then $n \approx 46.68$ {using technology}

$\therefore$ the loan will be repayed after 47 months (or 3 years and 11 months).

vi The total amount repaid $= 47 \times \$300$

$= \$14\,100$

$\therefore$ the total interest paid $= \$14\,100 - \$12\,000$

$= \$2100$

b **i** Using the working from **a** with repayment amount $\$p$, the closed form solution is $a_n = r^n 12\,000 - p\left[\frac{r^n - 1}{r - 1}\right]$.

Using technology to solve $\left(\frac{12.08}{12}\right)^{60} 12\,000 - p\left[\frac{\left(\frac{12.08}{12}\right)^{60} - 1}{\left(\frac{12.08}{12}\right) - 1}\right] = 0,$

we find $p \approx 243.32$

$\therefore$ a regular monthly repayment of \$244 is required to repay the loan over 5 years.

ii The total amount repaid $= 60 \times \$244$

$= \$14\,640$

$\therefore$ the total interest paid $= \$14\,640 - \$12\,000$

$= \$2640$

EXERCISE 1B.2

1 Write down the closed form solution for each given first-degree linear recurrence relation:

a $a_0 = 0, \ a_n = 100a_{n-1}, \ n \geqslant 1$

b $a_0 = 3, \ a_n = 100a_{n-1}, \ n \geqslant 1$

c $a_1 = 500, \ a_n = 10a_{n-1}, \ n \geqslant 2$

d $a_0 = 3, \ a_n = a_{n-1} - 5, \ n \geqslant 1$

e $a_0 = 0, \ a_n = a_{n-1} + 1, \ n \geqslant 1$

f $a_2 = -17, \ a_n = a_{n-1} - 4, \ n \geqslant 3$

g $a_0 = 1, \ a_n = 3a_{n-1} + 5, \ n \geqslant 1$

h $a_0 = 3, \ a_n = -2a_{n-1} + 6, \ n \geqslant 1$

i $a_0 = 0, \ a_n = 5a_{n-1} + 3, \ n \geqslant 1$

2 The number of cells in a culture triples every hour.
Let a_n equal the number of cells in the culture after n hours.

a Write a relation for a_n in terms of a_{n-1} for $n \geqslant 1$.

b Write down a closed form solution for a_n in terms of a_0, the number of cells in the culture initially.

c Suppose there are 20 000 cells in the culture after 6 hours.

i How many cells were in the culture initially?

ii How many cells will be in the culture after one full day?

iii How long will it take for the culture to grow to 51 000 000 cells?

3 A **binary sequence** or **bit string** of length n is a sequence of length n consisting of 0s and 1s. Find and solve a recurrence relation for the number of binary sequences of length n.

4 \$500 is deposited into an account which earns 10% interest per annum, calculated at the end of each year. There are no withdrawals.
Let a_n be the amount (in dollars) in the account n years after the initial deposit.

- **a** Calculate a_0, a_1, a_2, and a_3.
- **b** Write a recurrence relation for a_n in terms of a_{n-1}, $n \geqslant 1$. Include the necessary initial condition.
- **c** Derive the closed form solution for a_n, $n \in \mathbb{N}$.
- **d** Find the value of the investment after 10 years.
- **e** How long does it take for the inital value to be doubled?

5 A savings account earns interest at 12% per annum. Suppose a_0 is the initial investment, and let a_n be the amount in the account after n compounding periods. a_n satisfies the recurrence relation $a_n = ra_{n-1}$, $n \geqslant 1$, where r is a growth multiplier for each compounding period.

- **a** Solve the recurrence relation to obtain a closed form solution.
- **b** Find r if the interest is compounded:
  i annually **ii** quarterly **iii** monthly.
- **c** Suppose $a_0 = 10\,500$ dollars. Find the amount in the account after 3 years, if the interest is compounded:
  i annually **ii** quarterly **iii** monthly.

6 A radioactive substance decays by 15% each day. Initially there are a_0 grams of the substance in a sample.

- **a** Find and solve a recurrence relation for the amount of the substance remaining after n days.
- **b** What initial mass would be necessary for 80 g to remain after 7 days?

7 \$1000 is invested at 4.8% per annum compounding annually. At the end of each year, the interest is added, and then your Christmas bonus of \$100 is deposited into the account. There are no withdrawals.
Let a_n be the value of the investment after n years.

- **a** Find: **i** a_0 **ii** a_1 **iii** a_2 **iv** a_3.
- **b** Find and solve a recurrence relation for the amount in the account after n years.
- **c** How long does it take for the initial investment to double?

8 A bacterial culture doubles in size every three hours. Suppose 800 bacteria are present initially.
Let a_n be the number of bacteria present after $3n$ hours, $n \in \mathbb{N}$.

- **a** Find and solve a recurrence relation for a_n, $n \in \mathbb{N}$.
- **b** How many bacteria are present after 1 day?
- **c** How long does it take for the culture to grow to 1 000 000 bacteria?

9 A steel works initially produces 2000 tonnes of steel per month. Production is increased by 1% per month, while orders remain constant at 1600 tonnes per month.
Let a_n be the number of tonnes of steel held in stock after n months,
where $a_0 = 2000 - 1600 = 400$ tonnes.

- **a** Find and solve a recurrence relation for a_n, $n \in \mathbb{N}$.
- **b** How much steel is held in stock after:
  i 12 months **ii** 2 years.
- **c** How long will it take for the amount held in stock to reach 30 000 tonnes?

10 A savings account contains £5000 initially. The account earns 9% per annum compounded monthly, and at the end of each month an additional £40 is added to the account.
Let a_n be the amount in the account after n months.

- **a** Find a_0, a_1, a_2, and a_3.
- **b** Find and solve a recurrence relation for a_n, $n \in \mathbb{N}$.
- **c** Calculate the amount in the account after 4 years.
- **d** How long will it take for the investment to reach £15 000?

11 A credit card loan of \$3000 is taken out at a nominal interest rate of 24% per annum compounded monthly. The loan is to be repaid in monthly instalments of \$200 which begin at the end of the first month.
Let a_n be the amount owed after n months, $n \in \mathbb{N}$.

- **a** Find a_0, a_1, a_2, and a_3.
- **b** Find and solve a recurrence relation for a_n, $n \in \mathbb{N}$.
- **c** How long will it take to repay the entire loan?

12 Suppose an amount a_0 is borrowed with interest calculated and compounded at the end of each compounding period. Suppose also that immediately after the interest is calculated and compounded, a repayment of amount p is made in each period.
Let a_n be the outstanding debt after n compounding periods.
Show that:

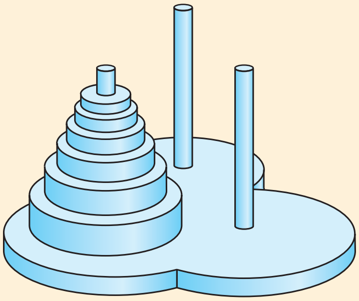
- **a** the recurrence relation for the amount outstanding is $a_0 = a_0$, $a_n = ra_{n-1} - p$, $n \geqslant 1$ where r is the growth multiplier for each compounding period
- **b** the corresponding closed form solution is $a_n = r^n a_0 - p\left[\dfrac{r^n - 1}{r - 1}\right]$, $n \in \mathbb{N}$.

13 \$20 000 is borrowed at 13% per annum compounded fortnightly. The loan is to be repaid in regular fortnightly instalments beginning one fortnight after the loan is taken out.
Let a_n be the amount owing after n fortnights, $n \in \mathbb{N}$.

- **a** Explain why the fortnightly repayment must be greater than \$100.
- **b** Suppose the regular fortnightly repayment is \$200.
  - **i** Calculate a_0, a_1, a_2, and a_3.
  - **ii** Write a recurrence relation for a_n in terms of a_{n-1}, $n \geqslant 1$, including the appropriate initial condition.
  - **iii** Show that $a_n = 40\,000 - 20\,000(1.005)^n$, $n \in \mathbb{N}$.
  - **iv** What is the outstanding debt after 2 years?
  - **v** How long will it take to repay the loan?
  - **vi** Calculate the total interest paid over the full term of the loan.
- **c** Suppose instead that the loan must be repaid in 4 years.
  - **i** Calculate the fortnightly repayment required to pay off the loan in 4 years.
  - **ii** Calculate the total interest paid over the full term of the loan.

INVESTIGATION 1 THE TOWER OF HANOI

The **Tower of Hanoi** is a famous puzzle consisting of n, $n \in \mathbb{N}$, discs with distinct radii placed from largest to smallest on one of three poles.



The objective of the puzzle is to move the discs one at a time from pole to pole, with no larger disc ever sitting on top of a smaller disc, and to finish with all discs on a different pole to the starting pole.

Let a_n be the smallest number of moves required to solve the puzzle for n discs, $n \in \mathbb{N}$.

What to do:

1 Play the game and verify that $a_0 = 0$, $a_1 = 1$, $a_2 = 3$, $a_3 = 7$, $a_4 = 15$, $a_5 = 31$.

GAME

2 Suppose the puzzle is solved for $n-1$ discs, $n \geqslant 1$, so that a_{n-1} is known.

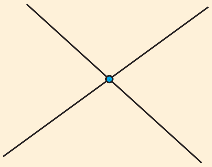
- **a** Consider the puzzle with n discs and explain why $a_n = 2a_{n-1} + 1$.
- **b** Hence show that:
  - **i** $a_n = 2^2 a_{n-2} + 2 + 1$
  - **ii** $a_n = 2^3 a_{n-3} + 2^2 + 2^1 + 2^0$.
- **c** Continue the process in **b** until a_n can be expressed in terms of a_0. Hence derive a closed form solution for a_n, $n \in \mathbb{N}$.

INVESTIGATION 2 LINES AND REGIONS

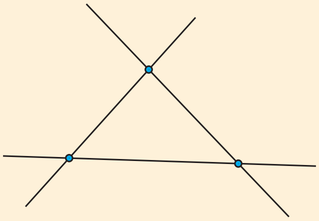
Suppose n lines are drawn in the Euclidean plane such that no two lines are parallel, and no three lines meet in a point.

The cases $n = 2$ and $n = 3$ are shown:

$n = 2$



$n = 3$



What to do:

1 Let a_n be the number of points of intersection in the configuration with n lines, $n \in \mathbb{N}$. For example: $a_2 = 1$ and $a_3 = 3$.

- **a** Draw the cases $n = 4$ and $n = 5$.
- **b** Write down the values for a_0, a_1, a_2, a_3, a_4, and a_5.

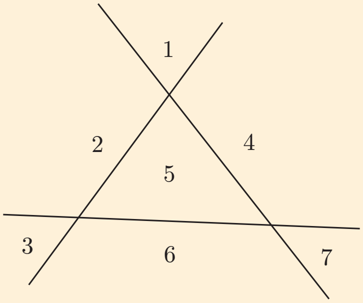
c Write down the relation between a_n and a_{n-1} for $n \geqslant 2$.
Hint: Consider how the case $n = 5$ is obtained from the case $n = 4$.

d Hence write a_n in terms of:

i a_{n-2} **ii** a_{n-3} **iii** a_0

e State the closed form solution for a_n, $n \in \mathbb{N}$.

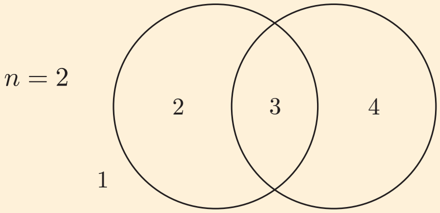
2 Repeat **1**, but this time let a_n be the number of regions the plane is divided into by the n lines, $n \in \mathbb{N}$.
For example: $a_3 = 7$ regions.

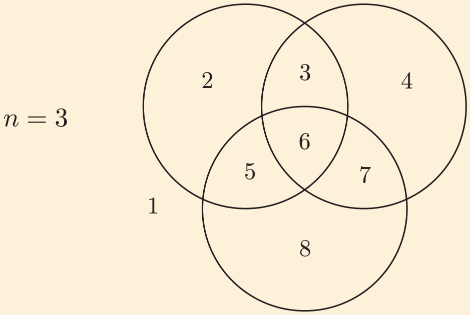


INVESTIGATION 3 INTERSECTING CIRCLES

Suppose n circles are drawn in the plane such that each pair of circles meet in exactly two distinct points and no three circles meet in a point.

The cases $n = 2$ and $n = 3$ are shown:





What to do:

Find and solve a recurrence relation for the number of regions into which the plane is divided by n such circles.

SOLVING HIGHER DEGREE RECURRENCE RELATIONS USING INDUCTION

Thus far we have made use of the following ad hoc process for solving recurrence relations:

1 Calculate the first few terms $a_0, a_1, a_2, ...$ of the sequence.

2 Observe a pattern either in the *values* $a_0, a_1, a_2, ...,$ or else in the *formula* for each term by leaving the terms in their general, un-summed form.

3 Derive or conjecture a closed form solution for the sequence.

4 Prove (if necessary) the conjectured solution is valid using an appropriate form of induction.

Some seemingly quite complicated recurrence relations can be solved using this approach, and in the absence of a general method of solution, it is worth trying.

Example 10

Consider the third-degree homogeneous recurrence relation with constant coefficients:

$$a_0 = a_1 = a_2 = 1$$
$$a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} = 0, \quad n \geqslant 3.$$

a Calculate the values of a_i for $i = 3$, 4, and 5.

b Conjecture a closed form solution for a_n, $n \in \mathbb{N}$.

c Use strong induction to prove your conjecture.

$a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} = 0, \quad n \geqslant 3$

$\therefore \quad a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3}$, where $a_0 = a_1 = a_2 = 1$

a $a_3 = 3a_2 - 3a_1 + a_0 = 3 \times 1 - 3 \times 1 + 1 = 1$

$a_4 = 3a_3 - 3a_2 + a_1 = 3 \times 1 - 3 \times 1 + 1 = 1$

$a_5 = 3a_4 - 3a_3 + a_2 = 3 \times 1 - 3 \times 1 + 1 = 1$

b We conjecture that $a_n = 1$ for all $n \in \mathbb{N}$.

c $a_0 = a_1 = a_2 = 1$ are given.

If $a_k = a_{k+1} = a_{k+2} = 1$ for $k \geqslant 0$

then
$$\begin{aligned} a_{k+3} &= 3a_{k+2} - 3a_{k+1} + a_k \\ &= 3 \times 1 - 3 \times 1 + 1 \\ &= 1 \end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = 1$ for all $n \in \mathbb{N}$.

Example 11

Find a closed form solution for the first-degree inhomogeneous recurrence relation

$$a_1 = 2, \quad a_n = 2a_{n-1} + 2^n, \quad n \geqslant 2.$$

$a_1 = 2$

$a_2 = 2a_1 + 2^2 = 2 \times 2 + 2^2 = 2 \times 2^2 = 8$

$a_3 = 2a_2 + 2^3 = 2 \times 8 + 2^3 = 3 \times 2^3 = 24$

$a_4 = 2a_3 + 2^4 = 2 \times 24 + 2^4 = 3 \times 2^4 + 2^4 = 4 \times 2^4 = 64$

We conjecture that $a_n = n2^n$, $n \geqslant 1$. We must prove this holds for all $n \geqslant 1$.

Now $a_1 = 1 \times 2^1 = 2$ ✓ is true.

If the conjecture is true for a_{k-1}, then $a_{k-1} = (k-1)2^{k-1}$

$$\begin{aligned} \therefore \quad a_k &= 2a_{k-1} + 2^k \\ &= 2(k-1)2^{k-1} + 2^k \\ &= (k-1)2^k + 2^k \\ &= (k-1+1)2^k \\ &= k2^k \quad ✓ \end{aligned}$$

$\therefore$ by the Principle of Mathematical Induction, $a_n = n2^n$ for all $n \geqslant 1$.

EXERCISE 1B.3

1 Consider the third-degree homogeneous recurrence relation with constant coefficients:

$$a_0 = 0, \;\; a_1 = 1, \;\; a_2 = 2$$
$$a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} = 0, \;\; n \geqslant 3.$$

- **a** Calculate values of a_i for $i = 3, 4, ..., 7$.
- **b** Conjecture a closed form solution for a_n, $n \in \mathbb{N}$.
- **c** Use strong induction to prove your conjecture.

2 Repeat question **1**, replacing the initial conditions with $a_0 = 0$, $a_1 = 1$, $a_2 = 4$.

3 Solve the third-degree homogeneous recurrence relation with constant coefficients:

$$a_n - 7a_{n-1} + 16a_{n-2} - 12a_{n-3} = 0, \;\; n \geqslant 3$$

with initial conditions:

a $a_0 = 1$, $a_1 = 2$, $a_2 = 4$ **b** $a_0 = 0$, $a_1 = 2$, $a_2 = 8$ **c** $a_0 = 1$, $a_1 = 3$, $a_2 = 9$

4 Consider the first-degree inhomogeneous linear recurrence relation

$$a_0 = 0, \;\; a_n = a_{n-1} + 2n(2n+1)(n-2) + 8n - 1.$$

- **a** Calculate values for a_1, a_2, a_3, and a_4.
- **b** Conjecture a closed form solution for a_n, $n \in \mathbb{N}$.
- **c** Prove your conjecture.

5 Find a closed form solution for each of the following second-degree recurrence relations:

a $a_0 = 1$, $a_1 = 2$, $a_n = 3a_{n-1} - 2a_{n-2}$ **b** $a_0 = 1$, $a_1 = 3$, $a_n = 4a_{n-1} - 3a_{n-2}$

6 Find a closed form solution for each of the following first-degree inhomogeneous recurrence relations:

a $a_0 = 1$, $a_n = na_{n-1} + n!$, $n \in \mathbb{Z}^+$ **b** $a_0 = 1$, $a_n = 2na_{n-1} + n!2^n$, $n \in \mathbb{Z}^+$

SECOND-DEGREE LINEAR HOMOGENEOUS RECURRENCE RELATIONS WITH CONSTANT COEFFICIENTS

In only special cases is it possible to observe a pattern in the initial values of a sequence and hence postulate a closed form solution. It is not a method that will work in general.

For example, using only the initial values of the Fibonacci sequence: 0, 1, 1, 2, 3, 5, 8, 13, ...
it is near impossible to guess the closed form solution

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n, \;\; n \in \mathbb{N}.$$

We can find this closed form solution because the Fibonacci recurrence relation belongs to a class of recurrence relations for which there is a known general method of solution.

Second-degree linear homogeneous recurrence relations with constant coefficients are of the form

$$a_n = aa_{n-1} + ba_{n-2}, \;\; n \geqslant 2$$

with initial conditions a_0, a_1, where a_0, a_1, a, b are given constants.

We have seen that any *first*-degree linear homogeneous recurrence relation with constant coefficients,

$$a_n = \lambda a_{n-1}, \quad n \geqslant 1 \quad \text{with } a_0 \text{ and } \lambda \text{ constants,}$$

has closed form solution $a_n = a_0\lambda^n$, $n \in \mathbb{N}$, which is a geometric sequence.

This gives us the clue that for second-degree linear homogeneous recurrence relations we should try solutions which involve geometric sequences.

Example 12

Consider the second-degree linear homogeneous recurrence relation with constant coefficients:

$$a_n = 5a_{n-1} - 6a_{n-2}, \quad n \geqslant 2 \quad \text{where} \quad a_0 = 0, \quad a_1 = 1.$$

a For the geometric sequence $a_n = 2^n$, $n \in \mathbb{N}$, show that $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geqslant 2$.

b For the geometric sequence $a_n = 3^n$, $n \in \mathbb{N}$, show that $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geqslant 2$.

c Let $a_n = c_1 2^n + c_2 3^n$, $n \in \mathbb{N}$, for c_1, c_2 any constants.

i Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geqslant 2$.

ii Use the initial conditions $a_0 = 0$, $a_1 = 1$ to solve for constants c_1, c_2. Hence write a closed form solution for the recurrence relation.

a If $a_n = 2^n$

then $a_{n-1} = 2^{n-1}$ and $a_{n-2} = 2^{n-2}$.

$$\begin{aligned}\therefore \quad & 5a_{n-1} - 6a_{n-2}\\ &= 5 \times 2^{n-1} - 6 \times 2^{n-2}\\ &= 5 \times 2^{n-1} - 3 \times 2 \times 2^{n-2}\\ &= 5 \times 2^{n-1} - 3 \times 2^{n-1}\\ &= 2 \times 2^{n-1}\\ &= 2^n\\ &= a_n\end{aligned}$$

b If $a_n = 3^n$

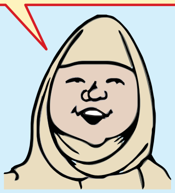
then $a_{n-1} = 3^{n-1}$ and $a_{n-2} = 3^{n-2}$.

$$\begin{aligned}\therefore \quad & 5a_{n-1} - 6a_{n-2}\\ &= 5 \times 3^{n-1} - 6 \times 3^{n-2}\\ &= 5 \times 3^{n-1} - 2 \times 3 \times 3^{n-2}\\ &= 5 \times 3^{n-1} - 2 \times 3^{n-1}\\ &= 3 \times 3^{n-1}\\ &= 3^n\\ &= a_n\end{aligned}$$

c **i** If $a_n = c_1 2^n + c_2 3^n$, then $a_{n-1} = c_1 2^{n-1} + c_2 3^{n-1}$ and $a_{n-2} = c_1 2^{n-2} + c_2 3^{n-2}$.

$$\begin{aligned}\therefore \quad & 5a_{n-1} - 6a_{n-2}\\ &= 5(c_1 2^{n-1} + c_2 3^{n-1}) - 6(c_1 2^{n-2} + c_2 3^{n-2})\\ &= c_1(5 \times 2^{n-1} - 6 \times 2^{n-2}) + c_2(5 \times 3^{n-1} - 6 \times 3^{n-2})\\ &= c_1 2^n + c_2 3^n \qquad \{\text{using } \mathbf{a} \text{ and } \mathbf{b}\}\\ &= a_n, \quad \text{as required.}\end{aligned}$$

This is what it means for the recurrence relation to be *linear*: any linear combination of solutions will also be a solution.



ii $a_0 = 0 = c_1 2^0 + c_2 3^0 \;\Rightarrow\; c_1 + c_2 = 0$

$a_1 = 1 = c_1 2^1 + c_2 3^1 \;\Rightarrow\; 2c_1 + 3c_2 = 1$

On solving the simultaneous equations $\begin{cases} c_1 + c_2 = 0 \\ 2c_1 + 3c_2 = 1 \end{cases}$ we obtain $c_1 = -1$, $c_2 = 1$

$\therefore \quad a_n = 3^n - 2^n$ is a solution to the given recurrence relation.

Motivated by this example, we seek solutions of the form $a_n = \lambda^n$ to a general second-degree linear homogeneous recurrence relation with constant coefficients

$$a_n = aa_{n-1} + ba_{n-2}, \quad n \geqslant 2, \quad \text{where } a \text{ and } b \text{ are constants.}$$

We need to solve $\lambda^n = a\lambda^{n-1} + b\lambda^{n-2}$, where $a_n = \lambda^n$, $a_{n-1} = \lambda^{n-1}$, and $a_{n-2} = \lambda^{n-2}$.

Assuming $\lambda \neq 0$, we divide through by λ^{n-2} and rearrange to obtain the quadratic equation

$$\lambda^2 - a\lambda - b = 0$$

called the **characteristic equation** of the recurrence relation.

If λ_1 and λ_2 are the solutions to the characteristic equation, then $a_n = {\lambda_1}^n$ and $a_n = {\lambda_2}^n$ are solutions to the relation $a_n = aa_{n-1} + ba_{n-2}$.

Consider the **second-degree linear homogeneous recurrence relation with constant coefficients**

$$a_n = aa_{n-1} + ba_{n-2}, \quad n \geqslant 2$$

with initial conditions a_0, a_1, where a_0, a_1, a, b are constants.

The **auxiliary** (or **characteristic**) **equation** for this recurrence relation is $\lambda^2 - a\lambda - b = 0$. We suppose the solutions to this equation are λ_1 and λ_2.

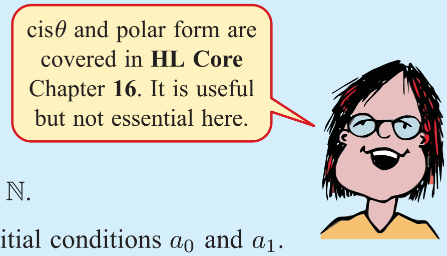
Case 1: If λ_1, λ_2 are **distinct real roots** then the recurrence relation has closed form solution
$$a_n = c_1{\lambda_1}^n + c_2{\lambda_2}^n, \quad n \in \mathbb{N}.$$

Case 2: If $\lambda_1 = \lambda_2 = \lambda$ are **equal roots**, then the recurrence relation has closed form solution
$$a_n = (c_1 + nc_2)\lambda^n, \quad n \in \mathbb{N}.$$

Case 3: If $\lambda_1, \lambda_2 = x \pm iy$ are **complex conjugate roots** then the recurrence relation has closed form solution
$$\begin{aligned} a_n &= c_1{\lambda_1}^n + c_2{\lambda_2}^n, \quad n \in \mathbb{N} \\ &= c_1(x+iy)^n + c_2(x-iy)^n. \end{aligned}$$

Using the appropriate polar form $x + iy = r\operatorname{cis}\theta = r(\cos\theta + i\sin\theta)$, the solution can also be written as
$$a_n = r^n(c_1 \operatorname{cis}(n\theta) + c_2 \operatorname{cis}(-n\theta)), \quad n \in \mathbb{N}.$$

In each case the constants c_1 and c_2 are found using the initial conditions a_0 and a_1.


cisθ and polar form are covered in **HL Core** Chapter **16**. It is useful but not essential here.

We do not provide a full proof of this result, but we can verify in each case that the given function is indeed a solution to the recurrence relation.

Case 1 and **Case 3:** Let $a_n = c_1{\lambda_1}^n + c_2{\lambda_2}^n$, $n \in \mathbb{N}$, where c_1, c_2 are constants and λ_1, λ_2 are distinct solutions to the characteristic equation $\lambda^2 - a\lambda - b = 0$.

$$\therefore \quad {\lambda_1}^2 = a\lambda_1 + b \quad \text{and} \quad {\lambda_2}^2 = a\lambda_2 + b \quad .... \ (*)$$

$$\begin{aligned} \text{and} \quad aa_{n-1} + ba_{n-2} &= a(c_1{\lambda_1}^{n-1} + c_2{\lambda_2}^{n-1}) + b(c_1{\lambda_1}^{n-2} + c_2{\lambda_2}^{n-2}) \\ &= c_1(a{\lambda_1}^{n-1} + b{\lambda_1}^{n-2}) + c_2(a{\lambda_2}^{n-1} + b{\lambda_2}^{n-2}) \\ &= c_1{\lambda_1}^{n-2}(a\lambda_1 + b) + c_2{\lambda_2}^{n-2}(a\lambda_2 + b) \\ &= c_1{\lambda_1}^{n-2}({\lambda_1}^2) + c_2{\lambda_2}^{n-2}({\lambda_2}^2) \qquad \{\text{using } (*)\} \\ &= c_1{\lambda_1}^n + c_2{\lambda_2}^n \\ &= a_n, \quad \text{as required.} \end{aligned}$$

Case 2: Let $a_n = (c_1 + nc_2)\lambda^n$, $n \in \mathbb{N}$, where c_1, c_2 are constants and λ is a repeated root of the characteristic equation $x^2 - ax - b = 0$.

$$\therefore \quad \lambda^2 = a\lambda + b \quad .... \text{ (1)}$$

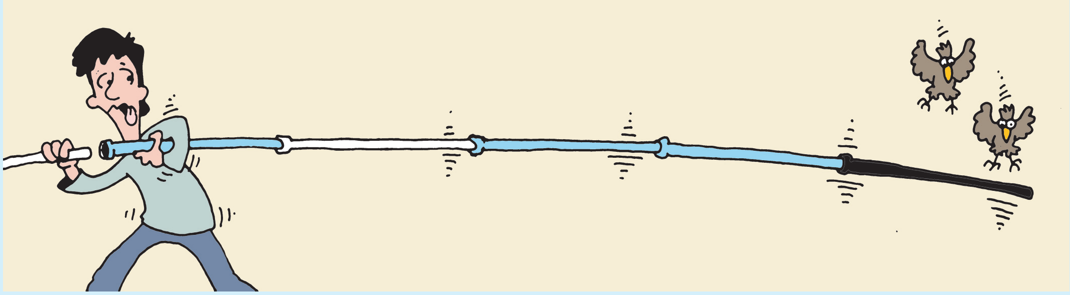
$$\begin{aligned} \text{and} \quad (x-\lambda)^2 &= x^2 - 2\lambda x + \lambda^2 \\ &= x^2 - ax - b \end{aligned}$$

$$\text{so that} \quad \lambda^2 = -b \quad \text{and} \quad \lambda = \frac{a}{2} \quad .... \text{ (2)}$$

$$\begin{aligned} \text{Consider} \quad aa_{n-1} + ba_{n-2} &= a(c_1 + (n-1)c_2)\lambda^{n-1} + b(c_1 + (n-2)c_2)\lambda^{n-2} \\ &= c_1(a\lambda^{n-1} + b\lambda^{n-2}) + c_2(a(n-1)\lambda^{n-1} + b(n-2)\lambda^{n-2}) \\ &= c_1\lambda^{n-2}(a\lambda + b) + c_2\lambda^{n-2}(a(n-1)\lambda + b(n-2)) \\ &= c_1\lambda^{n-2}(\lambda^2) + c_2\lambda^{n-2}(n(a\lambda + b) - (a\lambda + 2b)) && \{\text{using (1)}\} \\ &= c_1\lambda^n + c_2\lambda^{n-2}(n\lambda^2 - (\lambda^2 + b)) && \{\text{using (1)}\} \\ &= c_1\lambda^n + nc_2\lambda^n && \{\text{using (2)}\} \\ &= (c_1 + nc_2)\lambda^n \\ &= a_n, \quad \text{as required} \end{aligned}$$

Example 13

Long straight pipes are constructed from 1 m long sections connected end to end. The sections of pipe are coloured blue, white, or black depending on the material used to construct them. Any two sections of pipe can be joined together except no two white pipe sections can be joined.



a How many different constructions of pipe can be made with length:

i 0 metres **ii** 1 metre?

b Find the recurrence relation for the number a_n of different pipes of length n metres, $n \in \mathbb{N}$, $n \geqslant 2$.

c Hence find the first seven terms of the corresponding sequence.

d Verify the value of a_2 by considering the different possible pipes of length 2 metres.

e How many possible pipes of length 20 m are there?

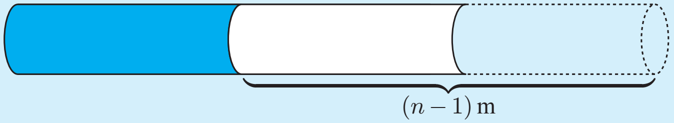
a **i** The empty set is unique, so there is only 1 construction.

ii 3; A blue, white, or black section of pipe can be used, so there are 3 different constructions.

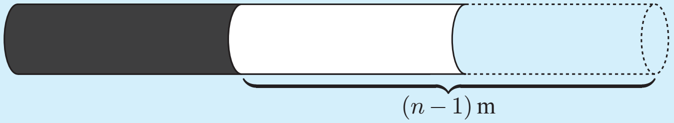
b From **a**, $a_0 = 1$, $a_1 = 3$.

For $n \geqslant 2$, we note that either the first pipe section is white, or it is not white.

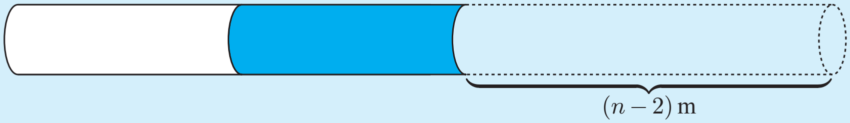
Case 1: If the first pipe section is *not* white, then it is blue or black, and the remaining length of pipe can be constructed in a_{n-1} ways.



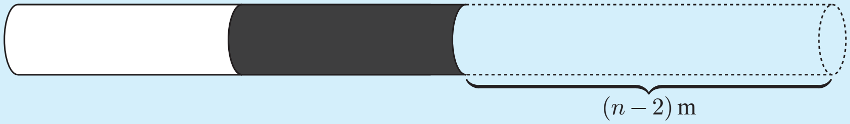
or



Case 2: If the first section of pipe is white, then the second section of pipe must be blue or black, and the remaining $n-2$ metres of pipe can be constructed in a_{n-2} ways.



or



The recurrence relation is $a_0 = 1,\ a_1 = 3,\ a_n = 2a_{n-1} + 2a_{n-2},\ n \geqslant 2.$

c $a_0 = 1$

$a_1 = 3$

$a_2 = 2 \times 1 + 2 \times 3 = 8$

$a_3 = 2 \times 3 + 2 \times 8 = 22$

$a_4 = 2 \times 8 + 2 \times 22 = 60$

$a_5 = 2 \times 22 + 2 \times 60 = 168$

$a_6 = 2 \times 60 + 2 \times 168 = 456$

d For a pipe of length 2 metres, each of the two sections can be blue, white, or black (3 options) except we cannot have white and white together.

$$\therefore \quad a_2 = 3 \times 3 - 1 = 8$$

3 choices for the first section.

3 choices for the second section.

remove the possibility of white - white.

e This is a second-degree linear homogeneous recurrence relation with constant coefficients.

$$a_n - 2a_{n-1} - 2a_{n-2} = 0$$

$\therefore$ the characteristic equation is $\lambda^2 - 2\lambda - 2 = 0$

$$\text{with roots} \quad \lambda = \frac{2 \pm \sqrt{4+8}}{2}$$

$$= \frac{2 \pm 2\sqrt{3}}{2}$$

$$= 1 \pm \sqrt{3}, \quad \text{distinct real roots.}$$

$\therefore$ the general solution is $a_n = c_1(1+\sqrt{3})^n + c_2(1-\sqrt{3})^n,\ n \in \mathbb{N}.$

Using the initial conditions:

$$a_0 = 1 \qquad\qquad a_1 = 3$$

$$\therefore \quad c_1(1+\sqrt{3})^0 + c_2(1-\sqrt{3})^0 = 1 \qquad \therefore \quad c_1(1+\sqrt{3})^1 + c_2(1-\sqrt{3})^1 = 3$$

$$\therefore \quad c_1 + c_2 = 1 \quad .... \text{ (1)} \qquad \therefore \quad c_1(1+\sqrt{3}) + c_2(1-\sqrt{3}) = 3$$

$$\therefore \quad c_1(1+\sqrt{3}) + (1-c_1)(1-\sqrt{3}) = 3 \qquad \{\text{using (1)}\}$$

$$\therefore \quad 2\sqrt{3}c_1 = 2+\sqrt{3}$$

$$\therefore \quad c_1 = \frac{2+\sqrt{3}}{2\sqrt{3}} \times \frac{\sqrt{3}}{\sqrt{3}}$$

$$\therefore \quad c_1 = \frac{3+2\sqrt{3}}{6}$$

$$\therefore \quad c_1 = \tfrac{1}{2} + \tfrac{1}{\sqrt{3}}$$

$$\therefore \quad c_2 = \tfrac{1}{2} - \tfrac{1}{\sqrt{3}} \qquad \{\text{using (1)}\}$$

$\therefore$ the general solution is $a_n = \left(\frac{1}{2}+\frac{1}{\sqrt{3}}\right)(1+\sqrt{3})^n + \left(\frac{1}{2}-\frac{1}{\sqrt{3}}\right)(1-\sqrt{3})^n, \ n \in \mathbb{N}$.

Hence $a_{20} = 578\,272\,256$.

Notice in the above Example that since the initial values are integers, the relation $a_n = 2a_{n-1} + 2a_{n-2}$ will always result in an integer.

This is not necessarily obvious from the closed form solution!

Example 14

Solve the recurrence relation $a_{n+2} = 6a_{n+1} - 9a_n, \ n \geqslant 0$ with initial conditions $a_0 = 2$, $a_1 = 2$. Hence find a_{10}.

This is a second-degree linear homogeneous recurrence relation with constant coefficients.

$$a_{n+2} - 6a_{n+1} + 9a_n = 0$$

$\therefore$ the characteristic equation is $\lambda^2 - 6\lambda + 9 = 0$

$$\therefore \quad (\lambda-3)^2 = 0$$

$$\therefore \quad \lambda = 3 \quad \text{is a repeated root.}$$

$\therefore$ the general solution is $a_n = (c_1 + nc_2)3^n, \ n \in \mathbb{N}$.

Using the initial conditions:

$$a_0 = 2 \qquad\qquad a_1 = 2$$

$$\therefore \quad (c_1 + 0 \times c_2) \times 3^0 = 2 \qquad \therefore \quad (c_1 + 1 \times c_2) \times 3^1 = 2$$

$$\therefore \quad c_1 = 2 \qquad \therefore \quad (2+c_2) \times 3 = 2$$

$$\therefore \quad 3c_2 = -4$$

$$\therefore \quad c_2 = -\tfrac{4}{3}$$

$\therefore$ the general solution is $a_n = (2 - \frac{4}{3}n)3^n, \ n \in \mathbb{N}$.

Hence $a_{10} = (2 - \frac{40}{3})3^{10} = -669\,222$.

Example 15

Solve the recurrence relation $x_n + 2x_{n-1} + 5x_{n-2} = 0$, $n \geqslant 2$ with initial conditions $x_0 = 2$, $x_1 = -2$. Hence find the closed form solution.

This is a second-degree linear homogeneous recurrence relation with constant coefficients.

The characteristic equation is $\lambda^2 + 2\lambda + 5 = 0$

$$\therefore \quad \lambda = \frac{-2 \pm \sqrt{4-20}}{2}$$

$$\therefore \quad \lambda = -1 \pm 2i, \quad \text{complex conjugate roots.}$$

$\therefore$ the general solution is $x_n = c_1(-1+2i)^n + c_2(-1-2i)^n$, $n \in \mathbb{N}$.

Using initial conditions:

$$x_0 = 2$$
$$\therefore \quad c_1 + c_2 = 2 \quad .... \ (1)$$

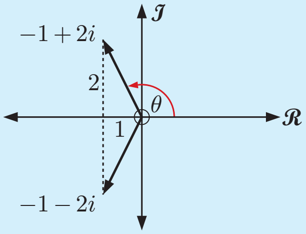
$$x_1 = -2$$
$$\therefore \quad c_1(-1+2i) + c_2(-1-2i) = -2$$
$$\therefore \quad c_1(-1+2i) + (2-c_1)(-1-2i) = -2$$
$$\therefore \quad c_1(-1+2i+1+2i) - 2 - 4i = -2$$
$$\therefore \quad 4ic_1 = 4i$$

$\therefore \quad c_1 = 1, \ \ c_2 = 1.$

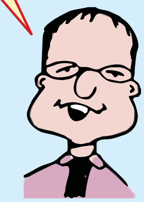
$\therefore \quad x_n = (-1+2i)^n + (-1-2i)^n, \ \ n \in \mathbb{N}$

We can also write the solution using polar form.

In this case $r = \sqrt{(-1)^2 + 2^2} = \sqrt{5}$
and $\theta = \pi - \arctan(2)$



If you have not yet studied polar form, leaving the solution as $x_n = (-1+2i)^n + (-1-2i)^n$, $n \in \mathbb{N}$ is sufficient.



$$x_n = (\sqrt{5})^n(\text{cis}\, n\theta + \text{cis}\,(-n\theta))$$

$\therefore \quad x_n = 2(\sqrt{5})^n \cos(n\theta), \ \ \theta = \pi - \arctan(2), \ \ n \in \mathbb{N}.$

EXERCISE 1B.4

1 Find the closed form solution for each recurrence relation:

a $a_n = a_{n-1} + 12a_{n-2}$, $n \geqslant 2$ with $a_0 = 12$, $a_1 = 24$

b $a_n - 3a_{n-1} + 2a_{n-2} = 0$, $n \geqslant 2$ with $a_0 = 2$, $a_1 = 3$

c $x_{n+2} - x_{n+1} - 2x_n = 0$, $n \in \mathbb{N}$ with $x_0 = 1$, $x_1 = 1$

d $a_n - a_{n-1} - 2a_{n-2} = 0$, $n \geqslant 2$ with $a_0 = 7$, $a_1 = 11$

e $a_n = 5a_{n-1} - 6a_{n-2}$, $n \geqslant 2$ with $a_0 = 3$, $a_1 = 5$

2 Solve the recurrence relation $a_n = a_{n-1} + a_{n-2}$, $n \geqslant 1$ with $a_0 = 0$, $a_1 = 1$ to find the closed form solution for the Fibonacci sequence.

3 Find the following recurrence relations:

- **a** $a_n = 2a_{n-1} - a_{n-2},\ \ n \geqslant 2$ with $a_0 = 2,\ a_1 = 2$
- **b** $a_n - 10a_{n-1} + 25a_{n-2} = 0,\ \ n \geqslant 2$ with $a_0 = 7,\ a_1 = 4$
- **c** $a_{n+2} + 4a_{n+1} + 4a_n = 0,\ \ n \in \mathbb{N}$ with $a_0 = 2,\ a_1 = -2$
- **d** $x_{n+2} + 8x_{n+1} + 16x_n = 0,\ \ n \in \mathbb{N}$ with $x_0 = 2,\ x_1 = 0$
- **e** $x_{n+2} - 2x_{n+1} + 2x_n = 0,\ \ n \in \mathbb{N}$ with $x_0 = 2,\ x_1 = 2$
- **f** $a_{n+2} - 2a_{n+1} + 5a_n = 0,\ \ n \in \mathbb{N}$ with $a_0 = 4,\ a_1 = 4$

4 Let $a_n = aa_{n-1} + ba_{n-2},\ \ n \geqslant 2,\ \ a_0,\ a_1$, be a second-degree linear homogeneous recurrence relation with constant coefficients, where $a_0,\ a_1,\ a,\ b$ are all *integer* constants.

Suppose the recurrence relation has solution $a_n = c_1\lambda_1^n + c_2\lambda_2^n$ where $\lambda_1,\ \lambda_2 = x \pm iy$ are conjugate complex numbers, and $c_1,\ c_2$ are constants.

Prove that $c_1 = c_2 = \dfrac{a_0}{2}$.

5 Solve the following recurrence relations:

- **a** $a_n = -2a_{n-1} - 2a_{n-2},\ \ n \geqslant 2$ with $a_0 = 2,\ a_1 = -2$
- **b** $a_n + a_{n-1} + a_{n-2} = 0,\ \ n \geqslant 2$ with $a_0 = 4,\ a_1 = -2$
- **c** $u_{n+2} + 4u_{n+1} + 5u_n = 0,\ \ n \in \mathbb{N}$ with $u_0 = 4,\ u_1 = -8$
- **d** $a_n = 4a_{n-1} - 5a_{n-2},\ \ n \geqslant 2$ with $a_0 = 6,\ a_1 = 12$

6 A plumber has 3 different types of pipe sections. The red and blue types have length two units each, and the white type has length 1 unit. The sections of pipe are joined end to end to create one long pipe. Find and solve a recurrence relation for the number of different pipes of length n units.

7 Coloured blocks are lined up end to end to form one long line of blocks. There are three types of blocks. There are red and blue blocks of length 1 unit, and green blocks of length 2 units.

Find and solve a recurrence relation for the number of different lines of blocks of length n units.

8 A sequence of 0s, 1s, and 2s, is called a **ternary string**. The number of digits in the sequence is the *length* of the string.

Find and solve a recurrence relation for the number of ternary strings of length n with no consecutive 0s.

9 A multi-trip travel card worth \$$n$ can be purchased from a machine which accepts \$1 and \$2 coins only. The coins are deposited in the machine one after the other, creating a sequence of \$1 and \$2 coins.

Find and solve a recurrence relation for the number of ways to purchase an \$$n$ travel card.

C DIVISIBILITY, PRIME NUMBERS, AND THE DIVISION ALGORITHM

In previous studies of the positive integers, we have found that prime numbers are the essential building blocks of the factors of an integer. The study of divisibility, prime numbers, and the factors of an integer, are all intimately related.

INVESTIGATION 4 HOW MANY PRIMES ARE THERE?

Do you think that there are infinitely many prime numbers, or do you think that the list terminates with a highest prime number?

In this Investigation you will attempt to prove by contradiction the statement "There are an infinite number of primes".

What to do:

1 What is the negation (or opposite) of the statement: "There are an infinite number of primes"? This will be the statement we try to contradict.

2 Suppose there is a largest prime P.
Now consider the number $N = P! + 1$.

a Do you know whether N is prime or composite?
Hint: Consider $P = 3$ and $P = 5$.

b If N is prime, what does this say about your assumption about P?

c Suppose N is composite.

i Consider $N = 19! + 1$. Explain why N is not divisible by any of the integers 2, 3, 4, ..., 19.

ii Consider $N = P! + 1$. Explain why N is not divisible by any of the integers 2, 3, 4, ..., P.

iii If N is not divisible by any integer $\leqslant P$, but N is composite, what does this say about any prime factor k of N?

iv Complete the proof by contradiction, that there are an infinite number of primes.

3 The proof you obtained in **2** is a variant on **Euclid's proof of the infinitude of primes**, written around 300 B.C. Research Euclid's proof and see how it varies from the one in **2**.

Identifying primes and composites is an important task for digital security. However, it is a non-trivial task to identify very large primes quickly, even with very powerful computers. To understand better how primes and composites can be identified, we now look at the formal rules governing divisibility.

If d and n are integers, $d \neq 0$, then d **divides** $n \Leftrightarrow$ there exists $k \in \mathbb{Z}$ such that $n = dk$.

We use the notation $d \mid n$ to read *d divides n*
or *d is a divisor of n*
or *d is a factor of n*
or *n is a multiple of d.*

For example, we write $3 \mid 12$ to indicate that 3 divides 12.

We write $5 \nmid 12$ to indicate that 5 *does not divide* 12.

DIVISIBILITY PROPERTIES

- $n \mid n,\ n \neq 0$ (every non-zero integer divides itself)
- $d \mid n$ and $n \mid m \Rightarrow d \mid m$ (**transitivity**)
- $d \mid n$ and $d \mid m \Rightarrow d \mid (an + bm)$ for all $a, b \in \mathbb{Z}$ (**linearity**)
- $d \mid n \Rightarrow ad \mid an$ (**multiplicative**)
- $ad \mid an \Rightarrow d \mid n$ if $a \neq 0$ (**cancellation**)
- $1 \mid n$ (1 divides every integer)
- $n \mid 1 \Rightarrow n = \pm 1$
- $d \mid 0$ for every non-zero $d \in \mathbb{Z}$
- If $d, n \in \mathbb{Z}^+$ and $d \mid n$, then $d \leqslant n$.

The linearity property says that if d divides both n and m, then d divides **all** linear combinations of n and m. In particular, $d \mid (n+m)$ and $d \mid (n-m)$.

Example 16

Prove the transitivity property: If $d \mid n$ and $n \mid m$ then $d \mid m$.

Implicitly, we have that $d, n \neq 0$.

$d \mid n \Rightarrow$ there exists k_1 such that $n = k_1 d,\ k_1 \in \mathbb{Z}$

$n \mid m \Rightarrow$ there exists k_2 such that $m = k_2 n,\ k_2 \in \mathbb{Z}$

$\therefore\ m = k_2 n = k_2(k_1 d) = k_1 k_2 d$ where $k_1 k_2 \in \mathbb{Z}$

$\therefore\ d \mid m$

Example 17

Prove that $n \mid 1 \Rightarrow n = \pm 1$.

$n \mid 1 \Rightarrow$ there exists k such that $1 = kn,\ k \in \mathbb{Z}$

So, we have to solve $kn = 1$ where k and n are integers.

The only solutions are $k = 1,\ n = 1$ or $k = -1,\ n = -1$

$\therefore\ n = \pm 1$

EXERCISE 1C.1

1 Prove the multiplicative property: $d \mid n \Rightarrow ad \mid an$ where $a, d, n \in \mathbb{Z}$ and $d, a \neq 0$.

2 Prove the linearity property: $d \mid n$ and $d \mid m \Rightarrow d \mid (an + bm)$ for all $a, b \in \mathbb{Z}$.

3 Prove that if $d, n \in \mathbb{Z}^+$ and $d \mid n$, then $d \leqslant n$.

4 Prove that if $a \in \mathbb{Z}$, then the only positive divisor of both consecutive integers a and $a+1$, is 1.

5 Prove that there do not exist integers m and n such that:

a $14m + 20n = 101$ **b** $14m + 21n = 100$

6 Suppose $a, b, c \in \mathbb{Z}$, $a \neq 0$. Prove that $a \mid b$ and $a \mid c \Rightarrow a \mid (b \pm c)$.

7 Suppose $a, b, c, d \in \mathbb{Z}$ where $a, c \neq 0$. Prove that $a \mid b$ and $c \mid d \Rightarrow ac \mid bd$.

8 Given $p, q \in \mathbb{Z}$ such that $p \mid q$, prove that $p^n \mid q^n$ where $n \in \mathbb{Z}$.

THE DIVISION ALGORITHM

The **Division Algorithm** extends our notion of divisibility to the case where **remainders** are obtained.

> For any $a, b \in \mathbb{Z}$ with $b > 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leqslant r < b$.
>
> q is the greatest integer such that $q \leqslant \frac{a}{b}$ and is called the **quotient**.
>
> r is called the **remainder**, a is the **dividend**, and b is the **divisor**.

For example: For the integers 27 and 4, $27 = 6 \times 4 + 3$
The dividend is 27, the divisor is 4, the quotient is 6, and the remainder is 3.

Example 18

Find the quotient and remainder for:

a $a = 133$, $b = 21$ **b** $a = -50$, $b = 8$ **c** $a = 1\,781\,293$, $b = 1481$

a $\frac{a}{b} = 6.333....$

$\therefore\ q = 6$

Now $r = a - bq$

$\therefore\ r = 133 - 21 \times 6$

$\therefore\ r = 7$

b $\frac{a}{b} = -6.25$

$\therefore\ q = -7$

Now $r = a - bq$

$\therefore\ r = -50 - 8(-7)$

$\therefore\ r = 6$

c $\frac{a}{b} = 1202.76....$

$\therefore\ q = 1202$

Now $r = a - bq$

$\therefore\ r = 1\,781\,293 - 1481 \times 1202$

$\therefore\ r = 1131$

If the divisor $b = 5$, then $a = 5q + r$ where $r = 0, 1, 2, 3,$ or 4. There are no other possible remainders on division by 5. The different values of r partition the set of integers into five disjoint subsets with membership of a given subset being dependent solely on the value of the remainder on division by 5.

Thus each integer can be written in the form $5k$, $5k+1$, $5k+2$, $5k+3$, or $5k+4$ for some $k \in \mathbb{Z}$, depending on its remainder on division by 5.

For example, 35 and 240 belong to the set {integers divisible by 5}
36 and 241 belong to the set {integers with remainder 1 on division by 5}.

The Division Algorithm states that if results about divisibility by 5 apply to "2" then they apply to all numbers with remainder 2 on division by 5, which are the integers with the form $5k + 2$ for some $k \in \mathbb{Z}$.

EXERCISE 1C.2

1 Show that:

a $3 \mid 66$ **b** $7 \mid 385$ **c** $654 \mid 0$

2 Find the quotient and remainder in the division process with divisor 17 and dividend:

a 100 **b** 289 **c** -44 **d** -100

3 What can be deduced about non-zero integers a and b if $a \nmid b$ and $b \nmid a$?

4 **a** Is it possible to find prime integers p, q, and r such that $p \mid qr$ but $p \nmid q$ and $p \nmid r$?

b When is it possible to find integers p, q, and r such that $p \mid qr$ but $p \nmid q$ and $p \nmid r$?

5 Prove that if the product of k integers is odd, then all of the individual integers are themselves odd.

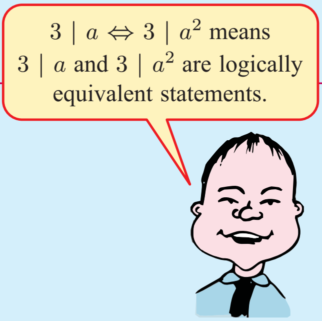
6 **a** Prove that the square of an integer can be written in the form $3k$ or $3k+1$ for some $k \in \mathbb{Z}$.

b Prove that the square of an integer can be written in the form $4q$ or $4q+1$ for some $q \in \mathbb{Z}$.

c Deduce that 1 234 567 is not a perfect square.

Example 19

Prove that if $a \in \mathbb{Z}$, then $3 \mid a \;\Leftrightarrow\; 3 \mid a^2$.


$3 \mid a \Leftrightarrow 3 \mid a^2$ means
$3 \mid a$ and $3 \mid a^2$ are logically
equivalent statements.

Proof:

$(\Rightarrow)$ If $3 \mid a$, then $a = 3q$ for some $q \in \mathbb{Z}$

$\Rightarrow\; a^2 = 9q^2$

$\Rightarrow\; a^2 = 3(3q^2)$ where $3q^2 \in \mathbb{Z}$

$\Rightarrow\; 3 \mid a^2$

$(\Leftarrow)$ Instead of showing $3 \mid a^2 \Rightarrow 3 \mid a$, we will prove the contrapositive $3 \nmid a \Rightarrow 3 \nmid a^2$.

Now if $3 \nmid a$,

then $a = 3q+1$ or $a = 3q+2$

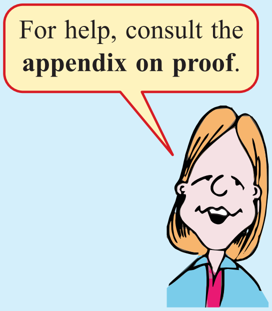
$\Rightarrow\; a^2 = 9q^2+6q+1$ or $a^2 = 9q^2+12q+4$

$\Rightarrow\; a^2 = 3(3q^2+2q)+1$ or $a^2 = 3(3q^2+4q+1)+1$

$\Rightarrow\; 3 \nmid a^2$ {since in each case the remainder is 1}

Hence $3 \nmid a \Rightarrow 3 \nmid a^2$, and therefore

$3 \mid a^2 \Rightarrow 3 \mid a$ {contrapositive}.



7 Prove that if $a \in \mathbb{Z}$ then:

a $5 \mid a \;\Leftrightarrow\; 5 \mid a^2$ **b** $3 \mid a^2 \;\Leftrightarrow\; 9 \mid a^2$

8 **a** Prove that $n = 2 \;\Rightarrow\; (n+3)(n-2) = 0$

b Is the converse in **a** true?

c There are several different ways to read the statement $p \Rightarrow q$. These are:

- "If p then q"
- "q if p"
- "p is sufficient for q"
- "q is necessary for p"

Using the above, which of the following are true and which are not?

i $n = 2$ if $n^2 + n - 6 = 0$

ii $n = 2$ is sufficient for $n^2 + n - 6 = 0$

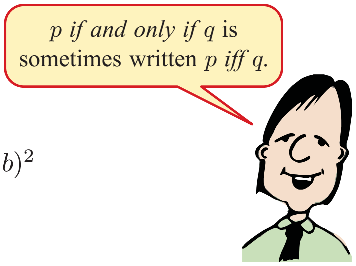
iii $n = 2$ is necessary for $n^2 + n - 6 = 0$

iv $a < b$ is sufficient for $4ab < (a+b)^2$

v $a < b$ is necessary and sufficient for $4ab < (a+b)^2$

vi $a < b$ if and only if $4ab < (a+b)^2$

vii $a < b$ is equivalent to $4ab < (a+b)^2$



9 **a** Prove that any integer of the form $8p + 7$, $p \in \mathbb{Z}$, is also of the form $4q + 3$, $q \in \mathbb{Z}$.

b Provide a counter example to show that the converse of **a** is not true.

10 Prove that:

a the cube of an integer takes either the form $9k$ or $9k \pm 1$

b the fourth power of an integer takes either the form $5k$ or $5k + 1$.

11 Prove that an integer of the form $3k^2 - 1$, $k \in \mathbb{Z}$, is never a square.
Hint: Consider the contrapositive of this statement.

12 Suppose $n \geqslant 1$. Prove, by considering exhaustive cases for the form of n, that $\dfrac{n(n+1)(2n+1)}{6} \in \mathbb{Z}$. Find another, alternative proof.

13 The nth repunit is the integer consisting of n "1"s. Prove that no repunit, except 1, can be a perfect square.
Hint: If necessary, see **Exercise 1A.1** question **3**.

14 Prove, by using exhaustive cases, that if an integer is both a perfect square and a perfect cube, then it will take one of the two forms $7k$ or $7k + 1$.

15 Suppose $n \in \mathbb{Z}^+$.

a Prove that $7n^3 + 5n$ is even by using the Division Algorithm and considering cases.

b Prove that $n(7n^2 + 5)$ is of the form $3k$, where $k \in \mathbb{Z}^+$.

c Hence, prove that the integer $n(7n^2 + 5)$ is of the form $6k$.

d Prove the result in **c** directly, by considering six exhaustive cases for the form of n.

16 Given $a \in \mathbb{Z}$, prove that $3 \mid (a^3 - a)$.

17 **a** Show that the product of any two integers of the form $4k + 1$ also has this form.

b Show that the product of any two integers of the form $4k + 3$ has the form $4p + 1$.

c What do these results tell you about the square of any odd number?

d Show that the fourth power of any odd integer is of the form $8k + 1$, $k \in \mathbb{Z}^+$.

18 **a** Prove by induction that the product of any three consecutive positive integers is divisible by 6.

b Prove this result for all integers using the Division Algorithm.

19 **a** Prove by induction that $5 \mid (n^5 - n)$ for all $n \in \mathbb{Z}^+$.

b Prove this result using the Division Algorithm.

20 Prove that the sum of the cubes of any three consecutive integers is divisible by 9.

INTEGER REPRESENTATION IN VARIOUS BASES

Repeated use of the Division Algorithm, and the uniqueness of its representation of integers, is the basis of our decimal number system.

We express numbers in the **decimal** system as a sum of powers of 10. We call 10 the **base** of our number system.

For example, $34\,765 = 3 \times 10^4 + 4 \times 10^3 + 7 \times 10^2 + 6 \times 10^1 + 5 \times 10^0$

The coefficients of the powers of 10 in such an expansion come from the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ which we denote $\mathbb{Z}_{10}$.

If a base number is not given, it is assumed to be base 10.

For example, 347, $(347)_{10}$, and 347_{10} all refer to the same base 10 integer.

We use 10 as the base probably because we have 10 fingers for counting! However, we could use any other positive integer as our base, since the Division Algorithm ensures that the representation of each integer is unique in that base.

Integers written in **binary** (base 2) are very important in computer science.

Integers are written in binary using powers of 2, and digits from the set $\mathbb{Z}_2 = \{0, 1\}$ as their coefficients.

For example, $101\,101_2 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$.

Example 20

Convert:

a $101\,101_2$ to a base 10 integer

b the base 10 integer 347 into binary.

a
$$\begin{aligned} 101\,101_2 &= 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^0 \\ &= 32 + 8 + 4 + 1 \\ &= 45_{10} \end{aligned}$$

b We need to write 347 in the form $a_k 2^k + a_{k-1} 2^{k-1} + ... + a_2 2^2 + a_1 2^1 + a_0$ where each $a_i \in \mathbb{Z}_2$ and $\mathbb{Z}_2 = \{0, 1\}$.

We obtain the coefficients a_i using repeated division by 2 and recording the remainders, in reverse.

2	347	r	
2	173	1	$347 = 2 \times 173 + 1$
2	86	1	$173 = 2 \times 86 + 1$
2	43	0	$86 = 2 \times 43 + 0$
2	21	1	$43 = 2 \times 21 + 1$
2	10	1	$21 = 2 \times 10 + 1$
2	5	0	$10 = 2 \times 5 + 0$
2	2	1	$5 = 2 \times 2 + 1$
	1	0	$2 = 2 \times 1 + 0$

So, $347_{10} = 101\,011\,011_2$

EXERCISE 1C.3

1 Convert $110\,101\,011_2$ from binary to a decimal (base 10) integer.

2 Convert $21\,012\,201_3$ from ternary to decimal notation.

3 Convert:

a 347 into base 3 b 1234 into base 8 c 5728 into base 7.

4 Write 87 532 in base 5.

5 Convert $1\,001\,111\,101_2$ from binary into:

a base 10 b base 4 c base 8.

6 Convert $201\,021\,102_3$ from ternary into:

a base 10 b base 9.

7 Convert $2\,122\,122\,102_3$ from ternary into base 9.

8 Detail a method of converting a given integer from base k into base k^2.

9 Detail a method of converting a given integer from base k^2 into base k.

10 Convert $313\,123\,012_4$ into binary.

11 Convert $6\,326\,452\,378_9$ into ternary.

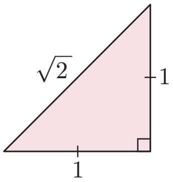
12 Convert $56\,352\,743_8$ into binary.

13 By repeated use of the Division Algorithm, find the infinite decimal representation of the rational number $\frac{5}{7}$.

Hint: Suppose $\frac{5}{7} = a_1 \times 10^{-1} + a_2 \times 10^{-2} + ...$ where each $a_i \in \mathbb{Z}_{10}$.

THE EXISTENCE OF IRRATIONALS

The first real number found to be irrational was probably $\sqrt{2}$. Its existence as a real number is readily observed from a right-angled triangle with perpendicular sides of length 1 unit and applying Pythagoras' theorem:



In this section we consider proofs for whether a number is rational or irrational.

Since each real number must be one or the other, an effective method for proving irrationality is a **proof by contradiction**.

For more information consult the **appendix on proofs**.

Example 21

a Suppose $p \in \mathbb{Z}^+$. Prove that if p^2 has 3 as a factor, then p has 3 as a factor.

b Prove that the real number $\sqrt{3}$ is irrational.

a Suppose $p \in \mathbb{Z}^+$. On division by 3, p has remainder 0, 1, or 2.

$\therefore$ $p = 3t$, $3t+1$, or $3t+2$ for some $t \in \mathbb{Z}$.

$\therefore$ $p^2 = 9t^2$, $9t^2+6t+1$, or $9t^2+12t+4$

$\therefore$ $p^2 = 3(3t^2)$, $3(3t^2+2t)+1$, or $3(3t^2+4t+1)+1$

Only the form $p^2 = 3(3t^2)$ has 3 as a factor.

$\therefore$ if p^2 has 3 as a factor then p has 3 as a factor.

b Suppose $\sqrt{3}$ is rational.

$\therefore$ $\sqrt{3} = \dfrac{p}{q}$ for some $p, q \in \mathbb{Z}^+$, $q \neq 0$ such that p and q have no common factors besides 1.

$\therefore$ $p = q\sqrt{3}$

$\therefore$ $p^2 = 3q^2$

$\therefore$ p^2 has 3 as a factor

$\therefore$ p has 3 as a factor {from **a**}

$\therefore$ $p = 3t$ for some $t \in \mathbb{Z}$

$\therefore$ since $p^2 = 3q^2$,

$(3t)^2 = 3q^2$

$\therefore$ $9t^2 = 3q^2$

$\therefore$ $3t^2 = q^2$

$\therefore$ q^2 has 3 as a factor

$\therefore$ q has 3 as a factor {from **a**}

$\therefore$ p and q have 3 as a common factor, which is a contradiction.

Therefore $\sqrt{3}$ is irrational.

EXERCISE 1C.4

1. Prove that $\sqrt{2}$ is irrational.
2. Prove that $\sqrt{5}$ is irrational.
3. Attempt to prove that $\sqrt{4}$ is irrational using the same argument as in **Example 21**. At which step does it fail?
4. Prove that $2^{\frac{1}{4}}$ is irrational.

D GCD, LCM, AND THE EUCLIDEAN ALGORITHM

GREATEST COMMON DIVISOR (GCD)

We know that $3 \mid 6$ and $3 \mid 15$, and no greater number has this property of dividing both 6 and 15. We say that the greatest common divisor of 6 and 15 is 3, and write $\gcd(6, 15) = 3$.

The **greatest common divisor** (or **highest common factor**) of non-negative integers a and b, is written $\gcd(a, b)$ (or simply (a, b) in some texts).

$d = \gcd(a, b) \Leftrightarrow$ (1) $d \mid a$ and $d \mid b$

(2) if $e \mid a$ and $e \mid b$ then $e \mid d$

For example: $\gcd(24, 36) = 12$, $\gcd(12, 0) = 12$, $\gcd(15, 28) = 1$

RELATIVELY PRIME INTEGERS

Integers a and b are called **relatively prime** (or **coprime**) if $\gcd(a, b) = 1$.

Theorem: If $d = \gcd(a, b)$ then (1) $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

(2) $\gcd(a, b) = \gcd(a + cb, b)$, $a, b, c \in \mathbb{Z}$

Proof:

(1) For $e \in \mathbb{Z}^+$, if $e \mid \left(\frac{a}{d}\right)$ and $e \mid \left(\frac{b}{d}\right)$ then there exist integers k and l such that $\frac{a}{d} = ke$ and $\frac{b}{d} = le$

$\Rightarrow$ $a = kde$ and $b = lde$

$\Rightarrow$ a and b have de as a common divisor.

But $d = \gcd(a, b)$ $\Rightarrow$ $de \leqslant d$ $\Rightarrow$ $e = 1$ $\Rightarrow$ $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

(2) Let e be a common divisor of a and b, so $e \mid a$ and $e \mid b$

$\Rightarrow$ $e \mid (a + cb)$ where $c \in \mathbb{Z}$ {linearity property of divisibility}

$\Rightarrow$ e is a common divisor of b and $a + cb$

$\Rightarrow$ $\gcd(a, b)$ is a common divisor of b and $a + cb$

$\Rightarrow$ $\gcd(a, b) \leqslant \gcd(a + cb, b)$ .... $(*)$

If f is a common divisor of b and $a + cb$

$\Rightarrow$ f is a common divisor of b and $(a + cb) - cb$ {linearity property of divisibility}

$\Rightarrow$ f is a common divisor of b and a

$\Rightarrow$ $\gcd(a + cb, b)$ is a common divisor of a and b

$\Rightarrow$ $\gcd(a + cb, b) \leqslant \gcd(a, b)$ .... $(**)$

From $(*)$ and $(**)$, $\gcd(a, b) = \gcd(a + cb, b)$.

Theorem:

For positive integers a and b, the $\gcd(a, b)$ is the least positive integer that is a linear combination of a and b.

In other words, if $d = \gcd(a, b)$ then $d = ma + nb$ where $m, n \in \mathbb{Z}$,

and if $k = pa + qb$, $p, q \in \mathbb{Z}$, then $k \geqslant d$.

Proof:

Let d be the least positive integer that is a linear combination of a and b.

We must now show that (1) $d \mid a$ and $d \mid b$

(2) $d = \gcd(a, b)$

(1) Since d is a linear combination of a and b, let $d = ma + nb$, $m, n \in \mathbb{Z}$.
Since $d > 0$, $a = dq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$. {Division Algorithm}

$$\begin{aligned} \therefore\quad r &= a - dq \\ &= a - q(ma + nb) \\ &= (1 - qm)a - qnb \end{aligned}$$

and so r is a linear combination of a and b.
However, we have defined d as the least positive linear combination of a and b.
$\therefore$ since $0 \leqslant r < d$, we can only conclude that $r = 0$.
Consequently $a = dq$, and hence $d \mid a$.
By similar argument, we also conclude that $d \mid b$.

(2) By the linearity property, if e is any common divisor of a and b, then $e \mid (ma + nb)$.
But $d = ma + nb$, so $e \mid d$.
Consequently, by definition, $d = \gcd(a, b)$.

Note that this is an *existence* proof. It tells us that the $\gcd(a, b)$ is a linear combination of a and b, but it does not tell us what the linear combination is. To calculate the $\gcd(a, b)$ as a linear combination of a and b, we need the Euclidean Algorithm, which we will study soon.

Corollary: For positive integers a and b, any linear combination of a and b is a multiple of $d = \gcd(a, b)$.

Proof:

From the above theorem, $d = ma + nb$ for some integers $m, n \in \mathbb{Z}$, and d is the least positive integer with this property.

Suppose $s = pa + qb$ where $p, q \in \mathbb{Z}$.

Case $s = 0$: $0 = 0 \times d$ is a multiple of d.

Case $s > 0$: If $s > 0$ then $s \geqslant d$ {d is the *least* positive linear combination of a and b}

$$\therefore\quad pa + qb \geqslant ma + nb$$

$$\therefore\quad (p - m)a + (q - n)b \geqslant 0$$

If $(p - m)a + (q - n)b \neq 0$, then this is a positive linear combination of a and b.

$\therefore$ since $d = ma + nb$ is the *least* such linear combination,

$$(p-m)a + (q-n)b \geqslant ma + nb$$
$$(p-2m)a + (q-2n)b \geqslant 0$$

Since p, q are finite, by repeating this argument we find that there exists $t \in \mathbb{Z}^+$ such that $(p-tm)a + (q-tn)b = 0$

$\therefore$ $p = tm$ and $q = tn$ {since a and b are positive}

$$\begin{aligned}\therefore \quad s &= (tm)a + (tn)b\\ &= t(ma+nb)\\ &= td\end{aligned}$$

$\therefore$ s is a multiple of d.

Case $s < 0$: In this case we consider $r = -s = (-p)a + (-q)b$.

Since $r > 0$, we repeat the above argument and obtain that r, and therefore s, is a multiple of $d = \gcd(a, b)$.

Corollary:

Consider positive integers a and b with $d = \gcd(a, b)$.

For any multiple rd of d, with $r \in \mathbb{Z}$, the equation $ax + by = rd$ has infinitely many integer solution pairs (x, y).

Proof: $d = ma + nb$ for some integers $m, n \in \mathbb{Z}$.

$$\begin{aligned}\therefore \quad rd &= rma + rnb\\ &= a(rm) + b(rn)\\ &= a\left(rm - \frac{tb}{d}\right) + b\left(rn + \frac{ta}{d}\right) \quad \text{where } t \text{ is any integer}\end{aligned}$$

$\therefore$ $rd = ax + by$ has infinitely many solution pairs (x, y) of the form

$$x = rm - t\,\frac{b}{d},$$
$$y = rn + t\,\frac{a}{d}.$$

These solutions are integers since $d = \gcd(a, b)$.

From the proof above, if $ax + by = s$ has a particular integer solution $x = x_0$, $y = y_0$, then all of its solutions can be written in the form

$$x = x_0 + t\left(\frac{b}{d}\right), \quad y = y_0 - t\left(\frac{a}{d}\right) \quad \text{where } d = \gcd(a, b) \text{ and } t \in \mathbb{Z}.$$

Example 22

Determine whether the following equations have integer solutions $x, y \in \mathbb{Z}$.

If an equation has integer solutions, state a solution pair by inspection, and hence write the form of *all* integer solutions.

a $24x + 36y = 12$ **b** $24x + 36y = 18$ **c** $24x + 36y = 48$

a Since $\gcd(24, 36) = 12$, there exist integers x, y such that $24x + 36y = 12$.
By inspection, a solution is $x_0 = -1$, $y_0 = 1$.
Since $\frac{24}{12} = 2$ and $\frac{36}{12} = 3$, the solutions have the form $x = -1 + 3t$, $y = 1 - 2t$ for any $t \in \mathbb{Z}$.

b Since $\gcd(24, 36) = 12$ and 18 is not a multiple of 12, there are no solutions for which x and y are both integers.

c Since $\gcd(24, 36) = 12$ and 48 is a multiple of 12, there exist integers x, y such that $24x + 36y = 48$.
By inspection, a solution is $x_0 = 2$, $y_0 = 0$.
Since $\frac{24}{12} = 2$ and $\frac{36}{12} = 3$, the solutions have the form $x = 2 + 3t$, $y = -2t$ for any $t \in \mathbb{Z}$.

Theorem:

For non-zero integers a and b, with $d = \gcd(a, b)$

a and b are relatively prime $\Leftrightarrow$ there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

Proof: $(\Rightarrow)$ a and b relatively prime
$\Rightarrow$ $\gcd(a, b) = 1$
$\Rightarrow$ there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$ {Theorem}

$(\Leftarrow)$ If $d = \gcd(a, b)$
$\Rightarrow$ $d \mid a$ and $d \mid b$
$\Rightarrow$ $d \mid ma + nb$ {divisibility property}
$\Rightarrow$ $d \mid 1$
$\Rightarrow$ $d = 1$
$\Rightarrow$ a and b are relatively prime.

Example 23

Prove that $\sqrt{2}$ is irrational.

Proof: (By contradiction)

Suppose that $\sqrt{2}$ is rational.

$\therefore$ $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{Z}^+$, $\gcd(p, q) = 1$

Since $\gcd(p, q) = 1$, there exist $r, s \in \mathbb{Z}^+$ such that $rp + sq = 1$

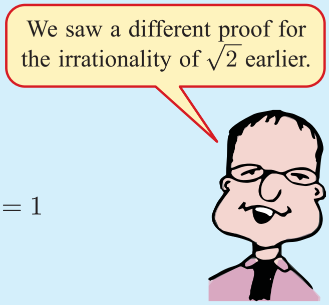
Hence, $\sqrt{2} = \sqrt{2}(rp + sq) = (\sqrt{2}p)r + (\sqrt{2}q)s$

$\therefore$ $\sqrt{2} = (\sqrt{2}\sqrt{2}q)r + (\sqrt{2}\,\frac{p}{\sqrt{2}})s$ {using $\sqrt{2} = \frac{p}{q}$}

$\therefore$ $\sqrt{2} = 2qr + ps$

$\therefore$ $\sqrt{2}$ is an integer {since $p, q, r, s \in \mathbb{Z}^+$}

This is a contradiction, so $\sqrt{2}$ must be irrational.


We saw a different proof for the irrationality of $\sqrt{2}$ earlier.

Corollary: If $a \mid c$ and $b \mid c$ with $\gcd(a, b) = 1$ then $ab \mid c$.

Proof: As $\gcd(a, b) = 1$, there exist integers m, n such that $ma + nb = 1$

$\therefore\ mac + nbc = c$

But $a \mid c$ and $b \mid c \Rightarrow c = ka$ and $c = lb$ for some integers k, l.

$\therefore\ ma(lb) + nb(ka) = c$

$\therefore\ ab(ml + nk) = c$

$\therefore\ ab \mid c$

Although it may seem trivial, this corollary is important in a practical way.

We know, for example, that $8 \mid 144$ and $9 \mid 144$ and $\gcd(8, 9) = 1$.

Hence $72 \mid 144$.

The result is not true for divisors which are not relatively prime.

For example, $8 \mid 144$ and $12 \mid 144$ but $\gcd(8, 12) = 4 \neq 1$. In this case $8 \times 12 \nmid 144$.

EUCLID'S LEMMA

If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof: As $\gcd(a, b) = 1$, there exist integers m, n such that $ma + nb = 1$

$\therefore\ mac + nbc = c$

But $a \mid bc \Rightarrow bc = ka$ for some integer k.

$\therefore\ mac + n(ka) = c$

$\therefore\ a(mc + nk) = c$

$\therefore\ a \mid c$

Note that if the condition $\gcd(a, b) = 1$ is not true, the Lemma in general fails.

For example, consider $a = 12$, $b = 9$ where $\gcd(12, 9) = 3 \neq 1$.

For $c = 8$, $12 \mid 9 \times 8$ but $12 \nmid 8$ so $a \nmid c$.

For $c = 24$, $12 \mid 9 \times 24$ but $12 \mid 24$ so $a \mid c$.

EXERCISE 1D.1

1 **a** Suppose $a, b, c, d \in \mathbb{Z}$. Prove that for $a \neq 0$:

i if $a \mid b$ then $a \mid bc$

ii if $a \mid b$ and $a \mid c$ then $a^2 \mid bc$

iii if $a \mid b$ and $c \mid d$ then $ac \mid bd$ $(c \neq 0)$

iv if $a \mid b$ then $a^n \mid b^n$.

b Is the converse of **a iv** true?

2 Suppose $k \in \mathbb{Z}$. Prove that one of k, $k + 2$, or $k + 4$ is divisible by 3.

3 Determine the truth or otherwise of the statement:

If $p \mid (q + r)$ then either $p \mid q$ or $p \mid r$.

4 Determine whether each of the following equations has integer solutions $x, y \in \mathbb{Z}$. If an equation has integer solutions, state a solution pair by inspection, and hence write the form of *all* integer solutions.

a $24x + 18y = 9$ **b** $2x + 3y = 67$ **c** $57x + 95y = 19$

d $1035x + 585y = 901$ **e** $45x - 81y = 108$

5 **a** Prove that:

i the product of any three consecutive integers is divisible by 3

ii the product of any three consecutive integers is divisible by 6

iii the product of any four consecutive integers is divisible by 8

iv the product of any four consecutive integers is divisible by 24.

b Is the product of any n consecutive integers divisible by $n!$?

6 Prove that $3 \mid k(k^2 + 8)$ for all $k \in \mathbb{Z}$.

7 Heta claims that "the product of four consecutive integers is one less than a square".

a Check Heta's statement by examining three examples.

b Prove or disprove Heta's claim.

8 **a** Prove that for $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, $\gcd(a, a + n) \mid n$.

b Hence, prove that for $a \in \mathbb{Z}$, $\gcd(a, a + 1) = 1$.

9 Use the linearity property to show that for $k \in \mathbb{Z}$,

a $\gcd(3k + 1, 13k + 4) = 1$ **b** $\gcd(5k + 2, 7k + 3) = 1$

10 **a** Given any non-zero integers a and b, prove that $\gcd(4a - 3b, 8a - 5b)$ divides b but not necessarily a.

b Hence, prove that $\gcd(4a + 3, 8a + 5) = 1$.

11 Prove that if $\gcd(a, b) = 1$ and $c \mid a$, then $\gcd(c, b) = 1$.

12 Suppose $\gcd(a, b) = 1$. Prove that $\gcd(a^2, b) = \gcd(a, b^2) = 1$, and hence that $\gcd(a^2, b^2) = 1$.

13 Prove, using a gcd theorem, that $\sqrt{3}$ is irrational.

14 **a** Using the identity $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + x^{k-3} + ... + x + 1)$ and by considering repunits, prove that if $d \mid n$ then $(2^d - 1) \mid (2^n - 1)$.

b Establish that $2^{35} - 1$ is divisible by both 31 and 127.

15 Show that for $k \in \mathbb{Z}^+$ the integers $3k + 2$ and $5k + 3$ are relatively prime.

16 Show that if k is an even positive integer then $5k + 3$ and $11k + 7$ are relatively prime.

17 Given $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, prove that $\gcd(a + b, a - b) = 1$ or 2.

THE EUCLIDEAN ALGORITHM

The Euclidean Algorithm is the most efficient (and ingenious) way of determining the greatest common divisor of two integers. It was detailed in Euclid's *Elements* and has been known in most of the world since antiquity. It is based on the Division Algorithm.

Lemma:

If $a = bq + r$ where a, b, and q are integers, then $\gcd(a, b) = \gcd(b, r)$.

Proof:

If $d \mid a$ and $d \mid b \Rightarrow d \mid (a - bq)$ {linearity property}
$\Rightarrow d \mid r$

Hence, any common divisor of a and b is also a common divisor of b and r.

Likewise, if $d \mid b$ and $d \mid r \Rightarrow d \mid (bq + r) \Rightarrow d \mid a$.

Hence, any common divisor of b and r is also a common divisor of a and b.

Since the common divisors of a and b are the same as the common divisors of b and r, it is clear that $\gcd(a, b) = \gcd(b, r)$.

The **Euclidean Algorithm** is the repeated use of the above Lemma, with two given integers, to find their greatest common divisor. It is remarkable in that it does not depend on finding any of the divisors of the two numbers in question, other than (of course) the greatest common divisor.

Although it is not the only method of doing so, it also provides a method for expressing $\gcd(a, b)$ as a linear combination of a and b if this is desired.

Suppose a and b are positive integers with $a \geqslant b$, and let $r_0 = a$ and $r_1 = b$.

When we successively apply the Division Algorithm, we obtain:

$$\begin{aligned}
r_0 &= r_1q_1 + r_2, && 0 \leqslant r_2 < r_1\\
r_1 &= r_2q_2 + r_3, && 0 \leqslant r_3 < r_2\\
r_2 &= r_3q_3 + r_4, && 0 \leqslant r_4 < r_3\\
&\vdots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, && 0 \leqslant r_n < r_{n-1}\\
r_{n-1} &= r_nq_n + 0
\end{aligned}$$

From the above Lemma,

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = ... = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

So, $\gcd(a, b)$ is the last non-zero remainder in the sequence of divisions.

Note that the remainder must eventually be zero since the sequence of non-negative integer remainders $r_0, r_1, r_2, r_3, ...$ is strictly decreasing.

Example 24

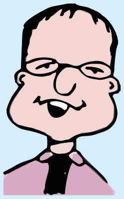
Use the Euclidean Algorithm to find $\gcd(945, 2415)$. Hence find two integers r and s such that $\gcd(945, 2415) = 945r + 2415s$.

Successive divisions give
$$\begin{aligned} 2415 &= 945(2) + 525 \\ 945 &= 525(1) + 420 \\ 525 &= 420(1) + 105 \\ 420 &= 105(4) \end{aligned}$$

Hence $\gcd(945, 2415) = 105$.

We now work backwards, substituting the remainder at each stage:
$$\begin{aligned} 105 &= 525 - 420 \\ &= 525 - (945 - 525) \\ &= 525 \times 2 - 945 \\ &= (2415 - 945(2)) \times 2 - 945 \\ &= 2415 \times 2 - 4 \times 945 - 945 \\ &= 2415 \times 2 - 5 \times 945 \end{aligned}$$

$\therefore$ two such integers are $r = -5$ and $s = 2$.



r and s are not necessarily unique. For example, $r = 41$, $s = -16$ is another solution.

LEAST COMMON MULTIPLE

The **least common multiple (lcm)** of positive integers a and b, denoted $\text{lcm}(a, b)$, is the positive integer m satisfying: (1) $a \mid m$ and $b \mid m$

(2) if $a \mid c$ and $b \mid c$ where $c > 0$, then $m \leqslant c$.

For example, the least common multiple of 6 and 8 is 24.

Note that for any positive integers a and b, $\text{lcm}(a, b) \leqslant ab$.

INVESTIGATION 5 CONNECTING GCD AND LCM

Consider $a, b \in \mathbb{Z}^+$.

The purpose of this investigation is to find a relationship between $\gcd(a, b)$ and $\text{lcm}(a, b)$.

What to do:

1 For each pair of positive integers a, b which follows, find:

i $\gcd(a, b)$ **ii** $\text{lcm}(a, b)$ **iii** $a \times b$

a 70, 120 **b** 37, 60 **c** 108, 168 **d** 450, 325

2 Postulate a result which connects $\gcd(a, b)$ and $\text{lcm}(a, b)$.

Theorem:

For positive integers a and b, $\gcd(a, b) \times \text{lcm}(a, b) = ab$.

Proof:

Let $d = \gcd(a, b)$

$\therefore \quad d \mid a$ and $d \mid b$ and $d \geqslant 1$.

$\therefore \quad a = dr$ and $b = ds$ for $r, s \in \mathbb{Z}^+$

Suppose $m = \dfrac{ab}{d}$.

$\therefore \quad m = \dfrac{(dr)b}{d}$ and $m = \dfrac{a(ds)}{d}$

$\therefore \quad m = br$ and $m = as$

$\therefore \quad m$ is a positive common multiple of a and b.

Now let c be *any* positive integer multiple of a and b.

$\Rightarrow \quad c = au$ and $c = bv$ for some $u, v \in \mathbb{Z}^+$ .... (1)

Since $d = \gcd(a, b)$, there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$

$$\therefore \quad \frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y$$

$$= vx + uy \qquad \{\text{using (1)}\}$$

$$\therefore \quad c = (vx + uy)m$$

$\therefore \quad m \mid c$

$\therefore \quad m \leqslant c$

$\therefore \quad m = \operatorname{lcm}(a, b)$

Corollary:

For positive integers a and b, $\operatorname{lcm}(a, b) = ab \Leftrightarrow \gcd(a, b) = 1$

EXERCISE 1D.2

1 For each of the following integer pairs a, b, use the Euclidean Algorithm to find $\gcd(a, b)$, and hence find integers r and s such that $\gcd = ra + sb$.

a 803, 154 **b** 12 378, 3054 **c** 3172, 793

d 1265, 805 **e** 55, 34

2 Suppose f_j is the jth Fibonacci number.

a Find $\gcd(f_{n+1}, f_n)$.

b **i** Find $\gcd(f_{4(n+1)}, f_{4n})$ for $n = 1, 2, 3, 4$.

ii Postulate and prove a formula for $\gcd(f_{4(n+1)}, f_{4n})$ which is true for all $n \in \mathbb{Z}^+$.

c Postulate and prove a formula for $\gcd(f_{5(n+1)}, f_{5n})$ which is true for all $n \in \mathbb{Z}^+$.

3 Find the gcd and lcm of:

a 143, 227 **b** 272, 1749 **c** 3054, 12 378 **d** 267, 1121

4 Prove the corollary: For positive integers a and b, $\operatorname{lcm}(a, b) = ab \Leftrightarrow \gcd(a, b) = 1$.

THE LINEAR DIOPHANTINE EQUATION $ax + by = c$

A **Diophantine equation** is a polynomial equation that allows two or more variables to take integer values only.

The most famous Diophantine equations are the **Pythagorean equations** whose integer solutions are the Pythagorean triples, and its generalisation to higher dimensions as in **Fermat's last theorem**, $a^n + b^n = c^n$.

In this section we apply the Euclidean Algorithm to the simplest of all Diophantine equations, the linear Diophantine equation $ax + by = c$ where $a, b, c \in \mathbb{Z}$ are constants, and $x, y \in \mathbb{Z}$ are the variables.

Linear Diophantine equations are always to be solved (or proved insolvable) in the integers or sometimes in just the positive integers. There are two variables (x and y) in the equation, and there are either an infinite number of solutions in $\mathbb{Z}$, or none.

For example:

- $3x + 6y = 18$ has an infinite number of solutions in the integers
- $2x + 10y = 17$ has none at all, since $2x + 10y$ is even for all $x, y \in \mathbb{Z}$, whereas 17 is odd.

Theorem:

Suppose $a, b, c \in \mathbb{Z}$, and let $d = \gcd(a, b)$.

(1) $ax + by = c$ has solutions $\Leftrightarrow$ $d \mid c$.

(2) If x_0, y_0 is any particular solution, all solutions are of the form

$$x = x_0 + \left(\frac{b}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t \quad \text{where} \quad t \in \mathbb{Z}.$$

Proof:

(1) $(\Rightarrow)$ $d = \gcd(a, b) \;\Rightarrow\; d \mid a$ and $d \mid b$

$\Rightarrow\; a = dr$ and $b = ds$ for some integers r and s

Now if $x = x_0$ and $y = y_0$ is a solution of $ax + by = c$ then $ax_0 + by_0 = c$

$\Rightarrow\; c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$

$\Rightarrow\; d \mid c$

$(\Leftarrow)$ If $d \mid c$ then $c = dt$ for some integer t .... (1)

Now since $d = \gcd(a, b)$, there exist $x_0, y_0 \in \mathbb{Z}$ such that $d = ax_0 + by_0$.

Multiplying by t gives $dt = (ax_0 + by_0)t$

$\therefore\; c = a(x_0t) + b(y_0t)$ {using (1)}

Hence $ax + by = c$ has a particular solution $x = tx_0$, $y = ty_0$.

(2) x_0, y_0 is a known solution of $ax + by = c$, so $ax_0 + by_0 = c$.

If x', y' is another solution then $ax_0 + by_0 = c = ax' + by'$

$\Rightarrow\; a(x_0 - x') = b(y' - y_0)$ .... (1)

Since $d = \gcd(a, b)$, there exist integers r and s which are relatively prime with $a = dr$ and $b = ds$.

$\Rightarrow\quad dr(x_0 - x') = ds(y' - y_0)$

$\Rightarrow\quad r(x_0 - x') = s(y' - y_0)$

$\Rightarrow\quad r \mid s(y' - y_0)$ with $\gcd(r, s) = 1$ .... (2)

Now **Euclid's Lemma** states that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

$\therefore$ from (2), $r \mid (y_0 - y')$

$$\therefore \; y_0 - y' = rt \quad \text{for some } t \in \mathbb{Z}$$
$$\therefore \; y' = y_0 - rt$$

Substituting into (1), $a(x_0 - x') = b(-rt)$

$$\therefore \; dr(x_0 - x') = ds(-rt)$$
$$\therefore \; x_0 - x' = -st$$
$$\therefore \; x' = x_0 + st$$

So, $x' = x_0 + st$ and $y' = y_0 - rt$

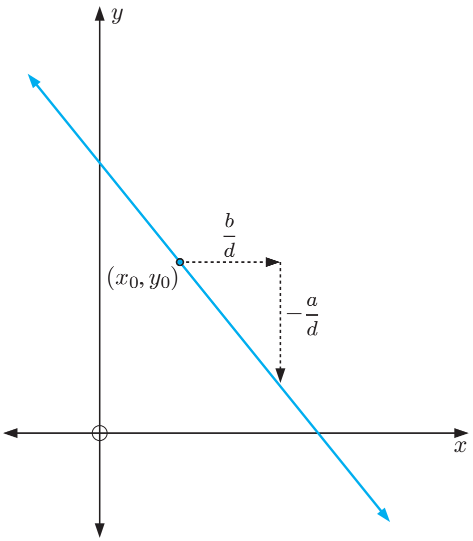
$\therefore$ $x' = x_0 + \left(\frac{b}{d}\right)t$ and $y' = y_0 - \left(\frac{a}{d}\right)t$, $t \in \mathbb{Z}$

Checking the solution for any $t \in \mathbb{Z}$:

$$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)t\right) + b\left(y_0 - \left(\frac{a}{d}\right)t\right) = ax_0 + \frac{abt}{d} + by_0 - \frac{abt}{d} = ax_0 + by_0 = c \quad \checkmark$$

$\therefore$ the given solutions constitute all, infinitely many, solutions.

Graphically, the theorem takes this form:



The equation $ax + by = c$ is that of a straight line with gradient $-\frac{a}{b}$.

Since $\gcd(a, b) \mid c$, c is a multiple of $d = \gcd(a, b)$.

$\therefore$ there exists an integer pair solution (x_0, y_0) on this line.

The general solution is obtained by moving the horizontal distance $\frac{b}{d}$ (an integer) to the right, then moving downwards the vertical distance $-\frac{a}{d}$ (also an integer) back to the line.

Thus all of solutions are integer pairs (x, y).

Example 25

Solve $172x + 20y = 1000$ for x, y in: **a** $\mathbb{Z}$ **b** $\mathbb{Z}^+$.

a We first find $\gcd(172, 20)$ using the Euclidean Algorithm.

$$172 = 20(8) + 12$$
$$20 = 12(1) + 8$$
$$12 = 8(1) + 4$$
$$8 = 4(2) \qquad \therefore \; \gcd(172, 20) = 4$$

Now $4 \mid 1000$, so integer solutions exist.

We now need to write 4 as a linear combination of 172 and 20.

Working backwards:
$$\begin{aligned}4 &= 12-8\\ &= 12-(20-12)\\ &= 2\times 12-20\\ &= 2(172-20(8))-20\\ &= 2\times 172-17\times 20\end{aligned}$$

Multiplying by 250 gives $1000 = 500\times 172 - 4250\times 20$

$\therefore\ x_0 = 500,\ y_0 = -4250$ is one solution pair.

All other solutions have the form $x = 500 + \left(\frac{20}{4}\right)t,\ y = -4250 - \left(\frac{172}{4}\right)t,$

which is, $x = 500+5t,\ y = -4250-43t,\ t\in\mathbb{Z}.$

b If x and y are in $\mathbb{Z}^+$ we need to solve for $t\in\mathbb{Z}$ such that:

$500+5t > 0$ *and* $-4250-43t>0$

$\therefore\ 5t > -500$ *and* $43t < -4250$

$\therefore\ t > -100$ *and* $t < -98.33....$

$\therefore\ t = -99$

$\therefore\ x = 500+5(-99)$ and $y = -4250-43(-99)$

$\therefore\ x = 5$ and $y = 7$ is the unique solution for which $x, y\in\mathbb{Z}^+$.

Corollary:

If $\gcd(a, b) = 1$ and if x_0, y_0 is a particular solution of $ax+by=c$, then all solutions are given by $x = x_0+bt,\ y = y_0-at,\ t\in\mathbb{Z}.$

Linear Diophantine equations often are observed in word puzzles, as in the following example.

Example 26

A cow is worth 10 pieces of gold, a pig is worth 5 pieces of gold, and a hen is worth 1 piece of gold. 220 gold pieces are used to buy a total of 100 cows, pigs, and hens.

How many of each animal is bought?

Let the number of cows be c, the number of pigs be p, and the number of hens be h.

$\therefore\ c+p+h = 100$ {the total number of animals}

and $10c+5p+h = 220$ {the total number of gold pieces}

Subtracting these equations gives $9c+4p = 120$ where $\gcd(9, 4) = 1$.

By observation, $c_0 = 0$ and $p_0 = 30$ is one solution pair.

$\therefore\ c = 0+4t$ and $p = 30-9t,\ t\in\mathbb{Z}$ is the general solution,
which is, $c = 4t,\ p = 30-9t,\ h = 100-p-c = 70+5t.$

But c, p, and h are all positive

$$\therefore\ 4t > 0 \quad \textit{and} \quad 30 - 9t > 0 \quad \textit{and} \quad 70 + 5t > 0$$
$$\therefore\ t > 0 \quad \textit{and} \quad t < \tfrac{30}{9} \quad \textit{and} \quad t > -\tfrac{70}{5}$$

$\therefore\ 0 < t < 3.33$ where $t \in \mathbb{Z}$.

So, there are three possible solutions, corresponding to $t = 1$, 2, or 3. These are:

$\{c = 4,\ p = 21,\ h = 75\}$ or $\{c = 8,\ p = 12,\ h = 80\}$ or $\{c = 12,\ p = 3,\ h = 85\}$

EXERCISE 1D.3

1 Find, where possible, all $x, y \in \mathbb{Z}$ such that:

a $6x + 51y = 22$ **b** $33x + 14y = 115$ **c** $14x + 35y = 93$

d $72x + 56y = 40$ **e** $138x + 24y = 18$ **f** $221x + 35y = 11$

2 Find all positive integer solutions of:

a $18x + 5y = 48$ **b** $54x + 21y = 906$ **c** $123x + 360y = 99$

d $158x - 57y = 11$

3 Two positive numbers add up to 100. One number is divisible by 7, and the other is divisible by 11. Find the numbers.

4 There are a total of 20 men, women, and children at a party.
Each man has 5 drinks, each woman has 4 drinks, and each child has 2 drinks. They have 62 drinks in total. How many men, women, and children are at the party?

5 I wish to buy 100 animals. Cats cost me €50 each, rabbits cost €10 each, and fish cost 50 cents each. I have €1000 to spend, and buy at least one of each animal.
If I spend all of my money on the purchase of these animals, how many of each kind of animal do I buy?

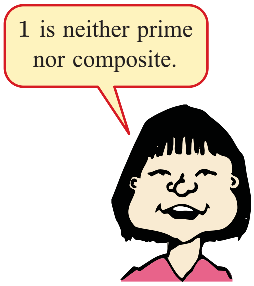
6 The cities A and M are 450 km apart. Smith travels from A to M at a constant speed of 55 km h^{-1}, and his friend Jones travels from M to A at a constant speed of 60 km h^{-1}. When they meet, they both look at their watches and exclaim: "It is exactly half past the hour, and I started at half past!". Where do they meet?

7 A person buys a total of 100 blocks of chocolate. The blocks are available in three sizes, which cost \$3.50 each, \$4 for three, and 50 cents each respectively. If the total cost is \$100, how many blocks of each size does the person buy?

E PRIME NUMBERS

An integer p is a **prime number** (or **prime**) if $p > 1$, and if the only positive numbers which divide p are 1 and p itself.

An integer greater than 1 that is not prime is said to be **composite**.



We have already proven that there are an infinite number of primes, but they appear to not follow any pattern. It would be very useful to discover an efficient method for finding prime numbers, because at present no such method exists. This is in fact the basis of the RSA encription system by which international financial and security transactions are protected. The study of number theory is therefore a highly important and applicable area of study. The basis of the RSA encryption system is a suitable topic for an Extended Essay in Mathematics.

Euclid's Lemma for primes

For integers a and b and prime p, if $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$ the proof is complete, so suppose $p \nmid a$.

Since $p \nmid a$ and p is prime, $\gcd(a, p) = 1$.

$\therefore$ there exist integers r and s such that $ar + ps = 1$.

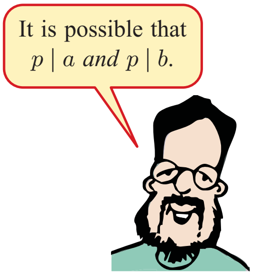
$\therefore$ $b = b \times 1 = b(ar + ps) = abr + bps$

But $p \mid ab$, so $ab = kp$ for some integer k

$\therefore$ $b = kpr + bps = p(kr + bs)$

$\therefore$ $p \mid b$.

So, either $p \mid a$ or $p \mid b$.



Lemma: If p is a prime and $p \mid a_1a_2a_3....a_n$ for $a_1, a_2, a_3, ..., a_n \in \mathbb{Z}$ then there exists i where $1 \leqslant i \leqslant n$ such that $p \mid a_i$.

For example, if $p \mid 6 \times 11 \times 24$ then $p \mid 6$ or $p \mid 11$ or $p \mid 24$. At least one of 6, 11, and 24 must be a multiple of p.

Proof: (By Induction)

(1) If $n = 1$ then $p \mid a_1$. $\therefore$ P_1 is true.

(2) If P_k is true, then $p \mid a_1a_2a_3....a_k \Rightarrow p \mid a_i$ for some i where $1 \leqslant i \leqslant k$.
Now if $p \mid a_1a_2a_3....a_ka_{k+1}$ then $p \mid (a_1a_2a_3....a_k)a_{k+1}$
$\therefore$ $p \mid a_1a_2a_3....a_k$ or $p \mid a_{k+1}$ {using Euclid's Lemma for primes}
$\therefore$ $p \mid a_i$ for some i in $1 \leqslant i \leqslant k$, or $p \mid a_{k+1}$
$\therefore$ $p \mid a_i$ for some i in $1 \leqslant i \leqslant k + 1$

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.
$\therefore$ P_n is true. {Principle of Mathematical Induction}

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every positive integer greater than 1 is either prime, or is expressible uniquely (up to the ordering) as a product of primes.

Proof:

Existence: Let S be the set of positive integers which cannot be written as a product of primes, and suppose S is non-empty.

By the Well Ordered Principle, S has a smallest number, which we will call a.

If the only factors of a are a and 1 then a is a prime, which is a contradiction.

$\therefore$ we can write a as the product of factors $a = a_1 a_2$ where $1 < a_1 < a$, $1 < a_2 < a$.

Neither a_1 nor a_2 are in S, since a is the smallest member of S.

$\therefore$ a_1 and a_2 can be factorised into primes: $a_1 = p_1 p_2 p_3 .... p_r$ and $a_2 = q_1 q_2 q_3 .... q_s$.

$\therefore$ $a = a_1 a_2 = (p_1 p_2 p_3 .... p_r)(q_1 q_2 q_3 .... q_s)$

$\therefore$ $a \notin S$, which is a contradiction. Therefore S is empty, and every positive integer greater than 1 is either prime, or is expressible as a product of primes.

Uniqueness: Suppose an integer $n \geqslant 2$ has two different factorisations
$n = p_1 p_2 p_3 .... p_s = q_1 q_2 q_3 .... q_t$ where $p_i \neq q_j$ for all i, j.

By Euclid's Lemma for primes, $p_1 \mid q_j$ for some j.
$\Rightarrow$ $p_1 = q_j$ {as these are primes}

Relabelling q_j as q_1 if necessary, we can instead write $p_1 = q_1$

$$\therefore \quad \frac{n}{p_1} = p_2 p_3 p_4 .... p_s = q_2 q_3 q_4 .... q_t$$

By the same reasoning, relabelling if necessary, $p_2 = q_2$ and

$$\frac{n}{p_1 q_1} = p_3 p_4 .... p_s = q_3 q_4 .... q_t$$

This can be done for all p_j, showing that $s \leqslant t$.

The same argument could be made swapping ps and qs, so $t \leqslant s$ also.

$\therefore$ $s = t$, the p_is are a rearrangement of the q_js, and the prime factorisation is unique up to the ordering of the primes.

Example 27

Discuss the prime factorisation of 360, including how many factors 360 has.

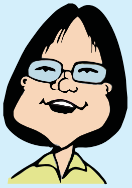
$$\begin{array}{r|r} 2 & 360 \\ \hline 2 & 180 \\ \hline 2 & 90 \\ \hline 3 & 45 \\ \hline 3 & 15 \\ \hline & 5 \end{array}$$

$360 = 2^3 \times 3^2 \times 5^1$ and this factorisation is unique up to the ordering of the factors.

The only prime factors of 360 are 2, 3, and 5.

Including 1 and 360, 360 has
$(3+1)(2+1)(1+1)$
$= 4 \times 3 \times 2$
$= 24$ factors.

Check this result by listing all 24 factors in a systematic way. For example:
$2^0 \times 3^0 \times 5^0$,
$2^2 \times 3^1 \times 5^0$, ...



Finally, we present a theorem that can be used to reduce the work in identifying whether a given integer, n, is prime. In it we show that we need only attempt to divide n by all the primes $p \leqslant \sqrt{n}$. If none of these is a divisor, then n must itself be prime.

Theorem:

If $n \in \mathbb{Z}^+$ is composite, then n has a prime divisor p such that $p \leqslant \sqrt{n}$.

Proof:

Let $n \in \mathbb{Z}^+$ be composite.

$\therefore$ $n = ab$ where $a, b \in \mathbb{Z}^+$ such that $n > a > 1$ and $n > b > 1$.

If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > n$, which is a contradiction.

$\therefore$ at least one of a or b must be $\leqslant \sqrt{n}$.

Without loss of generality, suppose $a \leqslant \sqrt{n}$.

Since $a > 1$, there exists a prime p such that $p \mid a$. {Fundamental Theorem of Arithmetic}

But $a \mid n$, so $p \mid n$. $\{p \mid a$ and $a \mid n \Rightarrow p \mid n\}$

Since $p \leqslant a \leqslant \sqrt{n}$, n has a prime divisor p such that $p \leqslant \sqrt{n}$.

EXERCISE 1E

1 Determine which of the following are primes:

a 143 **b** 221 **c** 199 **d** 223

2 Prove that 2 is the only even prime.

3 Which of the following repunits is prime?

a 11 **b** 111 **c** 1111 **d** 11 111

4 Show that if p and q are primes and $p \mid q$, then $p = q$.

5 $2^8 \times 3^4 \times 7^2$ is a perfect square. It equals $(2^4 \times 3^2 \times 7)^2$.

a Prove that:

i all the powers in the prime-power factorisation of $n \in \mathbb{Z}^+$ are even $\Leftrightarrow$ n is a square

ii given $n \in \mathbb{Z}^+$, the number of factors of n is odd $\Leftrightarrow$ n is a square.

b Hence prove that $\sqrt{2}$ is irrational.

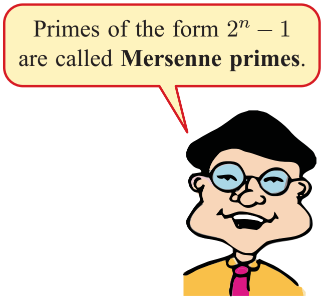
6 **a** Prove that if $a, n \in \mathbb{Z}^+$, $n \geqslant 2$ and $a^n - 1$ is prime, then $a = 2$.

Hint: Consider $1 + a + a^2 + ... + a^{n-1}$ and its sum.

b It is claimed that $2^n - 1$ is always prime for $n \geqslant 2$. Is the claim true?

c It is claimed that $2^n - 1$ is always composite for $n \geqslant 2$. Is the claim true?

d If n is prime, is $2^n - 1$ always prime? Explain your answer.


Primes of the form $2^n - 1$ are called **Mersenne primes**.

7 Find the prime factorisation of:

a 9555 **b** 989 **c** 9999 **d** 111 111

8 Which positive integers have exactly:

a three positive divisors **b** four positive divisors?

9 **a** Find all prime numbers which divide 50!

b How many zeros are at the end of 50! when written as an integer?

c Find all $n \in \mathbb{Z}$ such that $n!$ ends in exactly 74 zeros.

10 Given that p is prime, prove that:

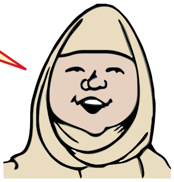
a $p \mid a^n \Rightarrow p^n \mid a^n$ **b** $p \mid a^2 \Rightarrow p \mid a$ **c** $p \mid a^n \Rightarrow p \mid a$

11 There are infinitely many primes, and 2 is the only even prime.

a Explain why the form of odd primes can be $4n+1$ or $4n+3$.

b Prove that there are infinitely many primes of the form $4n+3$.

There are also infinitely many primes of the form $4n+1$, but the proof is beyond the scope of this course.



12 The **Fermat primes** are primes of the form $2^{2^n}+1$.

a Find the first four Fermat primes.

b Fermat conjectured that all such numbers were prime whenever n was prime. By examining the case $n=5$, show that Fermat was incorrect.

RESEARCH

- The first two **perfect numbers** are 6 and 28. Research how these numbers are connected to the Mersenne primes of the form 2^n-1.
- The repunits R_k are prime only if k is prime, and even then only rarely. Thus far, the only prime repunits discovered are R_2, R_{19}, R_{23}, R_{317}, and R_{1031}.
  Research a proof that a repunit R_k may only be prime if k is prime.

F CONGRUENCES

The German mathematician **Carl Friedrich Gauss** is often quoted as saying "Mathematics is the queen of sciences and the theory of numbers is the queen of mathematics". Gauss was responsible for the development of the theory of **congruences**.

Suppose $m \in \mathbb{Z}^+$.

Two integers a and b are **congruent** modulo m $\Leftrightarrow$ $m \mid (a-b)$. We write $a \equiv b \pmod{m}$.

If $m \nmid (a-b)$, then a is **incongruent** (or not congruent) to b modulo m. We write $a \not\equiv b \pmod{m}$.

For example, $64 - 7 = 57 = 3 \times 19$, so $3 \mid (64 - 7)$.

$\therefore$ $64 \equiv 7 \pmod{3}$.

We observe that 7 and 64 have the same remainder when divided by 3.

$$\begin{aligned} 7 &= 3 \times 2 + 1 \\ 64 &= 3 \times 21 + 1 \end{aligned}$$

We have therefore, for $m \in \mathbb{Z}^+$:

$$\begin{aligned} a \equiv b \pmod{m} &\Leftrightarrow m \mid (a-b) \\ &\Leftrightarrow \text{there exists } k \in \mathbb{Z} \text{ such that } a = b + km. \end{aligned}$$

For example:

- $37 \equiv 2 \pmod{5}$ as $37 - 2 = 35$ is divisible by 5.
- $43 \equiv 1 \pmod{7}$ as $43 - 1 = 42$ is divisible by 7.
- $a \equiv 0 \pmod{7}$ $\Leftrightarrow$ $a = 7t$, $t \in \mathbb{Z}$ $\Leftrightarrow$ a is a multiple of 7.

Note that in modulo algebra, if $2x \equiv 3 \pmod{5}$ then $x \neq 1.5$. In fact, $x = 4$ is one solution, and all other solutions have the form $x = 4 + 5k$, $k \in \mathbb{Z}$.

For $m \in \mathbb{Z}^+$, congruence modulo m is an **equivalence relation** since it has the following three properties:

Reflexive: If $a \in \mathbb{Z}$ then $a \equiv a \pmod{m}$.

Symmetric: If $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Transitive: If $a, b, c \in \mathbb{Z}$ with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

Proof:

For any fixed $m \in \mathbb{Z}^+$:

Reflexive: $m \mid (a-a)$ $\therefore$ $a \equiv a \pmod{m}$ for all $a \in \mathbb{Z}$.

Symmetric:

$$\begin{aligned} & a \equiv b \pmod{m} \\ \Leftrightarrow\ & m \mid (a-b) \\ \Leftrightarrow\ & m \mid (b-a) \\ \Leftrightarrow\ & b \equiv a \pmod{m}. \end{aligned}$$

Transitive: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $m \mid (a-b)$ and $m \mid (b-c)$

$\therefore \quad m \mid [(a-b)+(b-c)]$ {linearity}

$\therefore \quad m \mid (a-c)$

$\therefore \quad a \equiv c \pmod{m}$.

Since congruence modulo m is reflexive, symmetric, and transitive, it is an equivalence relation.

Suppose $m \in \mathbb{Z}^+$. The m **residue classes modulo** $\boldsymbol{m}$ are the following subsets of $\mathbb{Z}$:

$$\begin{aligned} [0] &= \{\text{multiples of } m\} \\ [1] &= \{\text{integers which have remainder 1 on division by } m\} \\ &\vdots \\ [m-1] &= \{\text{integers which have remainder } (m-1) \text{ on division by } m\} \end{aligned}$$

For $a \in \mathbb{Z}$, if a has remainder r on division by m, we say r is the **residue of** $\boldsymbol{a}$ **modulo** $\boldsymbol{m}$.

Theorem:

For $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, and $r \in \{0, 1, 2, ..., m-1\}$:

(1) $a \equiv r \pmod{m} \Leftrightarrow$ a has remainder r on division by m $\Leftrightarrow a \in [r]$.

(2) $a \equiv b \pmod{m} \Leftrightarrow$ a and b have the same remainder on division by m
$\Leftrightarrow$ a and b belong to the same residue class modulo m.

Proof:

(1) $a \equiv r \pmod{m} \Leftrightarrow a = r + km$ and $0 \leqslant r \leqslant m-1 \Leftrightarrow a \in [r]$.

(2) $a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$
$\Leftrightarrow a = b + km$ for some $k \in \mathbb{Z}$.

By the Division Algorithm, $a = mq_1 + r_1$
and $b = mq_2 + r_2$
for some $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ with $0 \leqslant r_1, r_2 \leqslant m-1$.

Thus $a = b + km$
$\Leftrightarrow mq_1 + r_1 = mq_2 + r_2 + km$
$\Leftrightarrow m(q_1 - q_2 - k) = r_2 - r_1$
$\Leftrightarrow r_2 - r_1$ is a multiple of m
$\Leftrightarrow r_2 - r_1 = 0$ since $r_1, r_2 \in \{0, 1, 2, ..., m-1\}$.
$\Leftrightarrow$ a and b have the same remainder on division by m.
$\Leftrightarrow$ a and b belong to the same residue class modulo m (by definition).

It follows that for $m \in \mathbb{Z}$:

The equivalence relation **congruence modulo** $\boldsymbol{m}$ has **equivalence classes** which are the m residue classes modulo m.

The residue classes modulo m partition the set of integers into m disjoint subsets.

Clearly, the form of the definition of congruences $a \equiv b \pmod{m} \Leftrightarrow a = b + km$ links neatly with the Division Algorithm.

Consider the equation $a = bm + r$, where $0 \leqslant r \leqslant m - 1$. Clearly, $a \equiv r \pmod{m}$ and we call r the **residue of $a \pmod{m}$**.

Generalising this to all integers, we can state that **all** integers are congruent to one of the possible values of r, namely, one of the set $\{0, 1, 2, 3, ..., (m-1)\}$. This set is called the **complete system of residues modulo m**, for $m \in \mathbb{Z}^+$.

MODULAR ARITHMETIC

Modular arithmetic deals with the manipulation of residues.

As a general rule, we try to reduce all integers to their **least** residue equivalent at all times. This simplifies the arithmetic.

For example:

$$\begin{aligned} & 19 + 14 \pmod 8 \\ = {} & 3 + 6 \pmod 8 \\ = {} & 9 \pmod 8 \\ = {} & 1 \pmod 8 \end{aligned} \qquad \begin{aligned} & 19 - 14 \pmod 8 \\ = {} & 5 \pmod 8 \end{aligned} \qquad \begin{aligned} & 19 \times 14 \pmod 8 \\ = {} & 3 \times 6 \pmod 8 \\ = {} & 18 \pmod 8 \\ = {} & 2 \pmod 8 \end{aligned}$$

Addition, subtraction, and multiplication $\pmod m$ are relatively straight forward. However, division is more complicated.

For example, can you solve the equivalence equations by inspection?

- $3x \equiv 4 \pmod 7$
- $4x - 3 \equiv 5 \pmod 6$
- $x^2 \equiv 3 \pmod 6$

Is there a unique solution to each equation?

INVESTIGATION 6 MODULAR ALGEBRA

In this Investigation we use the property that $a \equiv b \pmod m \Leftrightarrow m \mid (a - b) \Leftrightarrow a = b + km$ for $k \in \mathbb{Z}$, to develop rules for modular algebra.

What to do:

Prove the following results:

1 Rules for $+$, $-$, and $\times$ with $k, a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$:
Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$:

a $a + c \equiv b + d \pmod m$ **b** $a - c \equiv b - d \pmod m$

c $ka \equiv kb \pmod m$ **d** $ac \equiv bd \pmod m$

2 Condition for division (cancellation)

a If $ka \equiv kb \pmod m$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod m$.

b If $ka \equiv kb \pmod m$ and $\gcd(k, m) = d$, then $a \equiv b \pmod{\frac{m}{d}}$.

3 If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$ for all $n \in \mathbb{Z}^+$.
Note: The converse is not necessarily true.

4 If $f(x)$ is a polynomial with integer coefficients and $a \equiv b \pmod m$, then $f(a) \equiv f(b) \pmod m$.

In the **Investigation** you should have proven the following results:

- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then:
  - $a \pm c \equiv b \pm d \pmod{m}$
  - $ka \equiv kb \pmod{m}$
  - $a^n \equiv b^n \pmod{m}$
  - $ac \equiv bd \pmod{m}$.
- If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = d$ then $a \equiv b \pmod{\frac{m}{d}}$.
- If $f(x)$ is a polynomial with integer coefficients and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Example 28

Find $65^{22} \pmod{7}$.

$$\begin{aligned} 65 &\equiv 2 \pmod{7} \qquad \{\text{since } 65 - 2 = 63 = 9 \times 7\} \\ \therefore\ 65^{22} &\equiv 2^{22} \pmod{7} \\ &\equiv (2^3)^7 \times 2 \pmod{7} \\ &\equiv 1 \times 2 \pmod{7} \qquad \{\text{since } 2^3 = 8 \equiv 1\} \\ &\equiv 2 \pmod{7} \end{aligned}$$

Example 29

Prove that $2^{40} - 1$ is divisible by 41.

$$\begin{aligned} 2^5 &= 32 \equiv -9 \pmod{41} \\ \therefore\ 2^{40} &= (2^5)^8 \equiv (-9)^8 \pmod{41} \\ \text{But } (-9)^2 &= 81 \equiv -1 \pmod{41} \\ \therefore\ 2^{40} &\equiv (-1)^4 \pmod{41} \\ &\equiv 1 \pmod{41} \\ \therefore\ 2^{40} - 1 &\equiv 0 \pmod{41} \end{aligned}$$

$\therefore\ 41 \mid (2^{40} - 1)$.

Example 30

Find $\sum\limits_{k=1}^{50} k! \pmod{30}$.

We first note that $5! = 120 \equiv 0 \pmod{30}$

$\therefore\ k! \equiv 0 \pmod{30}$ for all $k \geqslant 5$

$$\begin{aligned} \therefore\ \sum_{k=1}^{50} k! \pmod{30} &\equiv 1! + 2! + 3! + 4! \pmod{30} \\ &= 1 + 2 + 6 + 24 \pmod{30} \\ &\equiv 3 \pmod{30} \end{aligned}$$

GRAPHICS CALCULATOR INSTRUCTIONS

EXERCISE 1F.1

1 Determine whether the following pairs of numbers are congruent $(\bmod 7)$:

a $1,\ 15$ **b** $-1,\ 8$ **c** $2,\ 99$ **d** $-1,\ 699$

2 Determine the positive integers m for which:

a $29 \equiv 7 \pmod{m}$ **b** $100 \equiv 1 \pmod{m}$ **c** $53 \equiv 0 \pmod{m}$ **d** $61 \equiv 1 \pmod{m}$

3 Find:

a $2^{28} \pmod 7$ **b** $10^{33} \pmod 7$ **c** $3^{50} \pmod 7$ **d** $41^{23} \pmod 7$

4 Find:

a $2^{28} \pmod{37}$ **b** $3^{65} \pmod{13}$ **c** $7^{44} \pmod{11}$

5 Prove that:

a $53^{103} + 103^{53}$ is divisible by 39 **b** $333^{111} + 111^{333}$ is divisible by 7.

6 Find the remainder when $2^{100} + 3^{100}$ is divided by 5.

7 Find the last two digits of 203^{20}.

8 Find:

a $\sum\limits_{k=1}^{50} k! \pmod{20}$ **b** $\sum\limits_{k=1}^{50} k! \pmod{42}$ **c** $\sum\limits_{k=10}^{100} k! \pmod{12}$ **d** $\sum\limits_{k=4}^{30} k! \pmod{10}$

9 **a** Find:

i $5^{10} \pmod{11}$ **ii** $3^{12} \pmod{13}$ **iii** $2^{18} \pmod{19}$ **iv** $7^{16} \pmod{17}$

b Use your results from **a** to formulate a conjecture.

c Find:

i $4^{11} \pmod{12}$ **ii** $5^{8} \pmod 9$ **iii** $33^{10} \pmod{11}$ **iv** $34^{16} \pmod{17}$

d Use your results from **c** to give conditions under which your conjecture in **b** is valid.

10 **a** Find:

i $2! \pmod 3$ **ii** $4! \pmod 5$

iii $10! \pmod{11}$ **iv** $6! \pmod 7$

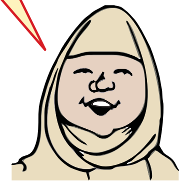
b Use your results from **a** to postulate a theorem.

c Find:

i $3! \pmod 4$ **ii** $5! \pmod 6$

d Use your results from **c** to give conditions under which your theorem in **b** is valid.

The proof of this result is linked with properties of the cyclic group $\{\mathbb{Z}_p \setminus \{0\},\ \times_p\}$, p prime, studied in the option **Sets, Relations, and Groups**.



11 Prove that:

a $7 \mid (5^{2n} + 3 \times 2^{5n-2})$ **b** $13 \mid (3^{n+2} + 4^{2n+1})$ **c** $27 \mid (5^{n+2} + 2^{5n+1})$

12 Prove that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

13 Prove that:

a the square of any even integer $\equiv 0 \pmod 4$

b the square of any odd integer $\equiv 1 \pmod 4$

c the square of any integer $\equiv 0$ or $1 \pmod 3$

d the cube of any integer $\equiv 0$ or 1 or $8 \pmod 9$.

14 **a** Prove that the square of any odd integer $\equiv 1 \pmod 8$.

b Comment on the squares of even integers $\pmod 8$.

15 Suppose $a, b, c \in \mathbb{Z}^+$ such that $a \equiv b \pmod c$. Show that $\gcd(a, c) = \gcd(b, c)$, and interpret this result.

16 **a** Solve the congruence: **i** $x^2 \equiv 1 \pmod 3$ **ii** $x^2 \equiv 4 \pmod 7$.

b Suppose $x^2 \equiv a^2 \pmod p$ where $x, a \in \mathbb{Z}$ and p is prime. What can you deduce about the relationship between x and a?

17 **a** Show that if n is an odd positive integer, then $\sum_{k=1}^{n} k \equiv 0 \pmod n$.

b Determine what happens if n is even.

18 By considering n having each of the forms $n = 4m + r$ for $r = 0, 1, 2, 3,$ determine conditions under which $\sum_{k=1}^{n-1} k^3 \equiv 0 \pmod n$. **Hint:** $\sum_{i=1}^{n} i^3 = \left[\frac{n}{2}(n+1)\right]^2$

19 For which positive integers n is $\sum_{k=1}^{n} k^2 \equiv 0 \pmod n$?

20 **a** Prove by induction that for $n \in \mathbb{Z}^+$:

i $3^n \equiv 1 + 2n \pmod 4$ **ii** $4^n \equiv 1 + 3n \pmod 9$ **iii** $5^n \equiv 1 + 4n \pmod{16}$

b Prove a general result of the cases in **a**.

21 Prove that the eleventh Mersenne number $2^{11} - 1$ is divisible by 23, and thus not prime.

CANCELLATION IN CONGRUENCES

In **Investigation 6** we saw that for $m \in \mathbb{Z}^+$, $a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod m$ then $ca \equiv cb \pmod m$.

The converse of this result only holds in particular cases.

Theorem:

If $ca \equiv cb \pmod m$ and $\gcd(c, m) = d$, then $a \equiv b \left(\bmod \frac{m}{d}\right)$.

Proof:

$ca \equiv cb \pmod m \Rightarrow ca = cb + km$ for some $k \in \mathbb{Z}$

Since $\gcd(c, m) = d$, there exist relatively prime r and s such that $c = rd$ and $m = sd$.

$\Rightarrow rda = rdb + ksd$

$\Rightarrow ra = rb + ks$

$\Rightarrow r(a - b) = ks$

$\Rightarrow s \mid r(a - b)$ where r, s are relatively prime

$\Rightarrow s \mid (a - b)$ {Euclid's Lemma}

Thus $a - b = ts = t\left(\frac{m}{d}\right)$ for some $t \in \mathbb{Z}$.

$\therefore$ $a \equiv b \left(\bmod \frac{m}{d}\right)$.

The consequences of this theorem are:

- A common factor c in a congruence can be cancelled if c and the modulus m are relatively prime: If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.
- If $ca \equiv cb \pmod{p}$ and $p \nmid c$ and p is prime, then $a \equiv b \pmod{p}$.

Notice that:

- $ab \equiv 0 \pmod{n}$ may occur without $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.
  For example, $4 \times 3 = 0 \pmod{12}$, but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$.
- If $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod{n}$ using the first consequence above.
- If $ab \equiv 0 \pmod{p}$ where p is prime, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$ using the second consequence above.

Example 31

a Use $33 \equiv 15 \pmod{9}$ to explain why $11 \equiv 5 \pmod{3}$.

b Use $-35 \equiv 45 \pmod{8}$ to explain why $-7 \equiv 9 \pmod{8}$.

a

$$33 \equiv 15 \pmod{9}$$

that is, $11 \times 3 \equiv 5 \times 3 \pmod{9}$

and $\gcd(3, 9) \equiv 3$

$\therefore\ 11 \equiv 5 \pmod{\frac{9}{3}}$

that is, $11 \equiv 5 \pmod{3}$

b

$$-35 \equiv 45 \pmod{8}$$

that is, $-7 \times 5 \equiv 9 \times 5 \pmod{8}$

and $\gcd(5, 8) = 1$

$\therefore\ -7 \equiv 9 \pmod{8}$

LINEAR CONGRUENCES

Linear congruences are equations of the form $ax \equiv b \pmod{m}$, where $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$.

In this section we develop the theory for finding the solution of these equations.

Suppose $x = x_0$ is a solution of $ax \equiv b \pmod{m}$, so $ax_0 = b \pmod{m}$.

$\therefore\ ax_0 = b + y_0 m$ for some $y_0 \in \mathbb{Z}$.

Thus, solving a linear congruence is equivalent to solving a linear Diophantine equation, except that there are not infinitely many solutions, but rather at most m solutions when working modulo m.

Our goal is to obtain all **incongruent** solutions to $ax \equiv b \pmod{m}$ as all congruent solutions are considered to be the same.

For example: Consider the equation $4x \equiv 8 \pmod{12}$
$x = 2$, $x = -10$, and $x = 14$ represent the same solution, since
$2 \equiv -10 \equiv 14 \pmod{12}$.
$x = 2$, $x = 5$, $x = 8$, and $x = 11$ are the distinct solutions modulo 12.
So, $4x \equiv 8 \pmod{12} \Rightarrow x = 2, 5, 8,$ or 11.

Theorem:

$ax \equiv b \pmod{m}$ has a solution $\Leftrightarrow$ $d \mid b$ where $d = \gcd(a, m)$, and in this case the equation has d mutually incongruent solutions modulo m.

Proof:

$ax \equiv b \pmod{m}$ is equivalent to solving the linear Diophantine equation $ax - my = b$.

Let $d = \gcd(a, m)$ and note that $\gcd(a, m) = \gcd(a, -m)$.

Hence $d \mid b$ is the necessary and sufficient condition for a solution to exist. {see the earlier work on Diophantine equations}

$\Rightarrow$ if x_0, y_0 is a solution then all solutions are of the form $x = x_0 + \left(\frac{m}{d}\right)t$, $y = y_0 + \left(\frac{a}{d}\right)t$, $t \in \mathbb{Z}$.

If $t = 0, 1, 2, 3, ..., (d-1)$ we obtain the solutions

$$x = x_0,\ x_0 + \left(\frac{m}{d}\right),\ x_0 + 2\left(\frac{m}{d}\right),\ x_0 + 3\left(\frac{m}{d}\right),\ ....,\ x_0 + (d-1)\left(\frac{m}{d}\right),\ \text{respectively.} \quad ....\ (*)$$

We now claim that these integers are incongruent modulo m, and any other solution is equivalent to one of these given solutions.

Suppose two of these solutions are equal, so $x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \pmod{m}$ where $0 \leqslant t_1 < t_2 \leqslant (d-1)$

$$\Rightarrow \left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \pmod{m}$$

Since $\gcd\left(\frac{m}{d}, m\right) = \frac{m}{d}$ we can use the cancellation law to obtain $t_1 \equiv t_2 \pmod{d}$.

But $t_1 \equiv t_2 \pmod{d} \Rightarrow d \mid (t_2 - t_1)$ which contradicts $0 \leqslant t_1 < t_2 \leqslant (d-1)$ since $0 < t_2 - t_1 \leqslant (d-1) < d$.

Thus the integers $(*)$ are mutually incongruent modulo m.

It remains to prove that any other solution $x_0 + \left(\frac{m}{d}\right)t$ is congruent $\pmod{m}$ to one of the d integers in $(*)$. We do this by using the Division Algorithm.

If $t > d$ or $t < -d$ then t can be written as $t = qd + r$ with $0 \leqslant r \leqslant (d-1)$

$$\begin{aligned}\Rightarrow x_0 + \left(\frac{m}{d}\right)t &= x_0 + \left(\frac{m}{d}\right)(qd + r)\\ &= x_0 + mq + \left(\frac{m}{d}\right)r\\ &\equiv x_0 + \left(\frac{m}{d}\right)r \pmod{m}\end{aligned}$$ which is one of the d selected solutions in $(*)$.

We conclude that:

If x_0 is any solution of $ax \equiv b \pmod{m}$, then there are $d = \gcd(a, m)$ incongruent solutions:

$$x = x_0,\ x_0 + \left(\frac{m}{d}\right),\ x_0 + 2\left(\frac{m}{d}\right),\ x_0 + 3\left(\frac{m}{d}\right),\ ....,\ x_0 + (d-1)\left(\frac{m}{d}\right),\ \text{where necessarily } d \mid b.$$

In the special case where a and m are relatively prime:

If $\gcd(a, m) = 1$, then $ax \equiv b \pmod{m}$ has a unique solution modulo m for each $b \in \mathbb{Z}$.

Example 32

Solve for x:

a $2x \equiv 3 \pmod 5$ **b** $12x \equiv 24 \pmod{54}$ **c** $9x \equiv 15 \pmod{24}$

a $2x \equiv 3 \pmod 5$ has $\gcd(2, 5) = 1$

$\therefore$ we have a unique solution.

By inspection, $x \equiv 4 \pmod 5$ $\{$as $2 \times 4 = 8 \equiv 3 \pmod 5\}$

b $12x \equiv 24 \pmod{54}$ has $\gcd(12, 54) = 6$ where $6 \mid 24$

$\therefore$ there are exactly 6 incongruent solutions.

Cancelling by 6 gives $2x \equiv 4 \pmod 9$

$\therefore$ $x \equiv 2 \pmod 9$

$\therefore$ the solutions are $x = 2 + (\frac{54}{6})t = 2 + 9t$ where $t = 0, 1, 2, 3, 4, 5.$

$\therefore$ $x \equiv 2, 11, 20, 29, 38,$ or $47 \pmod{54}$

c $9x \equiv 15 \pmod{24}$ has $\gcd(9, 24) = 3$ where $3 \mid 15$

$\therefore$ there are exactly 3 incongruent solutions.

Cancelling by 3 gives $3x \equiv 5 \pmod 8$

By inspection, $x \equiv 7$ is a solution.

$\therefore$ the solutions are $x = 7 + 8t \pmod{24}$, where $t = 0, 1, 2.$

$\therefore$ $x \equiv 7, 15,$ or $23 \pmod{24}$

EXERCISE 1F.2

1 Solve, if possible, the following linear congruences:

a $2x \equiv 3 \pmod 7$ **b** $8x \equiv 5 \pmod{25}$ **c** $3x \equiv 6 \pmod{12}$

d $9x \equiv 144 \pmod{99}$ **e** $18x \equiv 30 \pmod{40}$ **f** $3x \equiv 2 \pmod 7$

g $15x \equiv 9 \pmod{27}$ **h** $56x \equiv 14 \pmod{21}$

2 Determine whether the following statements are true:

a $x \equiv 4 \pmod 7 \Rightarrow \gcd(x, 7) = 1$

b $12x \equiv 15 \pmod{35} \Rightarrow 4x \equiv 5 \pmod 7$

c $12x \equiv 15 \pmod{39} \Rightarrow 4x \equiv 5 \pmod{13}$

d $x \equiv 7 \pmod{14} \Rightarrow \gcd(x, 14) = 7$

e $5x \equiv 5y \pmod{19} \Rightarrow x \equiv y \pmod{19}$

f $3x \equiv y \pmod 8 \Rightarrow 15x \equiv 5y \pmod{40}$

g $10x \equiv 10y \pmod{14} \Rightarrow x \equiv y \pmod 7$

h $x \equiv 41 \pmod{37} \Rightarrow x \pmod{41} = 37$

i $x \equiv 37 \pmod{40}$ and $0 \leqslant x < 40 \Rightarrow x = 37$

j There does not exist $x \in \mathbb{Z}$ such that $15x \equiv 11 \pmod{33}$.

G THE CHINESE REMAINDER THEOREM

The Chinese mathematician **Sun-Tsu** posed the following problem:

> When divided by 3, a number leaves a remainder of 1. When divided by 5 it leaves a remainder of 2, and when divided by 7 it leaves a remainder of 3. Find the number.

In congruence notation, we need to find x such that $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, and $x \equiv 3 \pmod 7$.

The general method of solution of such simultaneous linear congruences in different moduli is termed the **Chinese Remainder Theorem**, named in honour of this problem and its Chinese heritage. To be fair, however, similar puzzles are also found in old manuscripts on the Indian subcontinent and in Greek manuscripts of the same era.

THE CHINESE REMAINDER THEOREM

If $m_1, m_2, m_3, ..., m_r$ are pairwise relatively prime positive integers, then the system of congruences

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $x \equiv a_3 \pmod{m_3}$, ..., $x \equiv a_r \pmod{m_r}$

has a unique solution modulo $M = m_1 m_2 m_3 .... m_r$.

This solution is $x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r \pmod M$

where $M_k = \dfrac{M}{m_k}$ and x_i is the solution of $M_i x_i \equiv 1 \pmod{m_i}$.

Proof:

Existence: Let $M_k = \dfrac{M}{m_k} = m_1 m_2 m_3 .... m_{k-1} m_{k+1} .... m_r$.

Since $\gcd(M_k, m_k) = 1$, by our theory of linear congruences it is possible to solve all r linear congruences, $M_i x_i \equiv 1 \pmod{m_i}$, $i = 1, ..., r$.

The unique solution of $M_k x_k \equiv 1 \pmod{m_k}$ is denoted x_k.

Observe that $M_i \equiv 0 \pmod{m_k}$ for $i \neq k$ since $m_k \mid M_i$ in these cases.

$$\begin{aligned}\text{Hence } a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r &\equiv a_k M_k x_k \pmod{m_k}\\ &\equiv a_k(1) \pmod{m_k}\\ &\equiv a_k \pmod{m_k}\end{aligned}$$

$\therefore$ $X \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r$ is a solution of
$x \equiv a_k \pmod{m_k}$ for $k = 1, 2, 3, ..., r$

$\therefore$ a solution exists.

Uniqueness: Suppose X' is any other integer which satisfies the system

$\therefore$ $X = a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r \equiv a_k \equiv X' \pmod{m_k}$
for all $k = 1, 2, 3, 4, ..., r$

$\therefore$ $m_k \mid (X - X')$

Since the moduli are relatively prime,

$m_1 \mid (X - X')$, $m_2 \mid (X - X')$, ..., $m_r \mid (X - X')$

$\therefore$ $m_1 m_2 m_3 .... m_k \mid (X - X')$

$\therefore$ $M \mid (X - X')$

$\therefore$ $X \equiv X' \pmod M$

Example 33

Solve Sun-Tsu's problem:

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7)$$

3, 5, and 7 are pairwise relatively prime ✓

$M = 3 \times 5 \times 7 = 105$

$\therefore \quad M_1 = \frac{105}{3} = 35, \quad M_2 = 21, \quad \text{and} \quad M_3 = 15$

To find x_1 we solve $35x_1 \equiv 1 \pmod 3 \quad \Rightarrow \quad x_1 = 2$

To find x_2 we solve $21x_2 \equiv 1 \pmod 5 \quad \Rightarrow \quad x_2 = 1$

To find x_3 we solve $15x_3 \equiv 1 \pmod 7 \quad \Rightarrow \quad x_3 = 1$

Hence, $x \equiv (1)(35)(2) + (2)(21)(1) + (3)(15)(1) \pmod{105}$

$\therefore \quad x \equiv 157 \pmod{105}$

$\therefore \quad x \equiv 52 \pmod{105}$

Check: $52 \equiv 1 \pmod 3$ ✓ $52 \equiv 2 \pmod 5$ ✓ $52 \equiv 3 \pmod 7$ ✓

So, there are infinitely many solutions, the smallest of which is $x = 52$. The other solutions are $x = 157$, $x = 209$, $x = 261$, and so on.

Example 34

Solve Sun-Tsu's problem *without* using the Chinese Remainder Theorem.

The first congruence is $x \equiv 1 \pmod 3 \qquad \therefore \quad x = 1 + 3t, \ t \in \mathbb{Z}$

Substituting into the 2nd congruence $x \equiv 2 \pmod 5$, we get

$$1 + 3t \equiv 2 \pmod 5$$
$$\therefore \quad 3t \equiv 1 \pmod 5$$
$$\therefore \quad t \equiv 2 \pmod 5$$
$$\therefore \quad t \equiv 2 + 5u, \quad u \in \mathbb{Z}$$

Substituting into the 3rd congruence $x \equiv 3 \pmod 7$, we get

$$1 + 3(2 + 5u) \equiv 3 \pmod 7$$
$$\therefore \quad 7 + 15u \equiv 3 \pmod 7$$
$$\therefore \quad 15u \equiv -4 \pmod 7$$
$$\therefore \quad 15u \equiv 3 \pmod 7$$
$$\therefore \quad u \equiv 3 \pmod 7$$
$$\therefore \quad u \equiv 3 + 7v$$

$\therefore \quad x = 1 + 3t = 1 + 3(2 + 5u) = 7 + 15u = 7 + 15(3 + 7v) = 52 + 105v$

$\therefore \quad x \equiv 52 \pmod{105}$

Some congruence equations can be solved by converting to two or more simpler equations. The following example illustrates this procedure.

Example 35

Solve $13x \equiv 5 \pmod{276}$.

We notice that $276 = 3 \times 4 \times 23$ where 3, 4, and 23 are relatively prime.

$\therefore$ an equivalent problem is to find the simultaneous solution of

$$13x \equiv 5 \pmod 3, \quad 13x \equiv 5 \pmod 4 \quad \text{and} \quad 13x \equiv 5 \pmod{23}$$
$$\therefore \; x \equiv 2 \pmod 3, \quad x \equiv 1 \pmod 4 \quad \text{and} \quad x \equiv 11 \pmod{23}.$$

Using the Chinese Remainder Theorem, $M = 3 \times 4 \times 23 = 276$

$\therefore$ $M_1 = 92$, $M_2 = 69$, and $M_3 = 12$

To find x_1 we solve $92x_1 \equiv 1 \pmod 3 \;\Rightarrow\; x_1 = 2$
To find x_2 we solve $69x_2 \equiv 1 \pmod 4 \;\Rightarrow\; x_2 = 1$
To find x_3 we solve $12x_3 \equiv 1 \pmod{23} \;\Rightarrow\; x_3 = 2$

Hence, $x = (2)(92)(2) + (1)(69)(1) + (11)(12)(2) \equiv 701 \pmod{276}$
$\equiv 149 \pmod{276}$

EXERCISE 1G

1 Solve these systems using the Chinese Remainder Theorem:

a $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod 7$

b $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$

2 When divided by 3, a positive number leaves a remainder of 2. When divided by 5 it leaves a remainder of 3, and when divided by 7 it leaves a remainder of 2. Use the Chinese Remainder Theorem to find the number.

3 Solve these systems using the Chinese Remainder Theorem:

a $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$

b $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$

4 Solve these systems *without* using the Chinese Remainder Theorem:

a $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod 7$

b $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$

c $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$

5 Solve $17x \equiv 3 \pmod{210}$ by converting into simpler congruence equations and using the Chinese Remainder Theorem.

6 Which integers leave a remainder of 2 when divided by 3, and leave a remainder of 2 when divided by 4?

7 Find an integer that leaves a remainder of 2 when divided by either 5 or 7, but is divisible by 3.

8 Find an integer that leaves a remainder of 1 when divided by 3, and a remainder of 3 when divided by 5, but is divisible by 4.

9 Colin has a bag of sweets. If the sweets were removed from the bag 2, 3, 4, 5, or 6 at a time, the respective remainders would be 1, 2, 3, 4, and 5. However, if they were taken out 7 at a time, no sweets would be left in the bag. Find the smallest number of sweets that may be in the bag.

10 Seventeen robbers stole a bag of gold coins. They divided the coins into equal groups of 17, but 3 were left over. A fight began over the remaining coins and one of the robbers was killed. The coins were then redistributed, but this time 10 were left over. Another fight broke out and another of the robbers was killed in the conflict. Luckily, another equal redistribution of the coins was exact. What is the least number of coins that may have been stolen by the robbers?

11 **a** Solve the linear Diophantine equation $4x + 7y = 5$ by showing that the congruences $4x \equiv 5 \pmod 7$ and $7y \equiv 5 \pmod 4$ are equivalent to $x = 3 + 7t$ and $y = 3 + 4s$ and finding the relationship between t and s.

b Use a similar method to solve: **i** $11x + 8y = 31$ **ii** $7x + 5y = 13$

12 Find the smallest integer $a > 2$ such that $2 \mid a$, $3 \mid (a+1)$, $4 \mid (a+2)$, $5 \mid (a+3)$, and $6 \mid (a+4)$.

13 Solve the system: $2x \equiv 1 \pmod 5$, $3x \equiv 9 \pmod 6$, $4x \equiv 1 \pmod 7$, $5x \equiv 9 \pmod{11}$.

H DIVISIBILITY TESTS

One application of congruences is determining when a large integer is divisible by a given prime. In this section we will study divisibility tests for the first 16 integers.

We will write the decimal representation of an integer A as

$A = (a_{n-1}a_{n-2}a_{n-3}....a_1a_0) = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + a_{n-3}10^{n-3} + ... + a_1 10^1 + a_0.$

If A is an integer then:

(1) $2 \mid A \Leftrightarrow a_0 = 0, 2, 4, 6, \text{ or } 8$

(2) $5 \mid A \Leftrightarrow a_0 = 0 \text{ or } 5$

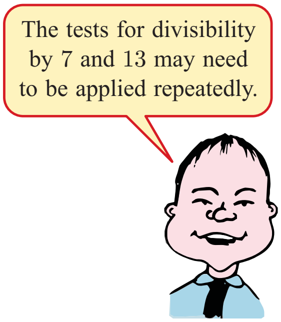
(3) $3 \mid A \Leftrightarrow 3 \mid (a_{n-1} + a_{n-2} + a_{n-3} + ... + a_1 + a_0)$

(4) $9 \mid A \Leftrightarrow 9 \mid (a_{n-1} + a_{n-2} + a_{n-3} + ... + a_1 + a_0)$

(5) $7 \mid A \Leftrightarrow 7 \mid ((a_{n-1}a_{n-2}a_{n-3}....a_2a_1) - 2a_0)$

(6) $11 \mid A \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - a_3 + ...)$

(7) $13 \mid A \Leftrightarrow 13 \mid ((a_{n-1}a_{n-2}a_{n-3}....a_2a_1) - 9a_0)$


The tests for divisibility by 7 and 13 may need to be applied repeatedly.

Proofs of some cases:

Consider the polynomial $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_0$

(1) Since $10 \equiv 0 \pmod 2$,

$f(10) \equiv f(0) \pmod 2 \qquad \{a \equiv b \pmod m \Rightarrow f(a) \equiv f(b) \pmod m\}$

$\Rightarrow A \equiv a_0 \pmod 2$

$\Rightarrow$ A is divisible by 2 if a_0 is divisible by 2

$\Rightarrow$ A is divisible by 2 if $a_0 = 0, 2, 4, 6,$ or 8.

(3) Since $10 \equiv 1 \pmod 3$,

$f(10) \equiv f(1) \pmod 3$

$\Rightarrow A \equiv a_{n-1} + a_{n-2} + ... + a_2 + a_1 + a_0 \pmod 3$

$\Rightarrow$ A is divisible by 3 $\Leftrightarrow$ $a_{n-1} + a_{n-2} + ... + a_2 + a_1 + a_0$ is divisble by 3.

(5) Let $c = (a_{n-1}a_{n-2}a_{n-3}....a_2a_1)$

$\therefore A = 10c + a_0$

$\therefore -2A = -20c - 2a_0$

$\therefore -2A \equiv c - 2a_0 \pmod 7$

Thus, $7 \mid A \Leftrightarrow 7 \mid -2A \Leftrightarrow 7 \mid c - 2a_0$

(6) Since $10 \equiv -1 \pmod{11}$,

$f(10) \equiv f(-1) \pmod{11}$

$\Rightarrow A \equiv a_0 - a_1 + a_2 - a_3 + a_4 - .... \pmod{11}$

$\Rightarrow$ A is divisible by 11 $\Leftrightarrow$ $a_0 - a_1 + a_2 - a_3 + a_4 - ....$ is divisible by 11.

Example 36

Determine whether the integer is divisible by 7:

a 259 **b** 2481

a $7 \mid 259 \Leftrightarrow 7 \mid (25 - 2(9))$
$\Leftrightarrow 7 \mid 7$
which is true, so $7 \mid 259$

b $7 \mid 2481 \Leftrightarrow 7 \mid (248 - 2(1))$
$\Leftrightarrow 7 \mid 246$
$\Leftrightarrow 7 \mid (24 - 2(6))$
$\Leftrightarrow 7 \mid 12$
which is not true, so $7 \nmid 2481$

Example 37

Is 12 987 divisible by 13?

$13 \mid 12\,987 \Leftrightarrow 13 \mid (1298 - 9(7))$
$\Leftrightarrow 13 \mid 1235$
$\Leftrightarrow 13 \mid (123 - 9(5))$
$\Leftrightarrow 13 \mid 78$ which is true as $78 = 13 \times 6$
$\therefore$ 12 987 is divisible by 13.

EXERCISE 1H

1 Let $A = 187\,261\,321\,117\,057$.
For each of $m = 2, 3, 5, 9$, and 11, find $A \pmod{m}$ and hence determine whether A is divisible by m. If it is not, state the value of the remainder of the division.

2 **a** Suppose $A = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + ... + a_2 10^2 + a_1 10 + a_0$. Prove that:

i $A \pmod{10} = a_0$ **ii** $A \pmod{100} = 10a_1 + a_0$

iii $A \pmod{1000} = 100a_2 + 10a_1 + a_0$

b Hence, state divisibility tests for 10, 100, 1000.

3 **a** Determine divisibility tests for 4 and 8.

b Postulate a divisibility test for 16.

c Find the highest power of 2 that divides:

i 201 984 **ii** 765 432 **iii** 89 375 744

iv 62 525 654 **v** 41 578 912 246 **vi** 62 525 648

4 **a** $n \pmod{10} = 0, 1, 2, 3, 4, ..., 9$. Find the possible values of $n^2 \pmod{10}$.

b Hence explain why 5437, 364 428, 65 852, and 96 853 are not perfect squares.

5 Claudia claimed that $\sum_{r=1}^{n} r!$ for $n \geqslant 4$ is never a square. Is she correct?

6 For what values of k are the repunits R_k divisible by:

a 3 **b** 9 **c** 11?

7 Determine whether either of 6994 or 6993 are divisible by: **a** 7 **b** 13

8 Write a proof for the divisibility test for 13.

9 **a** Find a divisibility test for: **i** 25 **ii** 125

b Find the highest power of 5 that divides:

i 112 250 **ii** 235 555 790 **iii** 48 126 953 125

10 Find a divisibility test for: **a** 6 **b** 12 **c** 14 **d** 15

11 Determine whether each of these integers is divisible by 11:

a 10 763 732 **b** 8 924 310 064 538 **c** 1 086 326 715

12 Determine whether each of these integers is divisible by 3, 9, or 11:

a 201 984 **b** 101 582 283 **c** 41 578 912 245

d 10 415 486 358

13 Consider an integer of the form n^2-n+7, $n \in \mathbb{Z}$. By considering different values of n, determine the possible values of its last digit. Prove that these are the only possible values.

14 For each of the following binary numbers:

i find the highest power of 2 that divides the number

ii determine whether the number is divisible by 3.

a 101 110 101 001 **b** 1 001 110 101 000 **c** 1 010 101 110 100 100

15 For each of the following ternary (base 3) numbers:

i find the highest power of 3 that divides the number

ii determine whether the integer is divisible by 2

iii determine whether the integer is divisible by 4.

a 10 200 122 221 210 **b** 221 021 010 020 120 **c** 1 010 101 110 100 100

16 Find a divisibility test for 7 when the number is written in base 8. Generalise this result to base n.

17 Find a divisibility test for 9 when the number is written in base 8. Generalise this result to base n.

18 A positive integer X has a base 25 representation given by $(x_n x_{n-1} \dots . x_0)_{25}$.

a Show that X is divisible by 5 if x_0 is divisible by 5.

b Show that X is divisible by 2 if the sum of its digits (in base 25) is even.

c Without using a conversion to base 10, determine whether or not $(664\,089\,735)_{25}$ is divisible by 20.

I FERMAT'S LITTLE THEOREM

Fermat's Little Theorem states:

If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

For example, if $a = 8$ and $p = 5$, then $8^4 \equiv 1 \pmod{5}$
which is true as $8^4 \equiv 4096$.

HISTORICAL NOTE

Pierre de Fermat corresponded on number theory with (amongst others) **Marin Mersenne** and **Bernard Frénicle**, and it was usually one of these who coaxed from the rather secretive Fermat some of his most closely held results. Frénicle is responsible for bringing Fermat's Little Theorem to notice.

Fermat communicated his result in 1640, stating also, "I would send you the demonstration, if I did not fear it being too long", a comment reminiscent of that about his Last Theorem. Fermat's unwillingness to provide proofs for his assertions was quite common. Sometimes he had a proof, other times not.

Leonhard Euler published the first proof of the Little Theorem in 1736, however **Gottfried Leibniz** (little recognised for his contributions to Number Theory due to his lack of desire to publish) left an identical argument in a manuscript dated prior to 1683.

Proof:

Consider these multiples of a: $a, 2a, 3a, 4a, ..., (p-1)a$

Suppose any two of them are congruent modulo p, so

$ka \equiv la \pmod{p}$ for $1 \leqslant k < l \leqslant p-1$.

Since p is prime we can cancel, so $k \equiv l \pmod{p}$, a contradiction.

Thus no two of the multiples are congruent modulo p, and none are congruent to 0.

$\therefore$ $a, 2a, 3a, 4a, ..., (p-1)a$ are pairwise incongruent modulo p and so they must be congruent, in some order, to the system of least residues modulo p: $1, 2, 3, 4, ..., (p-1)$.

Thus, $a(2a)(3a)(4a)....(p-1)a \equiv (1)(2)(3)(4)....(p-1) \pmod{p}$
$\therefore$ $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$

Now since $p \nmid (p-1)!$, p being prime, we can cancel by $(p-1)!$

$\therefore$ $a^{p-1} \equiv 1 \pmod{p}$

Corollary:

If p is a prime then $a^p \equiv a \pmod{p}$ for any integer a.

Proof: If $p \mid a$, then $a \equiv 0 \pmod p$ and $a^p \equiv 0^p \pmod p$

$$\therefore\ a^p \equiv a \pmod p$$

If $p \nmid a$, then by Fermat's Little Theorem

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod p \\ \therefore\ aa^{p-1} &\equiv a \pmod p \\ \therefore\ a^p &\equiv a \pmod p \end{aligned}$$

Example 38

Find the value of $3^{152} \pmod{11}$.

Since 11 is prime, and $3^{10} \equiv 1 \pmod{11}$ {FLT}

$\therefore\ 3^{152} = (3^{10})^{15} \times 3^2 \equiv 1^{15} \times 9 \equiv 9 \pmod{11}$

$\therefore\ 3^{152} \pmod{11} \equiv 9$

Fermat's Little Theorem also allows us to solve linear congruences of the form $ax \equiv b \pmod p$ where p is prime.

Notice that: if $ax \equiv b \pmod p$ then

$$\begin{aligned} \Rightarrow\ a^{p-2}ax &\equiv a^{p-2}b \pmod p \\ \Rightarrow\ a^{p-1}x &\equiv a^{p-2}b \pmod p \\ \Rightarrow\ x &\equiv a^{p-2}b \pmod p \qquad \{\text{FLT}\} \end{aligned}$$

Suppose $ax \equiv b \pmod p$ where p is prime. If $p \nmid a$, then $x \equiv a^{p-2}b \pmod p$ is the unique solution modulo p.

Example 39

Solve for x: $5x \equiv 3 \pmod{11}$

$5x \equiv 3 \pmod{11}$ where $p = 11$ is prime, $a = 5$, $b = 3$

Since $p \nmid a$, the unique solution is

$$\begin{aligned} x &\equiv 5^9 \times 3 \pmod{11} \\ \therefore\ x &\equiv (5^2)^4 \times 15 \pmod{11} \\ \therefore\ x &\equiv 3^4 \times 4 \pmod{11} \qquad \{5^2 = 25 \equiv 3 \pmod{11}\} \\ \therefore\ x &\equiv 3^3 \times 12 \pmod{11} \\ \therefore\ x &\equiv 5 \times 1 \pmod{11} \\ \therefore\ x &\equiv 5 \pmod{11} \end{aligned}$$

A further use of Fermat's Little Theorem is in determining whether an integer is *not a prime*.

The contrapositive of FLT "p prime $\Rightarrow$ $a^p \equiv a \pmod p$ for any a" is:

If $a^n \not\equiv a \pmod n$ for any $a \in \mathbb{Z}$ $\Rightarrow$ n is **not** prime.

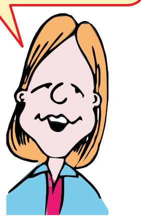
Example 40

Test whether 123 is prime.

We minimise computation by using $a = 2$.

$$\begin{aligned}
\text{Now } 2^{123} &= (2^7)^{17} \times 2^4 && \{2^7 = 128 \text{ is close to } 123\}\\
\therefore\ 2^{123} &\equiv 5^{17}2^4 \pmod{123} && \{2^7 = 128 \equiv 5 \pmod{123}\}\\
\therefore\ 2^{123} &\equiv (5^3)^5 5^2 2^4 \pmod{123} && \{5^3 = 125 \text{ is close to } 123\}\\
\therefore\ 2^{123} &\equiv 2^5 5^2 2^4 \pmod{123} && \{5^3 = 125 \equiv 2 \pmod{123}\}\\
\therefore\ 2^{123} &\equiv 2^7 \times 2^2 \times 5^2 \pmod{123} &&\\
\therefore\ 2^{123} &\equiv 5 \times 2^2 \times 5^2 \pmod{123} && \{\text{using } 2^7 \equiv 5 \pmod{123}\}\\
\therefore\ 2^{123} &\equiv 5^3 \times 2^2 \pmod{123} &&\\
\therefore\ 2^{123} &\equiv 2 \times 2^2 \pmod{123} && \{\text{using } 5^3 \equiv 2 \pmod{123}\}\\
\therefore\ 2^{123} &\equiv 2^3 \pmod{123} &&\\
\therefore\ 2^{123} &\equiv 8 \pmod{123} &&
\end{aligned}$$

Since $2^{123} \not\equiv 2 \pmod{123}$, 123 is not prime.



In most cases it is quicker to divide n by all primes $\leqslant \sqrt{n}$.

Note that the converse of Fermat's Little Theorem is false, since if $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then n need not be prime.

There exist numbers called **Carmichael numbers** which are composite and such that $a^{n-1} \equiv 1 \pmod{n}$ for all integers a such that $\gcd(a, n) = 1$.

For example, $n = 561 = 17 \times 33$ is a Carmichael number.

EXERCISE 1I

1 Use Fermat's Little Theorem to find the value of:

a $5^{152} \pmod{13}$ **b** $4^{56} \pmod{7}$ **c** $8^{205} \pmod{17}$ **d** $3^{95} \pmod{13}$

2 Use FLT to solve:

a $3x \equiv 5 \pmod{7}$ **b** $8x \equiv 3 \pmod{13}$ **c** $7x \equiv 2 \pmod{11}$ **d** $4x \equiv 3 \pmod{17}$

3 Use the method given in **Example 40** to test whether the following numbers are prime:

a 63 **b** 117 **c** 29

4 Show directly that $3^{10} \equiv 1 \pmod{11}$.

5 Use FLT to find the remainder of $13^{133} + 5$ on division by 19.

6 Use FLT to determine whether $11^{204} + 1$ is divisible by: **a** 13 **b** 17

7 Deduce by the Little Theorem that:

a $17 \mid (13^{16n+2} + 1)$ for all $n \in \mathbb{Z}^+$ **b** $13 \mid (9^{12n+4} - 9)$ for all $n \in \mathbb{Z}^+$.

8 Find the units digit of 7^{100}.

9 **a** Let p be prime and $\gcd(a, p) = 1$. Use the Little Theorem to verify that $x \equiv a^{p-2}b \pmod{p}$ is a solution of the linear congruence $ax \equiv b \pmod{p}$.

b Hence solve these systems of simultaneous congruences:

i $7x \equiv 12 \pmod{17}$, $4x \equiv 11 \pmod{19}$

ii $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, $3x \equiv 17 \pmod{29}$

10 Use the Little Theorem to prove that if p is an odd prime, then:

a $\displaystyle\sum_{k=1}^{p-1} k^{p-1} \equiv -1 \pmod{p}$ **b** $\displaystyle\sum_{k=1}^{p-1} k^{p} \equiv 0 \pmod{p}$

11 Use the Little Theorem to find the last digit of the base 7 expansion of 3^{100}.

12 In base 7, the integer X has representation $(t40\,000\,00(6-t)\,(2t)t3)_7$, which means $X = t \times 7^{11} + 4 \times 7^{10} + (6-t) \times 7^3 + (2t) \times 7^2 + t \times 7 + 3$.

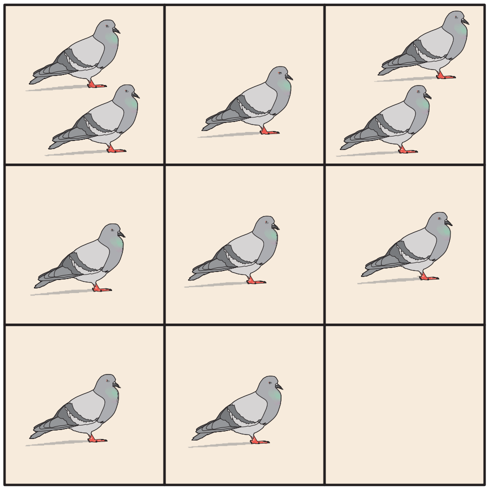
a In base 11, the representation of X is $(x_n x_{n-1} .... x_2 x_1 x_0)_{11}$, where $x_i \in \mathbb{Z}$ and $0 \leqslant x_i \leqslant 10$, $i = 0, ..., n$. Find x_0.

b For $t = 1$, find X in base 11.

13 **a** Use Fermat's Little Theorem to show that, in base 14, the last digit of an integer N equals the last digit of N^7.

b Show that this result is also true in base 21.

J THE PIGEONHOLE PRINCIPLE (DIRICHLET'S PRINCIPLE)



In the given picture there are 10 pigeons and 9 "pigeonholes".

In this case, two pigeonholes contain more than one pigeon.

Suppose the pigeons were taken out of their pigeonholes. Each pigeon is now systematically placed in a pigeonhole until they are all placed. Since the number of pigeons exceeds the number of pigeonholes, it is *guaranteed* that one of the holes will contain at least two birds.

Suppose now that 24 pigeons are placed into the 9 pigeonholes. They are placed systematically in separate pigeonholes, as far as is possible, until they are all placed.

Since $\frac{24}{9} \approx 2.33$, it is guaranteed that at least one pigeonhole will contain at least 3 pigeons.

The Pigeonhole Principle (PHP):

If n items are distributed amongst m pigeonholes with $n, m \in \mathbb{Z}^+$ and $n > m$, then:

(1) at least one pigeonhole will contain more than one item

(2) at least one pigeonhole will contain at least $\dfrac{n}{m}$ (or the smallest integer greater than $\dfrac{n}{m}$, if $\dfrac{n}{m}$ is not an integer) items.

Proof: (By contradiction)

(1) Suppose each pigeonhole contains 0 or 1 items.
$\therefore$ the total number of items in the pigeonholes is $\leqslant m < n$, a contradiction.
$\therefore$ at least one pigeonhole will contain more than one item.

(2) Suppose each pigeonhole contains less than $\dfrac{n}{m}$ items.

$\therefore$ the total number of items in the pigeonholes is $< m \times \dfrac{n}{m} = n$, a contradiction.

$\therefore$ at least one pigeonhole will contain at least $\dfrac{n}{m}$ (or the next integer greater than $\dfrac{n}{m}$, if $\dfrac{n}{m}$ is not an integer) items.

This simple and intuitive counting argument has many applications. Being able to determine when and how the pigeonhole principle can be applied is often the challenge.

Example 41

Consider a group of n people $(n > 1)$ meeting for the first time. Each person shakes hands with at least one other person. Prove there is a pair of people in the group who will shake hands the same number of times.

Each person shakes at least 1 and at most $n - 1$ hands.

$\therefore$ each person shakes $1, 2, ..., \text{or } (n - 1)$ hands. Let these possibilities be the pigeonholes.

Since there are n people, and $n > n - 1$, by the PHP at least two people are in the same pigeonhole.

$\therefore$ there is a pair of people in the group who shake hands the same number of times.

Example 42

Suppose five distinct points are arbitrarily drawn on the surface of a sphere.

Prove it is possible to cut the sphere in half so that four of the points will lie in one hemisphere. Assume that any point lying on the cut lies in both hemispheres.

Let O be the point at the centre of the sphere.

Any two of the points on the surface, together with O, define a plane which bisects the sphere.

The three remaining points lie in one or both of the two resulting hemispheres. Since $3 > 2$, by the PHP one hemisphere will contain at least two of these three remaining points. Together with the two original points chosen, this hemisphere contains at least four of the five original points.

Example 43

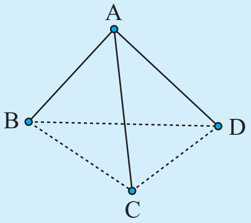
Six distinct points are arbitrarily drawn on a plane such that no three are collinear. Each pair of points is joined with a line segment called an *edge* which is coloured either red or blue.

Prove that in such a configuration it is always possible to find a triangle whose three edges have the same colour.

Choose one of the points and label it A.

Point A lies on five edges, each of which is either red or blue.

Since $\frac{5}{2} = 2.5$, by the PHP at least 3 edges through A will have the same colour. Call these edges AB, AC, and AD.



Consider the triangle formed by edges BD, BC, and CD.

If BD, BC, and CD all have the same colour, then $\triangle$BCD has all edges the same colour.

If BD, BC, and CD are not all the same colour, then both colours red and blue occur in $\triangle$BCD.

$\therefore$ one such edge will match the colour of edges AB, AC, and AD. Without loss of generality, we suppose this edge is BC.

$\therefore$ $\triangle$ABC is a triangle with all edges the same colour.

EXERCISE 1J

1 Show that in any group of 13 people there will be 2 or more people who are born in the same month.

2 Seven darts are thrown onto a circular dartboard of radius 10 cm. Assuming that all the darts land on the dartboard, show that there are two darts which are at most 10 cm apart.

3 17 points are randomly placed in an equilateral triangle with side length 10 cm. Show that at least two of the points are at most 2.5 cm away from each other.

4 10 children attended a party and each child received at least one of 50 party prizes. Show that there were at least two children who received the same number of prizes.

5 Show that if nine of the first twelve positive integers are selected at random, the selection contains at least three pairs whose sum is 13.

6 What is the minimum number of people needed to ensure that at least two of them have the same birthday (not including the year of birth)?

7 There are 8 black socks and 14 white socks in a drawer. Calculate the minimum number of socks needed to be selected from the drawer (without looking) to ensure that:

a a pair of the same colour is drawn **b** two different coloured socks are drawn?

8 Prove that for every 27 word sequence in the US constitution, at least two words will start with the same letter.

9 The capacity of Wembley stadium in London is 90 000. Prove that in a full stadium there are at least 246 people with the same birthday (not including the year of birth).

10 Prove that if six distinct numbers from the integers 1 to 10 are chosen, then there will be two of them which sum to eleven.

11 Prove that if eleven integers are chosen at random, then at least two have the same units digit.

12 Prove that, at any cocktail party with two or more people, there must be at least two people who have the same number of acquaintances at the party.

Hint: Consider the separate cases:

(1) where everyone has at least one acquaintance at the party

(2) where someone has no acquaintance at the party.

13 Draw a square of side length two units. Place five distinct points on the interior of the square. Prove that two of the points will be at most $\sqrt{2}$ units apart.

Hint: Partition the square into four congruent squares.

14 There are 25 students in a class. Each student received a score of 7, 6, 5, or 4 for a test. What is the largest number of students which are guaranteed to have the same score?

15 Are there two powers of 2 which differ by a multiple of 2001?

16 A barrel contains 5 red, 8 blue, 10 green, and 7 yellow identically shaped balls. Balls are randomly selected one by one. Find the least number of balls which must be selected to guarantee choosing:

a at least 3 red balls **b** at least 3 balls of the same colour

c at least 3 differently coloured balls.

17 Three dice are rolled and the sum total is recorded. Find the least number of rolls required to be guaranteed that a total will appear:

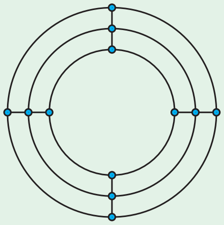
a twice **b** three times.

Graph theory 2

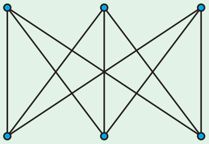
Contents:

OPENING PROBLEMS

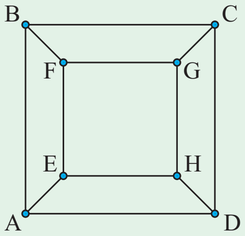
a Can you draw the diagram on the right without taking your pen from the paper and without tracing over any line more than once?
If you cannot, what is the minimum number of pen strokes that are required to draw the diagram?



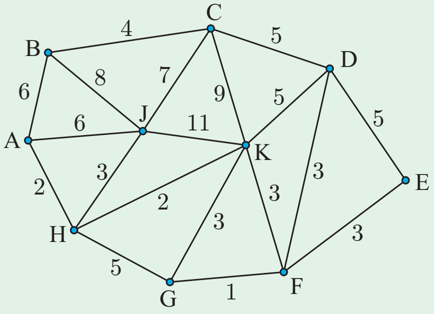
b Can you redraw the diagram on the right so that the lines (redrawn as curves if necessary) joining the points only intersect at the given points?



c Starting with point A, can you follow the lines and visit each of the dots on the diagram alongside once and once only, and then return to your starting point?



d **i** Suppose the diagram below represents an offshore oilfield. The dots represent the oil wells and the lines joining them represent pipelines that could be constructed to connect the wells. The number shown on each line is the cost (in millions of dollars) of constructing that pipeline.
Each oil well must be connected to every other, but not necessarily directly. Which pipelines should be constructed to minimise the cost? What is the minimum cost in this case?

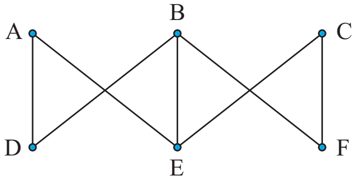


ii Now suppose the diagram in **d i** represents the walking trails in a national park. The numbers on the lines represent the suggested walk time in hours for that trail. If I want to walk from point A to point E in the shortest possible time, what route should I take?

A TERMINOLOGY

A **graph** $G = \{V, E\}$ is a finite set V of points called **vertices**, some or all of which are joined pairwise, by a finite set E of lines called **edges**.

An **edge** is an unordered pair AB of vertices A and B in the graph. Since the order of A and B is not important, the graphs we consider here are said to be **undirected**.

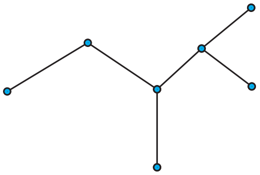


For the given graph G,
G is represented by $G = \{V, E\}$ where
$V = \{$A, B, C, D, E, F$\}$ is the **vertex set** and
$E = \{$AD, AE, BD, BE, BF, CE, CF$\}$ is the **edge set**.

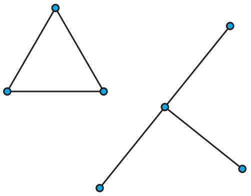
An edge AA, from a vertex A to itself, is called a **loop**.

A graph is called **simple** if it contains no loops, and if there is a maximum of one edge joining any pair of distinct vertices. For example:

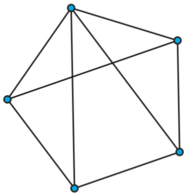
G_1:



G_2:

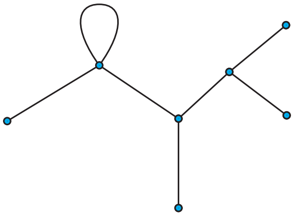


G_3:

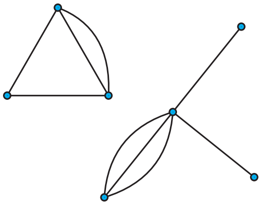


A graph is called a **multigraph** if it contains a loop and/or more than one edge connecting a pair of distinct vertices. For example:

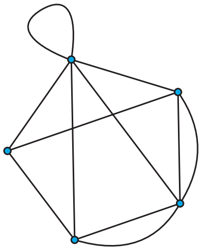
M_1:



M_2:



M_3:



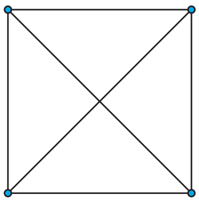
These are formal definitions of concepts you will meet in this section:

Degree of a Vertex	The number of edge endpoints incident on that vertex.
Degree Sequence	The sequence of vertex degrees for a given graph, listed in non-decreasing order.
Odd/Even Vertex	A vertex is called odd/even if its degree is odd/even.
Adjacent Vertices	Any two vertices which are joined by an edge within a graph.
Incident	An edge which connects two adjacent vertices is said to be incident on each vertex.
Adjacent Edges	Edges which are incident on a common vertex.

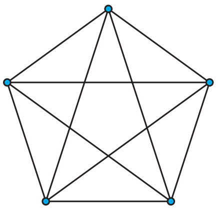
Order of a Graph	The number v of vertices in the graph.
Size of a Graph	The number e of edges in the graph.
Loop	An edge that connects a vertex to itself in a multigraph.
Connected Graph	A graph in which every vertex can be reached from every other vertex by a sequence of edges.
Complete Graph K_n	A simple graph with n vertices in which every vertex is adjacent to every other vertex.
Null Graph	A graph with no edges.
Subgraph	A graph made from a subset of the vertex set and a subset of the edge set of another graph.
Regular Graph	A graph in which every vertex has the same degree.
r-Regular Graph	A graph in which every vertex has degree r.
Graph Complement	The simple graph G' whose vertex set is the same as the given simple graph G, but whose edge set is constructed by vertices adjacent if and only if they were not adjacent in G.
Planar Graph	A graph which can be drawn in the plane with edges only crossing at vertices.
Bipartite Graph	A graph whose vertices can be divided into two disjoint sets with no two vertices of the same set being adjacent.
Complete Bipartite Graph	A simple bipartite graph which contains all possible edges.

For example, consider the following simple graphs:

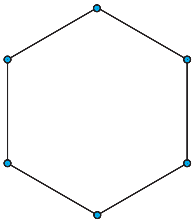
1



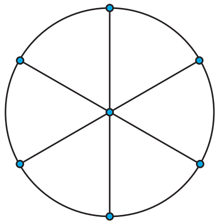
2



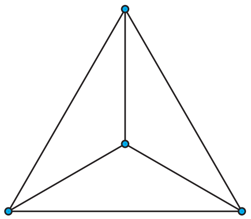
3



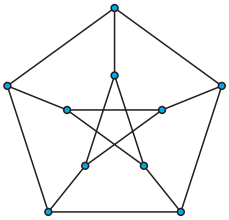
4



5



6



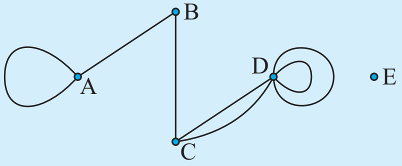
You should note the following features:

- In Graph **1** there is no vertex at the centre. The graph has 4 vertices, so its order is 4. The graph has 6 edges, so its size is 6.
- Graphs **1**, **2**, and **5** are complete, since each vertex is joined by an edge to every other vertex on the graph.
- Graph **2** is K_5, the complete graph on 5 vertices. 4 edges are incident at each vertex, so each vertex is adjacent to four vertices and has degree four. The graph is 4-regular.

- Graph **3** is denoted C_6, the **cycle graph** on 6 vertices.
- Graph **4** is W_7, the **wheel graph** on 7 vertices. It consists of a cycle of 6 vertices, plus a **hub** in the centre which is connected to every other vertex.
- Graph **5** is both W_4 and K_4.
- Graph **6** is known as the **Petersen Graph**. It is an example of a graph which is not complete, but which is regular. In this case the graph is 3-regular or **cubic**.
- Graphs **1** and **5** are both the complete graph on 4 vertices, they are just drawn differently. We say they are **isomorphic** to each other. However, note that **isomorphism** is outside the syllabus for this Option.

Example 1

Find the degree sequence of graph G shown.



$\deg(\text{A}) = 3$, $\deg(\text{B}) = 2$, $\deg(\text{C}) = 3$, $\deg(\text{D}) = 6$, $\deg(\text{E}) = 0$

$\therefore$ the degree sequence of G is 0, 2, 3, 3, 6.

Example 2

Consider the graph G shown:

a Define the graph in terms of its vertices and edges.

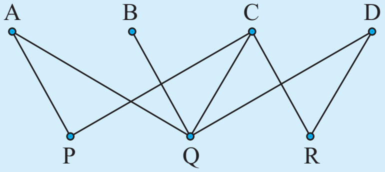
b Find the order and size of G.

c Comment on the nature of G.

d Is G planar? Explain your answer.

e Draw a subgroup of G which is:

i connected **ii** not connected.



a The graph is represented by $G = \{V, E\}$ where

$V = \{\text{A, B, C, D, P, Q, R}\}$ and

$E = \{\text{AP, AQ, BQ, CP, CQ, CR, DQ, DR}\}$

b G has 7 vertices and 8 edges.

$\therefore$ G has order $= 7$ and size $= 8$.

c G is *simple* because no vertex joins directly to itself and each pair of vertices is joined by at most one edge.

G is also *connected* since all of the vertices can be reached from all of the others.

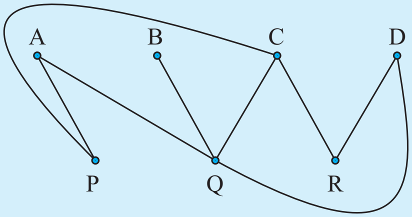
For example, A → R by an edge sequence of length 3 such as AQ, QD, DR.

The degrees of the vertices A, B, C, D, P, Q, R are 2, 1, 3, 2, 2, 4, 2 respectively. Thus the degree sequence for G is 1, 2, 2, 2, 2, 3, 4.

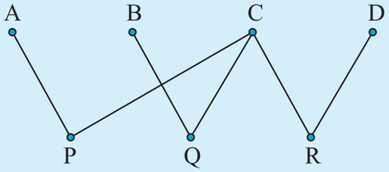
Since the degrees of the vertices are not all the same, G is not regular.

However, G is *bipartite* with the two disjoint vertex sets $V_1 = \{\text{A, B, C, D}\}$ and $V_2 = \{\text{P, Q, R}\}$.

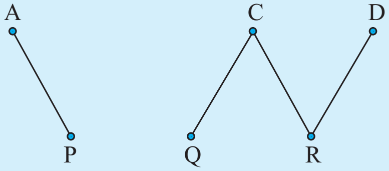
d G is *planar* since it can be drawn without any of the edges crossing, as illustrated opposite.



e **i** One connected subgraph of G is:



ii One subgraph of G which is not connected is:

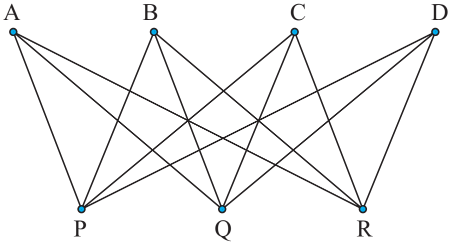


COMPLETE BIPARTITE GRAPHS

The simple graph shown opposite is a **complete bipartite graph**.

It has two disjoint vertex subsets of order 4 and 3. Each element in one vertex set is adjacent to every vertex in the other vertex set, but *not* adjacent to any vertex in the same vertex set.

The graph is denoted $K_{4,\,3}$ since there are 4 vertices in one set and 3 in the other.



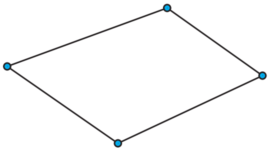
A **complete bipartite graph** $K_{m,\,n}$ has order $m+n$ and size mn.

EXERCISE 2A

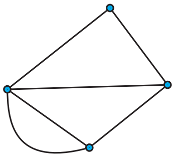
1 For each graph below, write down its:

i order **ii** size **iii** degree sequence.

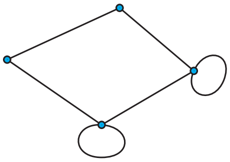
a



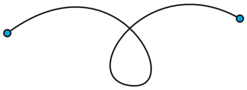
b



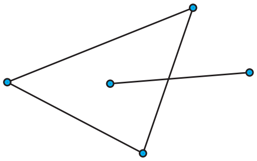
c



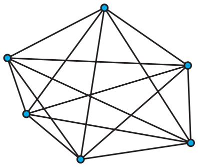
d



e



f



2 Which of the graphs in **1** are:

i simple **ii** connected **iii** complete?

3 **a** Draw:

i $G = \{V, E\}$ where $V = \{\text{A, B, C, D}\}$ and $E = \{\text{AB, BC, CD, AD, BD}\}$

ii $G = \{V, E\}$ where $V = \{\text{P, Q, R, S, T}\}$ and $E = \{\text{PQ, PR, RS, PT}\}$

iii $G = \{V, E\}$ where $V = \{\text{W, X, Y, Z}\}$ and $E = \{\text{XY, YZ, YZ, ZX, XX}\}$

iv a graph with 5 vertices, each joined to every other vertex by a single edge

v a simple, connected graph with 4 vertices and 3 edges.

b Is there more than one possible answer to **a v**? Explain your answer.

c Which of the graphs in **a** are **(1)** simple **(2)** connected **(3)** complete?

d Draw the complement of each graph **a i**, **ii**, and **iv**.

4 **a** What is the minimum number of edges a simple connected graph of order k can have?

b What is the size of the complete graph K_n of order n? What is the size of the complement of K_n?

c If G is a simple graph with order n and size e, write a formula for the size of the complement of G.

d Hence show that a simple connected graph with order n and size e satisfies the inequality $2n - 2 \leqslant 2e \leqslant n^2 - n$.

5 **a** By considering different graphs, establish a formula connecting the sum of the degrees of a graph and its size. Prove your result.

b A graph of order 7 has degree sequence 1, 2, 2, 3, 4, 5, 5. How many edges does it have?

6 Show that it is impossible to have a simple graph of order six with degree sequence 1, 2, 3, 4, 4, 5.

7 Determine whether a simple graph G can be drawn with degree sequence:

a 2, 3, 4, 4, 5 **b** 1, 2, 3, 4, 4

8 **a** Given the degrees of the vertices of a graph G, is it possible to determine its order and size?

b Given the order and size of a graph G, is it possible to determine the degrees of its vertices?

9 Wherever possible, draw an example of a simple graph with:

a no odd vertices **b** no even vertices

c exactly one vertex which has odd degree **d** exactly one vertex which has even degree

e exactly 2 odd vertices **f** exactly 2 even vertices.

10 Suppose G is a graph of order p and size q, and is r-regular with $p > r$. Express q in terms of p and r.

11 Give an example of a graph which is:

a 0-regular and not complete **b** 1-regular and not complete

c 2-regular and not complete **d** 3-regular and not complete.

12 Draw the following graphs and their complements:

a W_5 **b** $K_{3,\,3}$ **c** K_6

13 Determine the number of edges of:

a K_{10} **b** $K_{5,\,3}$ **c** W_8 **d** K_n **e** $K_{m,\,n}$

14 If possible, draw an example of:

a a bipartite graph that is regular of degree 3 **b** a complete graph that is a wheel

c a complete graph that is bipartite.

15 Describe the complement of $K_{m,\,n}$, including its size.

16 A simple graph G has the same number of vertices as edges, and the same number of edges as its complement G'. Find the order and size of G, and draw a possible example of G and its complement G'.

17 Let G be a simple graph with n vertices. Find the value of:

a order (G) + order (G')

b size (G) + size (G')

B FUNDAMENTAL RESULTS OF GRAPH THEORY

From **Exercise 2A**, you will have discovered some general results for graphs. In this section we explore and prove some of these results.

The Handshaking Lemma:

For any graph G, the sum of the degrees of the vertices in G is twice the size of G.

Proof:

Each edge has two endpoints, and each endpoint contributes one to the degree of each vertex, including edges which are loops.

$\therefore$ the sum of the degrees of the vertices in G is twice the number of edges of G, which is twice the size of G.

Result:

Any graph G has an even number of vertices of odd degree.

Proof (by contradiction):

Suppose the graph has an odd number of odd vertices.

$\therefore$ the sum of the degrees of all of the (odd and even) vertices gives a total which is odd.

However, by the Handshaking Lemma, the sum of the degrees must be twice the size of the graph, and hence is even. This is a contradiction, so it is not possible to have an odd number of odd vertices.

A vertex of odd degree is called an **odd vertex**.

Theorem:

In any *simple*, *connected* graph G, there are always at least two vertices of the same degree.

Proof:

Suppose G has n vertices. Since it is both simple and connected, the minimum degree of a vertex is 1, and maximum degree of a vertex is $n-1$.

Since there are n vertices with $n-1$ possible degrees, by the pigeonhole principle there must be at least two vertices with the same degree.

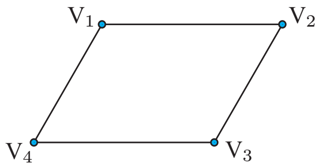
ADJACENCY TABLES

We have already seen how graphs can be represented as a list of vertices and edges. They can also be represented by **adjacency tables**.

Consider a graph $G = \{V, E\}$ of order n with vertices V_1, V_2, ..., V_n. The **adjacency table** for G is the $n \times n$ array (with n rows and n columns) such that the entry in row i and column j (called the **(i, j)th entry**) equals the number of distinct edges from vertex V_i to vertex V_j.

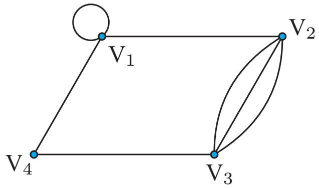
For example:

- the simple graph



has adjacency table $\begin{array}{c|cccc} & V_1 & V_2 & V_3 & V_4 \\ \hline V_1 & 0 & 1 & 0 & 1 \\ V_2 & 1 & 0 & 1 & 0 \\ V_3 & 0 & 1 & 0 & 1 \\ V_4 & 1 & 0 & 1 & 0 \end{array}$ or simply $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

- the multigraph



has adjacency table: $\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 3 & 0 \\ 0 & 3 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

Note that in some other treatments of graph theory, each loop contributes 2 to the value of the relevant entry on the main diagonal. Here, each loop contributes only 1.

PROPERTIES OF ADJACENCY TABLES

1 An adjacency table is **symmetric** about the main diagonal, since vertex V_i is adjacent to vertex V_j $\Leftrightarrow$ vertex V_j is adjacent to vertex V_i, for all $i \neq j$.

2 For **simple graphs**, the sum of the entries in any row (or column) equals the degree of the corresponding vertex.

$\therefore$ using the Handshaking Lemma, the sum of all entries in the adjacency table equals twice the size of the graph.

3 For **multigraphs**, the sum of the entries in any row (or column) not on the main diagonal, plus twice the entry on the main diagonal, equals the degree of the corresponding vertex.

$\therefore$ the sum of all entries on or below the main diagonal of the adjacency table equals the size of the graph.

EXERCISE 2B

1 Which of these adjacency tables cannot represent a graph?

a $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

b $\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

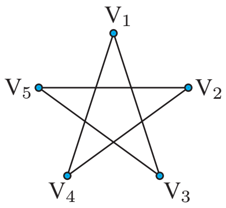
c $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

2 Consider the adjacency table $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

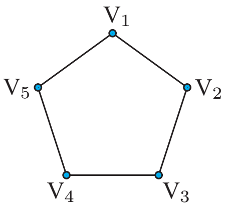
Draw the corresponding graph. Verify that the total number of 1s in the matrix equals the sum of the degrees of the vertices.

3 Determine the adjacency table for each graph:

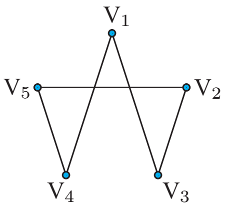
a



b



c



4 **a** Construct a graph for each adjacency table:

i $\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$ **ii** $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

b Find the complement of each graph in **a**, and write down the adjacency table for the complement.

c For a simple graph G, explain how the adjacency table for the complement G' of G can be obtained from the adjacency table of G.

5 Find the size of the graph G with adjacency table:

a $\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$ **b** $\begin{pmatrix} 3 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 2 \end{pmatrix}$

6 Represent each of the following graphs using an adjacency table:

a K_4 **b** C_4 **c** W_4 **d** $K_{1,\,4}$ **e** $K_{2,\,3}$

7 Find the form of the adjacency table for each of the following graphs:

a K_n **b** C_n **c** W_n **d** $K_{m,\,n}$

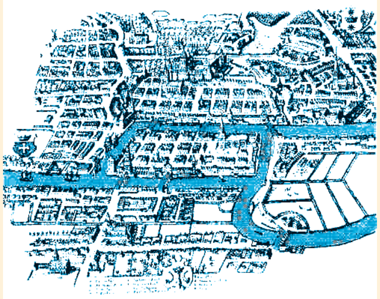
C JOURNEYS ON GRAPHS

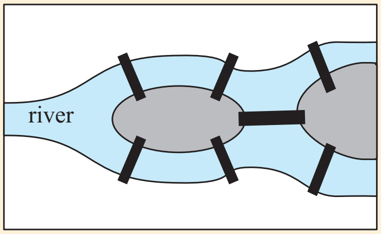
Having defined what a graph is, we now consider various ways of moving from vertex to vertex along the edges of a graph. For example, we may have to visit every vertex on our journey, or travel along every edge, or take account of the time it takes to traverse a given set of edges.

As we do this, we consider the work of two of the founding mathematicians of Graph Theory, **Leonard Euler** and **William Hamilton**, and introduce the two classic problems their work eventually gave rise to.

INVESTIGATION 1 THE BRIDGES OF KÖNIGSBERG

One of Euler's most famous contributions to mathematics concerned the town of Kaliningrad, or Königsberg as it was then known. The town is situated on the river Pregel in what was then Prussia, and has seven bridges linking two islands and the north and south banks of the river. A simplified map is shown alongside.





What to do:

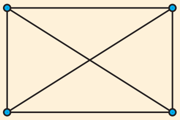
1 Can a tour be made of the town, returning to the original point, that crosses all of the bridges once only?

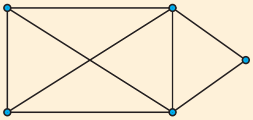
2 Euler determined that such a circuit is not possible. However, it would be possible if either one bridge was removed or one was added.

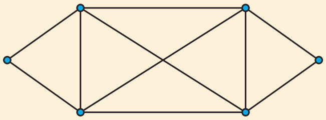
  a Which bridge would you remove?

  b Where on the diagram would you add a bridge?

3 The Bridges of Königsberg question is closely related to children's puzzles in which a graph can or cannot be drawn without the pen leaving the paper or an edge being drawn twice. If such a drawing can be made, the graph is said to be **traversable**. Note that in this case, the start and end points may or may not be the same vertex.
Which of these are traversable?







TERMINOLOGY

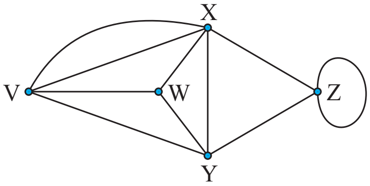
A **walk** is a finite sequence of linked edges.

We begin the walk at the **initial vertex** and end it at the **final vertex**. The **length** of the walk is the total number of steps (or times an edge is traversed) in the walk.

A walk can be described by its vertices and edges or (if there is no ambiguity) by listing only vertices or only edges.

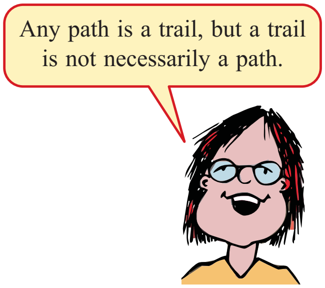
In the multigraph alongside, a walk of length 6 might be V → W → Y → Z → Z → Y → X.

In a walk, any vertex may be visited any number of times and any edge may be used as often as one wishes.



A **trail** is a walk where *all of the edges are distinct.* Vertices may be visited as often as one wishes, but once an edge has been used it may not be used again.

A **path** is a walk where *all vertices are distinct.*



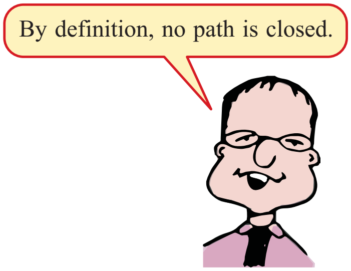
For example, in the multigraph above:

- X → V → W → Y → Z → X → Y is a trail of length 6
- V → W → Y → X and W → X → V → Y → Z are paths of length 3 and 4 respectively.

A walk or trail is said to be **closed** if the initial and final vertices are the same.

A closed trail is called a **circuit**.

A **cycle** is a circuit with only one repeated vertex, and this is both the initial and final vertex.



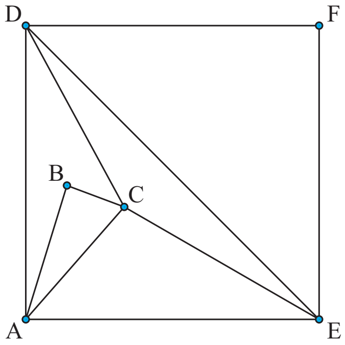
For example, in the multigraph above:

- The loop Z → Z is a cycle of length 1.
- V → X → V using the distinct edges is a cycle of length 2.
- V → W → Y → X → Z → Y → V is a circuit.
- W → X → Y → W and X → Y → W → X and X → W → Y → X all represent the same cycle, since they all contain the same set of edges.

EXERCISE 2C.1

1 For the given graph, find, if possible:

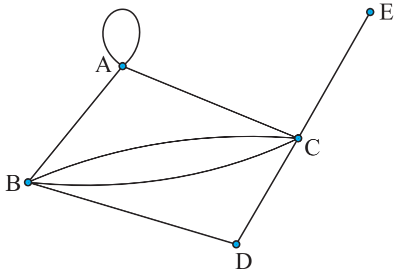
- **a** a path of length 2 from A to D
- **b** a path of length 3 from A to D
- **c** a path of length 4 from A to D
- **d** a trail which is not a path, of length 5 from B to D
- **e** a cycle of length 5
- **f** a cycle of length 7
- **g** a circuit which is not a cycle, of length 7
- **h** a circuit of length 10.



2 Consider the given graph. Find, if possible:

a a trail which includes every edge of the graph

b a circuit which includes every edge of the graph.



EULERIAN GRAPHS

An **Eulerian Trail** is a trail which uses every edge in the graph exactly once. If such a trail exists, the graph is **traversable**.

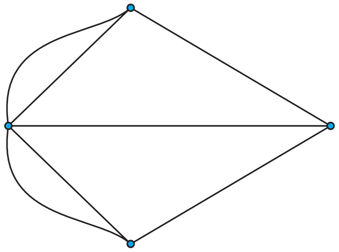
An **Eulerian Circuit** is an Eulerian trail which is a circuit.

A graph is **Eulerian** if it contains an **Eulerian circuit**.

A graph is **semi-Eulerian** if it contains an **Eulerian trail** but not an **Eulerian circuit**.

The Bridges of Königsberg problem attempts to find an Eulerian circuit of the corresponding graph shown.

Notice that the degree of each vertex is odd. This is why no Eulerian circuit is possible.



Theorem:

If a graph contains *any* vertices of odd degree, it is not Eulerian.

Proof:

For a graph to contain an Eulerian circuit, each vertex must be entered by an edge and left by another edge which is not a loop.

Therefore, if there is an odd vertex, then at least one edge from the vertex is unused, and the graph is not Eulerian.

Euler was also able to prove the (more difficult) converse of this statement as well. We are hence able to state the following results:

Theorem:

A connected graph is **Eulerian** if and only if all of its vertices are even.

Corollary:

A connected graph is semi-Eulerian if and only if exactly two of its vertices are odd.

Proof of Corollary:

$(\Rightarrow)$ Suppose the connected graph $G = \{V, E\}$ is traversable with $V_1V_2....V_n$ an Eulerian trail which is not a circuit.

The edge $V_1V_n \notin E$ since the trail uses all edges in E and the trail is not a circuit.

Consider the graph $G \cup \{V_1V_n\}$ of graph G with edge V_1V_n added to it.

Then $G \cup \{V_1V_n\}$ has an Eulerian circuit, namely $V_1V_2....V_nV_1$.

By the above theorem, the degree of each vertex in $G \cup \{V_1V_n\}$ is even.

$\therefore$ each vertex of the original graph G has even degree, except V_1 and V_n which have odd degree. The two vertices of odd degree are necessarily the endpoints of the Eulerian trail.

$(\Leftarrow)$ Suppose the connected graph $G = \{V, E\}$ has exactly two vertices V_1, V_2 each of odd degree. By the above theorem, G is not Eulerian.

Consider the graph $G \cup \{V_1V_2\}$ of graph G with edge V_1V_2 added to it.

Then the graph $G \cup \{V_1V_2\}$ has all vertices of even degree.

By the above theorem, $G \cup \{V_1V_2\}$ has an Eulerian circuit, which necessarily uses edge V_1V_2.

$\therefore$ the original graph G contained an Eulerian trail with endpoints V_1 and V_2, but not an Eulerian circuit.

$\therefore$ G is semi-Eulerian.

We can formalise the definition of a connected graph as follows:

A graph is **connected** if and only if there is a path between each pair of vertices.

Theorem:

A *simple* graph is bipartite if and only if each circuit in the graph is of even length.

Theorem:

A simple connected graph G with n vertices and e edges satisfies $n-1 \leqslant e \leqslant \frac{1}{2}n(n-1)$.

Proof:

K_n, the complete graph on n vertices, has the maximum number of edges for a simple graph on n vertices. The number is $\frac{1}{2}n(n-1)$.

$\therefore$ $e \leqslant \frac{1}{2}n(n-1)$.

Suppose V_1V_2 is an edge in G. Since the graph is connected, each of the remaining $n-2$ vertices are connected to V_1 or V_2 by a path of length $\geqslant 1$. Thus the graph must contain at least $n-2$ distinct edges, in addition to edge V_1V_2.

$$\therefore \quad e \geqslant n - 2 + \underset{\substack{\uparrow \\ \text{edge } V_1V_2}}{1} = n - 1.$$

Thus $n-1 \leqslant e \leqslant \frac{1}{2}n(n-1)$, as required.

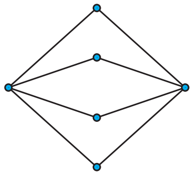
Corollary:

Any simple graph with n vertices and more than $\frac{1}{2}(n-1)(n-2)$ edges is connected.

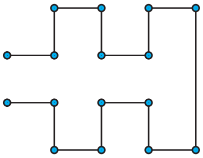
EXERCISE 2C.2

1 Classify the following as Eulerian, semi-Eulerian, or neither:

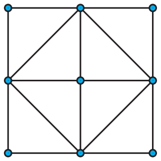
a



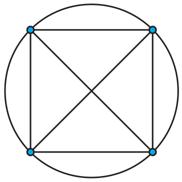
b



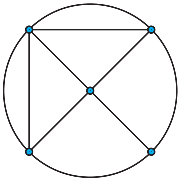
c



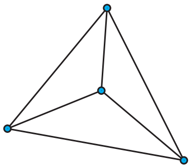
d



e



f



2 Give an example of a graph of order 7 which is:

a Eulerian b semi-Eulerian c neither

3 Decide whether the following graphs are Eulerian, semi-Eulerian, or neither:

a K_5 b $K_{2,\,3}$ c W_n d C_m

4 For which values of:

a n is K_n Eulerian b m, n is $K_{m,\,n}$ Eulerian?

5 A *simple* graph G has five vertices, and each vertex has the same degree d.

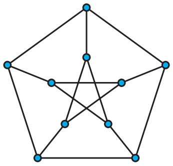
a State the possible values of d.

b If G is connected, what are the possible values of d?

c If G is Eulerian, what are the possible values of d?

6 The **girth** of a graph is defined as the length of its shortest cycle.
Find the girth of:

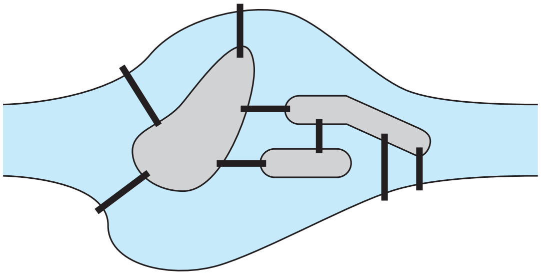
a K_9 b $K_{5,\,7}$ c the Petersen graph



7 Consider the Bonnigskerb bridge problem opposite.

a Can a circular walk be performed?

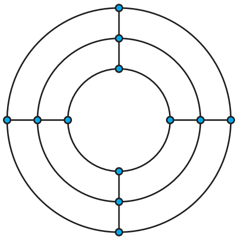
b Would either the addition or deletion of one bridge allow a circular walk to be performed?



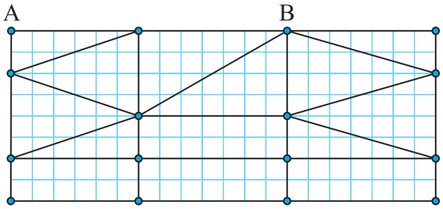
8 Show that is is possible to transform any connected graph G into an Eulerian graph by the addition of edges.

9 **a** How many continuous pen strokes are needed to draw the diagram on the right, without repeating any line segment between the given points?

b How is this problem related to Eulerian graphs?



10 Suppose you have a job as a road cleaner. The diagram of the roads to be cleaned is drawn to scale alongside.



a Is it possible to begin at A, clean every road exactly once, and return to A?

Is it possible to begin at B, clean every road exactly once, and return to B?

b Suppose that you have to begin and end your sweeping duties at A, so you will have to drive down some streets more than once. If your speed never varies, what is the most efficient way of completing your task?

11 Prove that a simple graph is bipartite if and only if each circuit in the graph is of even length.

12 Prove that any simple graph with n vertices and more than $\frac{1}{2}(n-1)(n-2)$ edges is connected. A diagram may be useful.

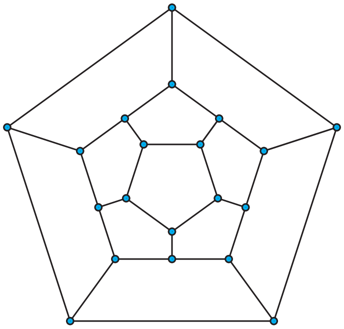
HAMILTONIAN GRAPHS

William Rowan Hamilton invented a game known as **The Icosian Game**. It was sold for £25 by Hamilton and was marketed as "Round the World". It essentially required finding a closed trail on the dodecahedron.

A picture of the game can be found at:

www.puzzlemuseum.com/month/picm02/200207icosian.htm

A **Schlegel** diagram is a graph whose edges do not cross, which is drawn to represent a 3-dimensional solid.



A Schlegel diagram of the dodecahedron in the Icosian game is shown opposite.

Is it possible, starting and finishing at the same vertex, to follow the edges and visit every other vertex exactly once without lifting the pen?

There are, in fact, two solutions!

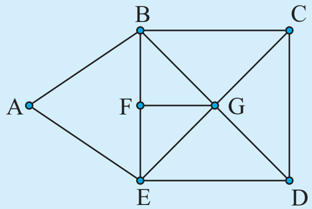
A graph is said to be **Hamiltonian** if there exists a cycle that passes through every vertex on the graph. Such a cycle is called a **Hamiltonian cycle**.

If a path exists that passes through every vertex on the graph exactly once then the graph is said to be **semi-Hamiltonian**. The path is called a **Hamiltonian path**.

Note that loops and multiple edges are irrelevant when determining whether a Hamiltonian path or cycle exists within a graph. Thus it is sufficient to consider simple graphs.

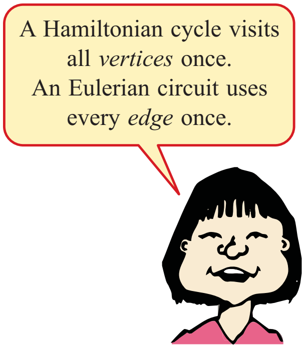
Example 3

Given the diagram alongside, does a Hamiltonian cycle exist?



Yes, there are several.

For example, G → F → B → A → E → D → C → G


A Hamiltonian cycle visits all *vertices* once.
An Eulerian circuit uses every *edge* once.

We have seen that for a graph to be Eulerian, all vertices must have even degree. By contrast, we cannot give a precise set of conditions for a graph to be Hamiltonian. However, we can state the following important theorems concerning Hamiltonian graphs:

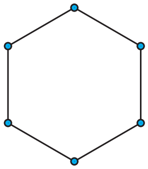
1 If G is a simple graph of order n, where $n \geqslant 3$, and if degree (V) + degree (W) $\geqslant n$ for each pair of non-adjacent vertices V and W, then there exists a Hamiltonian cycle. (**Ore**, 1960)

2 If G is a simple graph of order n, where $n \geqslant 3$, and if each vertex has degree $\geqslant \frac{1}{2}n$, then there exists a Hamiltonian cycle. (**Dirac**, 1952)

3 If G is a simple graph of order n, where $n \geqslant 3$, with at least $\frac{1}{2}(n-1)(n-2)+2$ edges, then there exists a Hamiltonian cycle.

Note that while these are all *sufficient* conditions for the existence of a Hamiltonian cycle, they are not *necessary*.

For example, in the graph of order 6 alongside, each vertex has degree 2 and the graph is Hamiltonian.



Proof of 1:

For cases $n \geqslant 5$, we use a proof by contradiction.

Suppose that G is a simple graph of order $n \geqslant 5$ which does not contain a Hamiltonian cycle, and for which $\deg(\text{V}) + \deg(\text{W}) \geqslant n$ for each pair of non-adjacent vertices V, W in G.

Note that K_n is Hamiltonian, so G is necessarily a subgraph of K_n and $G \neq K_n$, and therefore G has less than $\frac{1}{2}n(n-1)$ edges.

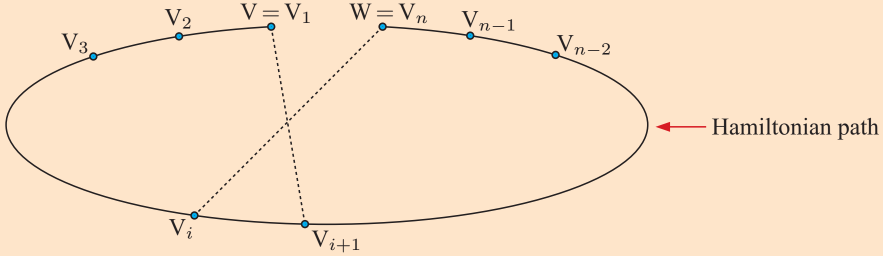
Without loss of generality we consider such a graph G, with the maximum possible number of edges so that the addition of a new edge results in a Hamiltonian graph.

Suppose vertices V, W are non-adjacent in G.

Let VW be a new edge and consider the graph $G \cup \{\mathrm{VW}\}$ which is necessarily Hamiltonian.

Then G has a Hamiltonian path from V to W, namely the Hamiltonian cycle of $G \cup \{\mathrm{VW}\}$ with edge VW deleted.
Suppose this Hamiltonian path is $\mathrm{V} = \mathrm{V}_1 \longrightarrow \mathrm{V}_2 \longrightarrow \mathrm{V}_3 \longrightarrow .... \longrightarrow \mathrm{V}_{n-2} \longrightarrow \mathrm{V}_{n-1} \longrightarrow \mathrm{V}_n = \mathrm{W}$.

We now consider the $(n-1)$ pairs of consecutive vertices $\{\mathrm{V}_i, \mathrm{V}_{i+1}\}$ for $i = 1, ..., n-1$, and check whether V is adjacent to V_{i+1}, and whether W is adjacent to V_i.



For any i, at most one of these adjacencies can occur, because if both occur G would contain the Hamiltonian cycle $\mathrm{V} \longrightarrow \mathrm{V}_2 \longrightarrow .... \longrightarrow \mathrm{V}_i \longrightarrow \mathrm{W} \longrightarrow \mathrm{V}_{n-1} \longrightarrow .... \longrightarrow \mathrm{V}_{i+1} \longrightarrow \mathrm{V}$.

But this means that $\deg(\mathrm{V}) + \deg(\mathrm{W}) \leqslant n-1$, which contradicts $\deg(\mathrm{V}) + \deg(\mathrm{W}) \geqslant n$.

So, G must contain a Hamiltonian cycle.

For $\boldsymbol{n = 3}$, a graph G satisfying the premise is necessarily K_3, which is Hamiltonian.

For $\boldsymbol{n = 4}$, a graph G satisfying the premise has C_4 as a subgraph, so it is Hamiltonian.

Proof of 2:

A graph G satisfying the premise of **2** must also satisfy the conditions of **1**, and is therefore Hamiltonian.

Proof of 3:

Suppose V, W are two non-adjacent vertices in G.

Consider a subgraph H of G which is the graph G with vertices V, W removed and all edges incident with V or W removed.

Note that since G is simple, H is simple and H is a subgraph of K_{n-2}.

$\therefore$ the number of edges in $K_{n-2} \geqslant$ the number of edges in H

$$\therefore \quad \frac{(n-2)(n-3)}{2} \geqslant \text{the number of edges in } G - \deg(\mathrm{V}) - \deg(\mathrm{W})$$

$$\therefore \quad \deg(\mathrm{V}) + \deg(\mathrm{W}) \geqslant -\frac{(n-2)(n-3)}{2} + \frac{(n-1)(n-2)}{2} + 2$$

$$\therefore \quad \deg(\mathrm{V}) + \deg(\mathrm{W}) \geqslant \frac{(n-2)}{2}[n-1-(n-3)] + 2$$

$$\therefore \quad \deg(\mathrm{V}) + \deg(\mathrm{W}) \geqslant \frac{(n-2)}{2} \times 2 + 2$$

$$\therefore \quad \deg(\mathrm{V}) + \deg(\mathrm{W}) \geqslant n$$

Hence G satisfies the conditions of **1**, and is therefore Hamiltonian.

EXERCISE 2C.3

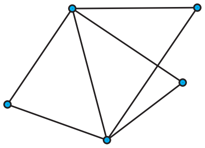
1 State whether each of the following graphs is Hamiltonian (and therefore also semi-Hamiltonian) or semi-Hamiltonian only:

a K_5

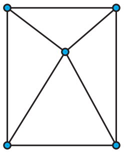
b $K_{2,\,3}$

c W_6

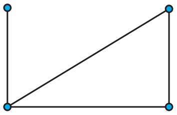
d



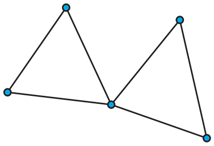
e



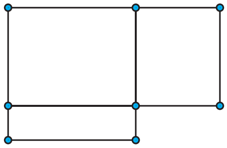
f



g



h



2 Which of the graphs in **1** satisfy any of the three theorems about Hamiltonian graphs?

3 Give examples of graphs which are:

a both Hamiltonian and Eulerian

b Hamiltonian but not Eulerian

c Eulerian but not Hamiltonian

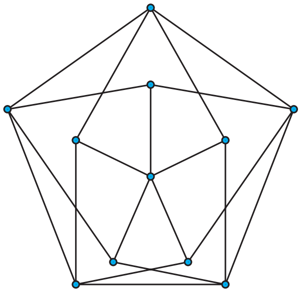
d semi-Hamiltonian and semi-Eulerian, but neither Hamiltonian nor Eulerian.

4 What are the conditions on m and n so that $K_{m,\,n}$ is Hamiltonian?

5 **a** Prove that K_n is Hamiltonian for all $n \geqslant 3$.

b How many distinct Hamiltonian cycles does K_n have?

6 Show that the Groetsch graph shown alongside is Hamiltonian.



7 **a** Prove that if G is a bipartite graph with an odd number of vertices, then G is not Hamiltonian.

b Deduce that the graph alongside is not Hamiltonian.

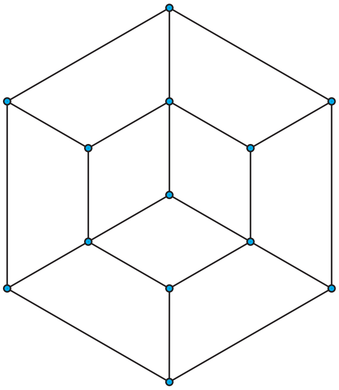
c Show that if n is odd, it is not possible for a knight to visit all of the squares on an $n \times n$ chessboard exactly once and return to its starting point.

d Give an example of a connected bipartite graph with an even number of vertices, which is:

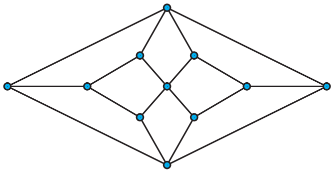
i Hamiltonian

ii semi-Hamiltonian but not Hamiltonian

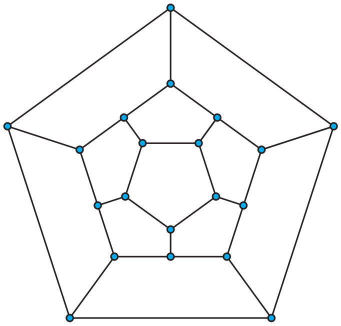
iii neither Hamiltonian nor semi-Hamiltonian.



8 Is it possible to find a Hamiltonian cycle in the Herschel graph alongside?



9 Find a Hamiltonian cycle for the dodecahedron. Trace it out on its Schlegel diagram.



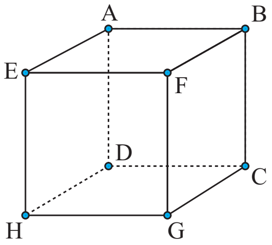
PRINTABLE DIAGRAMS

D PLANAR GRAPHS

A graph G is **planar** if it can be drawn in the plane without any edge crossing another.

Such a representation of the graph is called an **embedding** of the graph in the plane, or a **plane representation**.

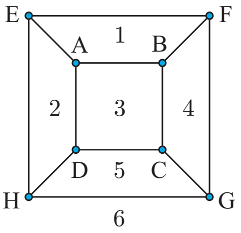
The property of planarity is important in the study of the class of three-dimensional solids known as **polyhedra**.



A **polyhedron** is a solid with flat or plane faces such as the cuboid alongside.

This is a two-dimensional perspective representation of a three-dimensional solid. It is also a graph. However, is it a *planar* graph?

The answer is yes, since the Schlegel diagram opposite shows the same vertex-edge incidence structure as the cuboid, but with edges which only meet at a vertex.



Note that the regions 1, 2, 3, 4, 5, and 6 (of infinite area) represent the **faces** of the cuboid.

Planar graphs can hence be described by their vertices and edges, and also by the regions (called **faces**) which they define in the plane.

For a planar graph we define the **degree of a face** to be the minimum number of edges in a closed walk around the border of the face.

Example 4

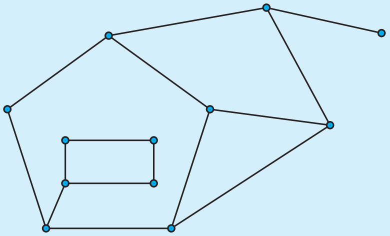
For the given connected planar graph G, find:

a the number of vertices v

b the number of edges e

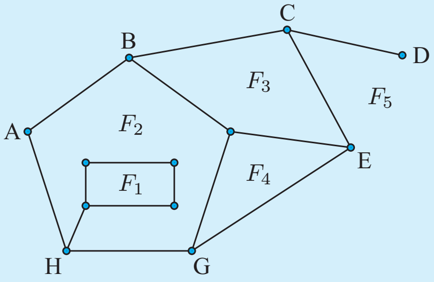
c the number of faces f

d the degree of each face.



a $v = 12$ **b** $e = 15$ **c** $f = 5$

d Label the faces F_1, F_2, F_3, F_4, F_5 as shown.
F_5 is the infinite face.
$\deg(F_1) = 4$, $\deg(F_2) = 11$,
$\deg(F_3) = 4$, $\deg(F_4) = 3$,
$\deg(F_5) = 8$

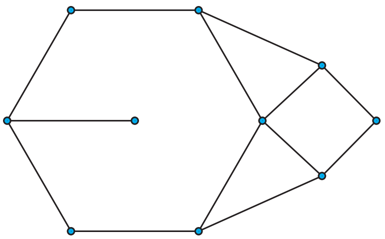


Note that a closed walk around the border of F_5 is for example
D → C → B → A → H → G → E → C → D,
with edge CD traversed twice.

EXERCISE 2D.1

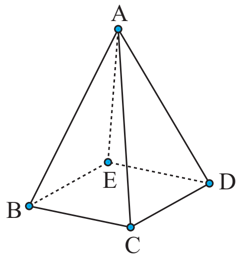
1 For the given connected planar graph, find:

- **a** the number of vertices v
- **b** the number of edges e
- **c** the number of faces f
- **d** the degree of each face.

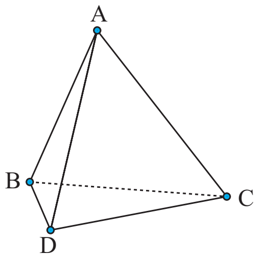


2 Represent the given polyhedra using a graph with a plane representation.

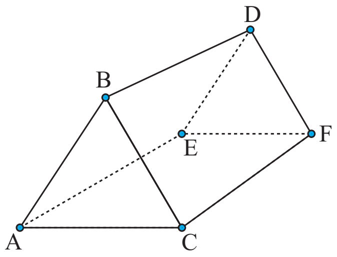
a



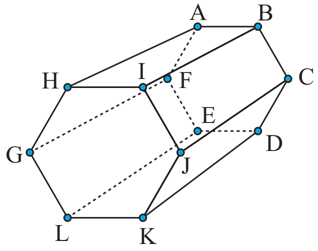
b



c

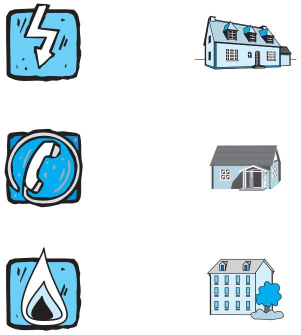


d



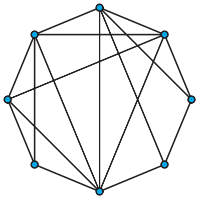
3 The following **utilities problem** is a famous problem based on planar graphs. The task is to connect each of the three houses to each of the three services electricity, telephone, and gas, with no pipes or cables crossing.

- **a** Can the problem be solved?
- **b** Could the problem be solved if we drew the houses and services on the surface of a cylinder or sphere rather than in the plane?

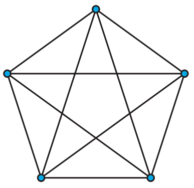


4 Decide whether each graph is planar or non-planar. Where possible, draw a plane representation of the graph.

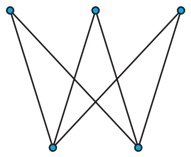
a



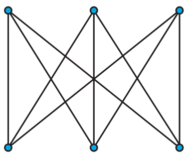
b



c



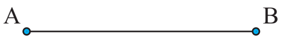
d



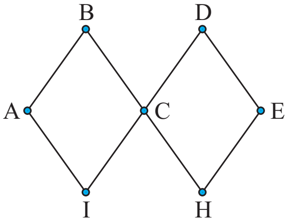
5 For each given graph:

- **i** Find a closed walk of minimum length around the border of the infinite face.
- **ii** Find the degree of each face.
- **iii** Verify that $\sum\limits_{F \text{ a face of } G} \deg(F) = 2e$.

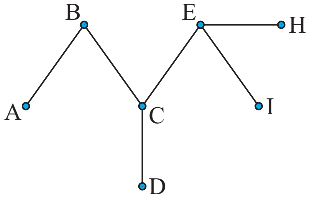
a



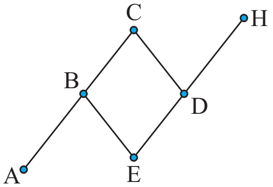
b



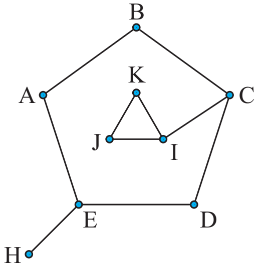
c



d



e



6 Prove that for any planar graph G with e edges, $\sum\limits_{F \text{ a face of } G} \deg(F) = 2e$.

INVESTIGATION 2 EULER'S FORMULA

Euler found a relationship for any **connected** planar graph between its number of vertices v, edges e, and faces f.

What to do:

1 Copy and complete the table alongside using the graphs from questions **2** and **5** in the previous **Exercise**.

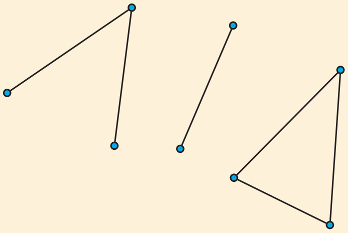
v	e	f

2 Using your table as a basis, suggest Euler's result.

3 Prove your result by induction, using the number of edges and the following steps:

- **a** Let your basic case be the graph K_2 and verify your result.
- **b** Now, add an edge to K_2 in as many different ways as you can. Note how this addition affects the number of vertices and/or faces, but does not affect the formula. This will be the inductive step.
- **c** Perform the inductive step on an arbitrary graph of size k for which Euler's relation is assumed to hold. Hence complete your proof.

4 There is a similar relation for *disconnected* planar graphs. Let n be the number of separate parts of the graph. For example, in the graph opposite, $n = 3$, $v = 8$, $e = 6$, and $f = 2$.



- **a** Determine a rule for this situation.
- **b** Prove your result by induction.

Euler's Formula:

If a connected graph G is planar with v vertices, e edges, and f faces, then it satisfies Euler's formula $e + 2 = f + v$.

Consider again the **utilities problem** in **Exercise 2D.1** question **3**, which is equivalent to asking whether the complete bipartite graph $K_{3,\,3}$ is planar. We can now use Euler's formula to prove it is not planar, and hence that the **utilities problem** is not solvable.

Example 5

Prove by contradiction that $K_{3,\,3}$ is not planar.

Suppose $K_{3,\,3}$ is planar.

Since $K_{3,\,3}$ has 6 vertices and 9 edges, by Euler's formula it must have 5 faces.

But $K_{3,\,3}$ is also bipartite, so none of the faces in its plane representation are triangles.

$\therefore$ each face has at least 4 edges, so if we count the edges around all 5 faces, we obtain at least $4 \times 5 = 20$.

In doing this we have counted each edge twice, since every edge is on the border of two faces.

$\therefore$ $K_{3,\,3}$ has at least $\frac{20}{2} = 10$ edges.

This is a contradiction, since $K_{3,\,3}$ has only 9 edges.

$\therefore$ $K_{3,\,3}$ is not a planar graph.

EXERCISE 2D.2

1 Prove by contradiction that K_5 is not planar.

2 Prove that if a simple connected graph with $v \geqslant 3$ vertices is planar, then $e \leqslant 3v - 6$.

3 Prove that if a connected planar graph is such that each face has degree $\geqslant 4$, then $e \leqslant 2v - 4$.

4 Prove that if a simple connected bipartite graph is planar, then $e \leqslant 2v - 4$.

5 In **2**, **3**, and **4**, you established the two inequalities $e \leqslant 2v - 4$ and $e \leqslant 3v - 6$. They state that for a set number of vertices, there is an upper bound on the number of edges before they have to start crossing each other.

- **a** Verify by substitution into these inequalities that K_5 and $K_{3,\,3}$ are not planar.
- **b** Show that these inequalities do not help to determine whether or not K_4 and $K_{2,\,3}$ are planar.
- **c** Show that K_4 and $K_{2,\,3}$ are planar by drawing appropriate plane representations.

6 Prove that if the length of the shortest cycle in a connected planar graph is 5, then $3e \leqslant 5v - 10$. Hence deduce that the Petersen graph is non-planar.

7 The **girth** g of a graph is the length of its shortest cycle. Establish a general inequality involving e, v, and g for connected simple planar graphs, using a similar counting technique to that used in **2** and **3**.

8 Using the inequality $e \leqslant 3v - 6$:

- **a** prove that in a simple connected planar graph with $v \geqslant 3$, there exists at least one vertex of degree less than or equal to 5
- **b** determine which complete graphs K_n are planar.

9 Draw a connected planar graph in which each vertex has degree 4.

10 Prove that all complete bipartite graphs of the form $K_{2,\,n}$ are planar.

11 For which values of $s, t > 1$ is the complete bipartite graph $K_{s,\,t}$ not planar?

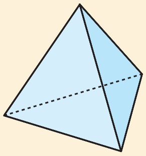
12 Prove that for a simple connected graph G with at least 11 vertices, G and its complement G' cannot both be planar.

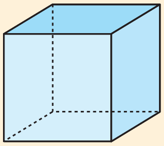
Hint: Consider the total number of edges in both G and G' and then use the inequality from **2**.

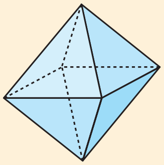
INVESTIGATION 3 PLATONIC SOLIDS

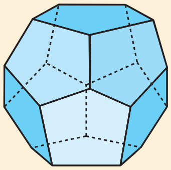
Platonic solids are regular polyhedra whose faces are all the same shape. Their existence has been known since the time of the ancient Greek civilisation.

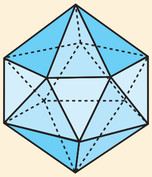
There are exactly five platonic solids: the tetrahedron, cube, octahedron, dodecahedron, and icosahedron.


Tetrahedron


Cube


Octahedron


Dodecahedron


Icosahedron

In this Investigation, we prove that there are only five platonic solids using Euler's formula and the fact that all platonic solids are planar.

Suppose that a regular polyhedron P under consideration has v vertices, e edges, and f faces. Since P is planar, we have Euler's relation $v - e + f = 2$.

P is also regular, so the degree of each vertex is the same. We let the degrees be p, where $p \geqslant 3$.

Each region of the graph of P has the same shape. We let the number of sides in each region be q, where $q \geqslant 3$.

$\Rightarrow \; pv = qf = 2e$.

What to do:

1 Show that $8 = v(4-p) + f(4-q)$.

2 Since v and f are both positive, $(4-p)$ and $(4-q)$ cannot both be negative.

$\therefore$ either $4 - p \geqslant 0$ or $4 - q \geqslant 0$

$\therefore$ $3 \leqslant p \leqslant 4$ or $3 \leqslant q \leqslant 4$, though not necessarily both together.

We now have four cases to investigate: $p = 3$, $p = 4$, $q = 3$, and $q = 4$ and we must consider each of these in turn to complete our proof.

a For the case $p = 3$, use $qf = 3v = 2e$ and the modified Euler relation derived in **1** to show $f(6 - q) = 12$, $f, q \in \mathbb{Z}^+$.

Using the factors of 12, we consider the separate cases from this equation:

- $f = 1 \quad \Rightarrow \quad q < 0$ which is invalid
- $f = 2 \quad \Rightarrow \quad q = 0$ which is invalid {a region without edges}
- $f = 3 \quad \Rightarrow \quad q = 2 \Rightarrow v = 2$ which is invalid {3 vertices required for a region}
- $f = 4 \quad \Rightarrow \quad q = 3 \Rightarrow v = 4, \; e = 6$ a tetrahedron
- $f = 6 \quad \Rightarrow \quad q = 4 \Rightarrow v = 8, \; e = 12$ a cube
- $f = 12 \quad \Rightarrow \quad q = 5 \Rightarrow v = 20, \; e = 30$ a dodecahedron

b For the case $p = 4$, use $qf = 4v = 2e$ and the modified Euler relation to show that $f(4 - q) = 8$, $f, q \in \mathbb{Z}^+$. Hence show that an octahedron is a platonic solid.

c Repeat **b** for the cases $q = 3$ and $q = 4$.

Having considered all cases, you should now have proven there are exactly five platonic solids.

3 Draw a Schlegel diagram for each platonic solid.

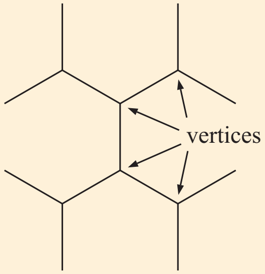
4 Draw a Hamiltonian path on each Schlegel diagram.

INVESTIGATION 4 SOCCER BALLS

Soccer balls are constructed by stitching together regular pentagons and regular hexagons. They may therefore be described as **semi-regular polyhedrons**.

If you look carefully at one of these balls, you will find it has exactly 12 pentagons. In the Investigation we find out why.

Suppose our soccer ball is a polyhedron constructed from p pentagons and h hexagons.



What to do:

1 Write down an expression for f, the number of faces in the graph of polyhedron, in terms of p and h.

2 **a** How many edges do the pentagons have in total?

b How many edges do the hexagons have in total?

c How many edges does the graph of the polyhedron have in total? Call this number e. Be careful to count each edge only once.

3 Given that each face meets with two other faces at a vertex, find a formula for v, the total number of vertices of the graph of the polyhedron.

4 Use Euler's rule to complete the proof.

5 There is no restriction on the number of hexagons. In fact, we do not need to use any. What shape would we obtain if we used only pentagons?

6 If we used pentagons and squares, would we end up with 12 pentagons and an unrestricted number of squares?

7 Prove that a soccer ball cannot be "tiled" out of hexagons alone.

EXTENSION

Click on the icon to obtain an extension section on **homeomorphic graphs** and **Kuratowski's theorem**.

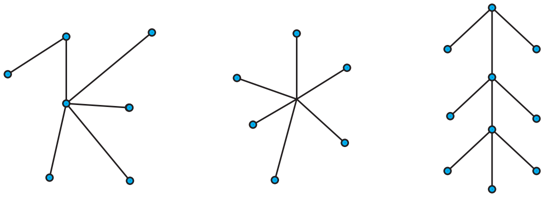
HOMEOMORPHIC GRAPHS

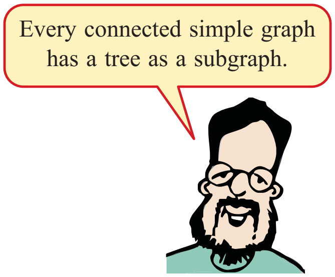
E TREES AND ALGORITHMS

A **tree** is a connected, simple graph with no circuits or cycles. We say it is **acyclic**.

The vertices in a tree are sometimes called **nodes**.

Some examples of trees are shown below:





A **spanning tree** is a connected subgraph with no cycles and which contains all the vertices of the original graph.

Theorem:

A graph G is connected if and only if it possesses a spanning tree.

Proof:

$(\Leftarrow)$ If G has a spanning tree T, then by definition T is connected and contains all the vertices in G.

$\therefore$ since G contains all the edges in T, G is also connected.

$(\Rightarrow)$ If G is connected, then *either*:

- G is a tree, in which case it is its own spanning tree, *or*
- G contains cycles. In this latter case, we can keep deleting edges of G without deleting vertices until it is impossible to continue without disconnecting G. At this time, we are left with a spanning tree of G.

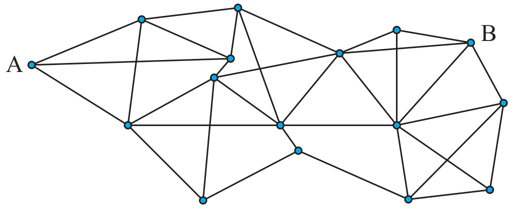
Note that it is possible for a graph to have many distinct spanning trees.

For example, consider the graph G and one of its spanning trees shown.

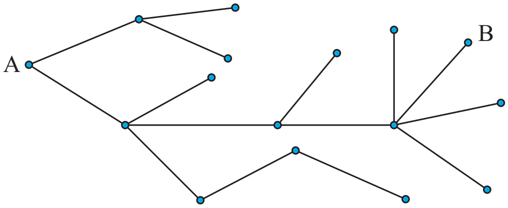
In the spanning tree:

- There are 16 vertices, so its order is 16.
- There are 15 edges, so its size is 15.
- There is one path only from A to B.
- If we delete any edge from the tree, then the graph would be disconnected.
- If we add an edge without adding a vertex, then the resulting graph has a cycle.

Graph G



Example spanning tree of G.



PROPERTIES OF TREES

The following properties of trees are all equivalent and may each be used to establish whether or not a given graph is a tree.

1 A simple graph T is a tree if and only if any two of its vertices are connected by exactly one path.

Proof:

$(\Rightarrow)$ If T is a tree then it is connected. Hence there exists a path between any two vertices.

Suppose there is more than one distinct path between two vertices.

$\therefore$ the paths are somewhere disjoint, and the disjoint sections of path create a cycle.

But T is acyclic, so we have a contradiction.

Thus in any tree there is a unique path between any two vertices.

$(\Leftarrow)$ Suppose T is a simple graph such that there exists a unique path between every pair of vertices. T is connected, and it is acyclic since otherwise there would exist two paths between two vertices.

$\therefore$ T is a tree.

2 A graph T is a tree if and only if it is connected and the removal of any one edge results in the graph becoming disconnected.

Proof:

$(\Rightarrow)$ If T is a tree, then by property **1**, any edge is the unique path between the two incident vertices.

$\therefore$ removing this edge disconnects the graph.

$(\Leftarrow)$ Suppose T is a connected graph and the removal of any edge results in a disconnected graph.

If T contains a cycle, then we can remove at least one further edge without the graph becoming disconnected, a contradiction.

$\therefore$ T is connected and acyclic, and is therefore a tree.

3 If graph T has order n, T is a tree if and only if it contains no cycles, and has $n-1$ edges.

Proof:

$(\Rightarrow)$ If T is a tree of order n, then by definition it contains no cycles.

Now if T has order 2, then T is K_2, which indeed has only 1 edge.

Now suppose that all trees with k vertices have $k-1$ edges.

Adding one edge to the tree without making a cycle requires us to add another vertex. We hence form a tree with $k+1$ vertices and k edges.

$\therefore$ by induction, a tree of order n has $n-1$ edges.

$(\Leftarrow)$ Suppose T is a graph with n vertices, $n-1$ edges, and no cycles.

Since there are no cycles, there exists no more than one path between any two vertices.

Now if T is disconnected, suppose it is made up of k connected subgraphs, $k>1$, none of which contains a cycle.

$\therefore$ T is made up of k components, each of which is a tree, by result **1**.

But we have just proved that a tree with m vertices has $m - 1$ edges, so for k disconnected trees with a total of n vertices, the total number of edges is $n - k$.

Hence $k = 1$, which is a contradiction.

$\therefore$ T must be connected, and since it contains no cycles, it is a tree.

4 If graph T has order n, T is a tree if and only if it is connected and has $n - 1$ edges.

Proof:

$(\Rightarrow)$ If T is a tree of order n, then by definition it is connected and acyclic.

Now if T has order 2, then T is K_2, which indeed has only 1 edge.

Now suppose that all trees with k vertices have $k - 1$ edges.

Adding one vertex to the tree without the tree becoming disconnected requires us to add another edge.

Hence we form a tree with $k + 1$ vertices and k edges.

$\therefore$ by induction, a tree of order n has $n - 1$ edges.

$(\Leftarrow)$ Let G be a connected graph with n vertices and $n - 1$ edges.

If G contains a cycle, then we can delete an edge from the graph to form a connected subgraph of G with the same number of vertices as G. We can continue this process r times $(r > 0)$ until we obtain a tree T with n vertices and $n - 1 - r$ edges.

However, we know that a tree with n vertices has $n - 1$ edges, so $r = 0$.

This is a contradiction, so G must be acyclic.

$\therefore$ since G is connected and acyclic, it is a tree.

5 A graph T is a tree if it contains no cycles and if the addition of any new edge creates exactly one cycle.

Proof:

If T is a tree, then by definition it is connected and contains no cycles.

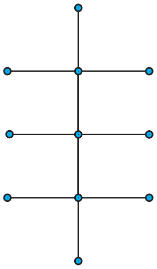
If we add an edge between two existing vertices A and B, then there are now exactly two paths from A to B.

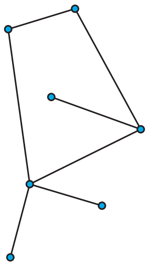
$\therefore$ there is now a single cycle which starts and finishes at A, and travels in either direction via B. The cycle through B is the same cycle since it contains the same set of edges.

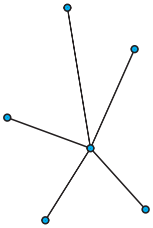
Hence exactly one cycle is created.

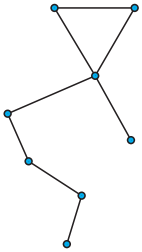
EXERCISE 2E.1

1 Which of the graphs below are trees?

a


b


c


d


2 Find all essentially distinct trees of order 6.

3 Can a complete graph be a tree? Explain your answer.

4 a Find the sum of the degrees of the vertices of a tree of order n.

b A tree has two vertices of degree 4, one of degree 3, and one of degree 2. All other vertices have degree 1.

i How many vertices does it have? ii Draw the tree.

c A tree has two vertices of degree 5, three of degree 3, and two of degree 2. All other vertices have degree 1.

i How many vertices does it have? ii Draw the tree.

5 Draw a tree with six vertices of degree 1, one vertex of degree 2, one vertex of degree 3, and one vertex of degree 5.

6 Which complete bipartite graphs $K_{m,\,n}$ are trees?

7 Show that for $n > 2$, any tree on n vertices has at least two vertices of degree one.

FINDING A SPANNING TREE: THE BREADTH FIRST SEARCH

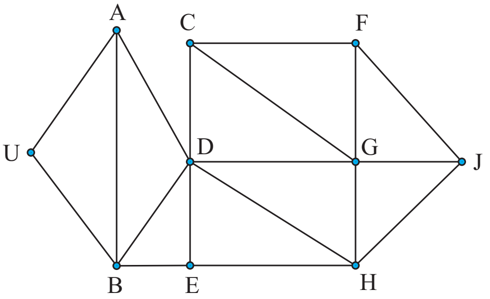
These are two algorithms for finding a spanning tree of a given connected graph in as efficient a way as possible. These are the **depth first search** and the **breadth first search**. In this course we consider only the **breadth first search** algorithm:

From a given starting vertex, we visit all adjacent vertices. Then for each of these vertices, we visit all the adjacent vertices except those we have already been to, and so on until we have visited all vertices.

For example, for the graph alongside:

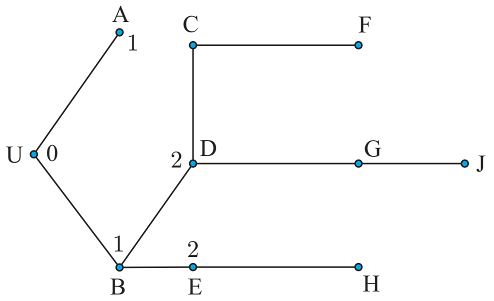
1 We choose a starting vertex, U. We label vertex U with 0, since it is 0 steps from itself.

2 We move to the vertices adjacent to U. These are A and B. We label them 1, because they are both 1 step from U.



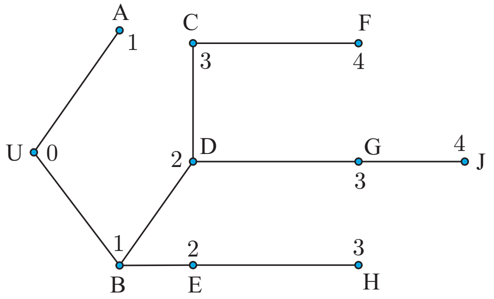
3 Next, we choose one of these two adjacent vertices. We choose B for no particular reason and move to the as yet *unlabelled* vertices adjacent to B. These are D and E, and we label them both 2 because they are both two steps from U. We repeat this with the *unlabelled* vertices adjacent to A, but in this case there are none.

Note that by moving only to the unlabelled vertices we ensure that we do not form a circuit.



4 All unlabelled vertices adjacent to those labelled with a 2 are labelled 3, as they are 3 steps from U and cannot be reached in less than 3 steps.

The process is continued until all vertices have been reached. We end up with the spanning tree shown alongside.



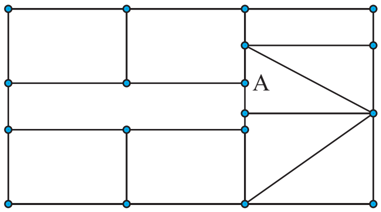
Note that:

- This spanning tree is not unique, because we could choose a different start vertex, or different orders in which to visit the adjacent vertices.
- Since a spanning tree exists if and only if the original graph is connected, this algorithm can be used to *test* whether or not a graph is connected. If the graph is not connected, we can never label all vertices.
- The BFS algorithm tells us the minimum number of edges on the path from the starting point to any other vertex on the graph.

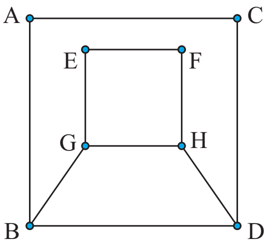
EXERCISE 2E.2

1 Starting at A, find spanning trees for these graphs:

a



b



PRINTABLE DIAGRAMS

2 How many different spanning trees are there for C_n, $n \geqslant 3$, with vertices labelled V_1, V_2, ..., V_n?

3 **a** For each of the following graphs, draw the different possible spanning tree configurations. Assume that the vertices of the graphs are unlabelled.

i K_2 **ii** K_3 **iii** K_4 **iv** K_5 **v** K_6

b Now suppose the vertices of the graph K_n are labelled $\text{V}_1, \text{V}_2, ..., \text{V}_n$.

i Count the number of spanning trees of each type for K_n, $n = 2, 3, 4, 5, 6$, and hence find the total number of spanning trees.

ii Postulate a formula for the total number of spanning trees for K_n, for $n \geqslant 2$.

4 **a** For each of the following graphs, draw the different possible spanning tree configurations. Assume that the vertices of the graphs are unlabelled.

i $K_{1,\,1}$ **ii** $K_{2,\,2}$ **iii** $K_{3,\,3}$

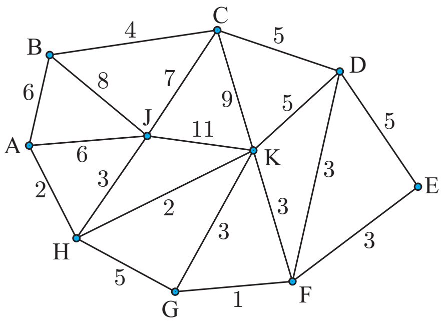
b Conjecture a formula for the number of spanning trees for $K_{n,\,n}$ with vertices labelled $\text{V}_1, ..., \text{V}_n, \text{W}_1, ..., \text{W}_n$, given that the total number of spanning trees for $K_{4,\,4}$ is 4096.

5 Conjecture a formula for the number of spanning trees of $K_{m,\,n}$ with vertices labelled $\text{V}_1, ..., \text{V}_m, \text{W}_1, ..., \text{W}_n$.

WEIGHTED GRAPHS

An undirected **weighted graph** is one in which a numerical value called a **weight** is given for each edge of the graph.

We will consider two types of problems for weighted graphs. These correspond to the situations we described in the **Opening Problem d** on page **90**. Both situations related to the weighted graph alongside.



Situation 1: The nodes represent oil wells and the edges represent pipelines. The weights represent the cost of constructing that pipeline. Each oil well must be connected to every other in a way which minimises the total cost.

We must therefore find a **minimum weight spanning tree** of the graph. The algorithm we consider for finding the spanning tree of minimum weight is **Kruskal's Algorithm**.

Situation 2: The edges represent the walking trails in a national park. The weights represent the suggested walk time in hours for that trail. We wish to find the shortest route from point A to point E. We therefore seek the minimum weight path, called the **minimum connector**, between the two given points. In this case we use **Dijkstra's Algorithm**.

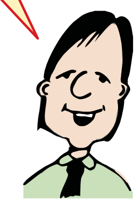
KRUSKAL'S ALGORITHM

In **Kruskal's algorithm**, we choose edges one at a time, taking the edge of least weight at every stage while ensuring that no cycles are formed. For a graph of order n, the minimum weight spanning tree is obtained after $n-1$ successful choices of edge.

Step 1: Start with the shortest (or **least weight**) edge. If there are several, choose one at random.

Step 2: Choose the shortest edge remaining that does not complete a cycle. If there is more than one possible choice, pick one at random.

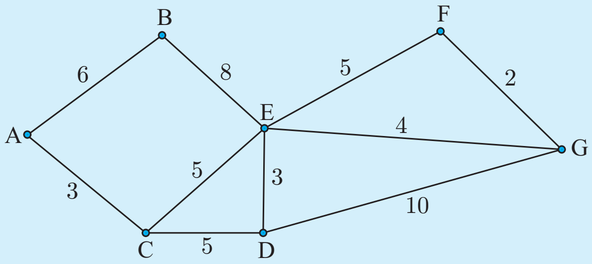
Step 3: Repeat *Step 2* until $n-1$ edges have been chosen.



Kruskal's algorithm is used to find a minimum weight spanning tree.

Example 6

Use Kruskal's algorithm to find the minimum weight spanning tree of the graph given.

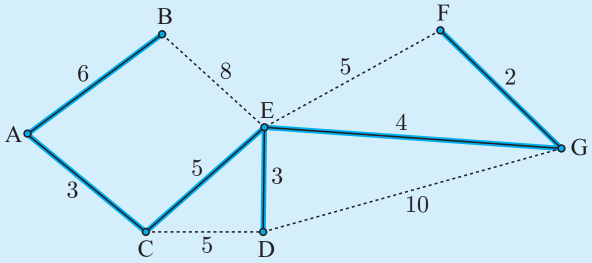


There are 7 vertices, so we require 6 edges. Edge FG has the shortest length.

Edge	*Length*	*Circuit*	*Edge List*	*Total Length*
FG	2	No	FG	2
DE	3	No	FG, DE	5
AC	3	No	FG, DE, AC	8
EG	4	No	FG, DE, AC, EG	12
EF	5	Yes - reject	FG, DE, AC, EG	12
CE	5	No	FG, DE, AC, EG, CE	17
CD	5	Yes - reject	FG, DE, AC, EG, CE	17
AB	6	No	FG, DE, AC, EG, CE, AB	23

We have 6 edges, so we stop the algorithm.

The minimum weight spanning tree has total weight 23, and is shown below.



In this case the minimum spanning tree is not unique. We could have chosen CD instead of CE.

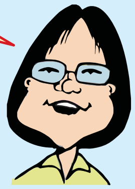


TABLE FORM FOR A WEIGHTED GRAPH

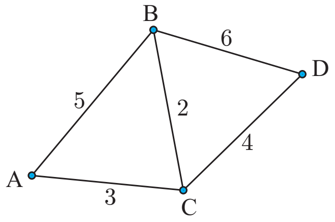
In this section we see how weighted graphs can be represented using tables. This form is useful for graphs with a large number of vertices, since we can then use a computer programme to perform our search.

The table form for the graph alongside is

	A	B	C	D
A	X	5	3	X
B	5	X	2	6
C	3	2	X	4
D	X	6	4	X

or

	A	B	C	D
A	-	5	3	-
B	-	-	2	6
C	-	-	-	4
D	-	-	-	-



where an X or - indicates that the two vertices (for the given row and column) are not adjacent. For adjacent vertices the corresponding entry is the weight of the edge.

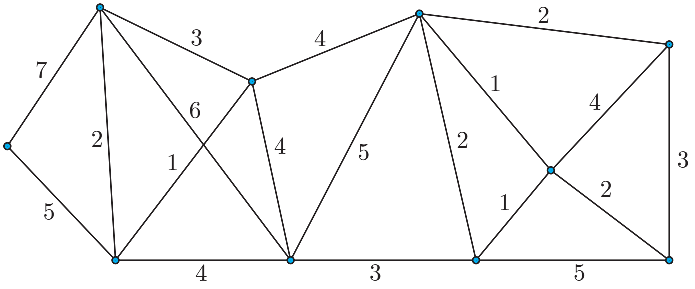
For undirected graphs the form on the left is symmetric about the main diagonal and therefore the form on the right contains all the necessary information required to construct or reconstruct the weighted graph.

EXERCISE 2E.3

1 Solve the **Opening Problem d i** on page **90** using the Kruskal algorithm.

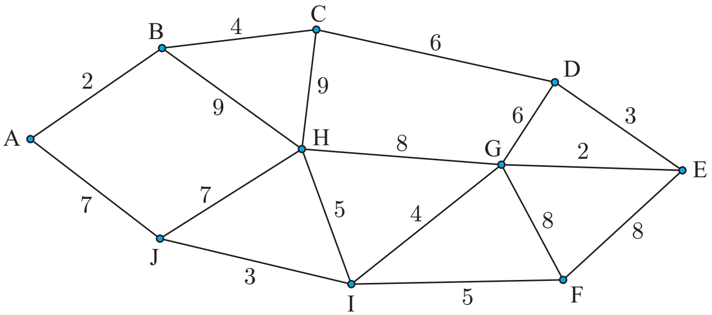
2 Find minimum weight spanning trees of the following graphs using the Kruskal algorithm.

a



PRINTABLE DIAGRAMS

b



3 The table represents a weighted complete graph.

a How do we know it is a complete graph?

b Draw the graph.

c Use Kruskal's algorithm to find a minimum weight spanning tree for the graph.

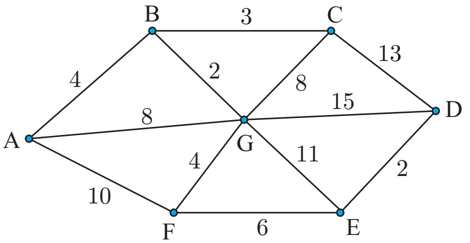
	A	B	C	D	E
A	X	10	8	7	10
B	10	X	5	4	9
C	8	5	X	7	10
D	7	4	7	X	8
E	10	9	10	8	X

4 Draw the weighted graph and find a minimum weight spanning tree for the network represented by the table opposite:

	A	B	C	D	E	F	G
A	X	X	30	X	X	50	45
B	X	X	70	35	40	X	X
C	30	70	X	50	X	X	20
D	X	35	50	X	10	X	15
E	X	40	X	10	X	15	X
F	50	X	X	X	15	X	10
G	45	X	20	15	X	10	X

THE MINIMUM CONNECTOR PROBLEM

The graph shows the shipping lanes between seven ports. The edge weights represent the estimated sailing time in days between the ports. A ship's captain wants to find the quickest route from A to D.



Problems with small graphs such as this, can usually be solved by inspection. In this case the quickest time is 18 days using either A → B → G → F → E → D
or A → F → E → D.

However, real life problems generally require much larger and more involved graphs that can only be sensibly handled using computers. Finding optimum paths through such graphs requires an algorithm or set of rules that can be programmed into a computer.

Finding efficient algorithms for this and other graph theory tasks is an active area of research, for they are used in areas as diverse as cancer research and electrical engineering.

In this course, we find the minimum weight path between two given vertices on a weighted connected graph using **Dijkstra's algorithm**.

It is important that for this algorithm to work, all weights on the graph must be non-negative. This is generally realistic anyway, since the cost, distance, or time of travelling along an edge would not be negative.

DIJKSTRA'S ALGORITHM

A starting vertex must be chosen or nominated.

Step 1: Assign a value of 0 to the starting vertex. We draw a box around the vertex label and the 0 to show the label is permanent.

Step 2: Consider all unboxed vertices adjacent to the latest boxed vertex. Label them with the minimum weight from the starting vertex via the set of boxed vertices.

Step 3: Choose the least of *all* of the unboxed labels on the *whole* graph, and make it permanent by boxing it.

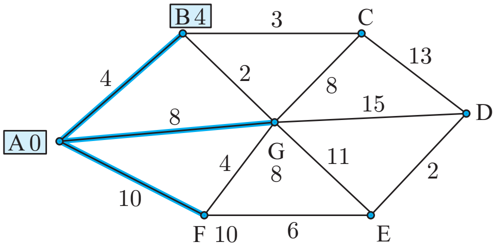
Step 4: Repeat *Steps 2* and *3* until the destination vertex has been boxed, then backtrack through the set of boxed vertices to find the shortest path through the graph.

In each stage we try to find the path of minimum weight from a given vertex to the starting vertex. We can therefore discard previously found shortest paths as we proceed, until we have obtained the path of minimum weight from the start to the finishing vertex.

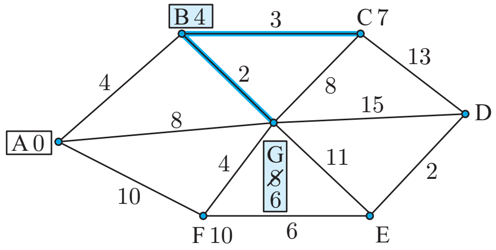
We will now apply Dijkstra's algorithm to the example on the previous page:

Begin by labelling A with 0 and drawing a box around it. Label the adjacent vertices B, G, and F with the weights of the edges from A.

The weight of edge AB is least, so we draw a box around B and its label.

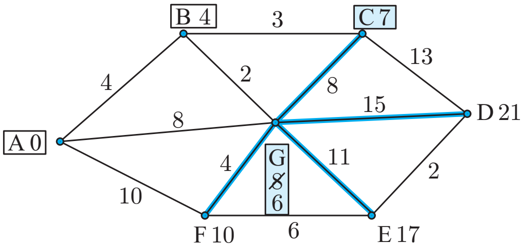


Next we consider moving from B to all adjacent vertices. These are C, which has cumulative minimum weight 7, and G, which has cumulative minimum weight via B of 6. We therefore label C with 7, and replace the 8 next to G with a 6 since the minimum weight path from A to G is via B, with weight 6. We know it is the minimum because it is the least of the unboxed labels on the graph. Therefore, we put a box around the G and the 6.



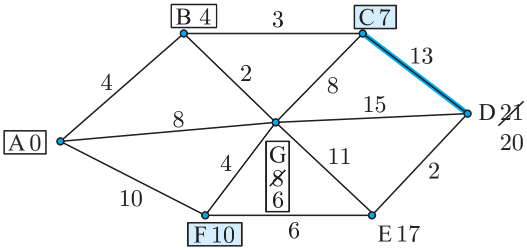
Now C is unboxed and adjacent to G, but $6 + 8 = 14 > 7$. We therefore do not update the label. We also label D with 21, E with 17, and F is labelled with 10. Notice that the minimum path of weight 10 from A to F is obtained by either A → B → G → F or A → F direct.

Of the new options, C is the least and is therefore boxed.

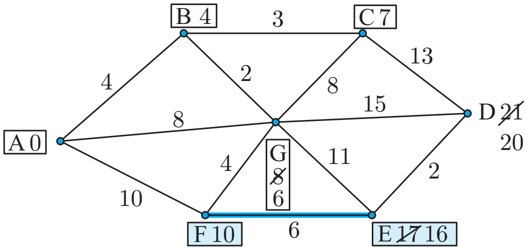


We now consider all unboxed vertices adjacent to C. We can update D from 21 to 20.

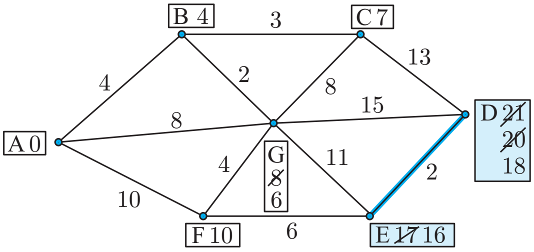
We choose the least of all of the unboxed labels on the whole graph. This is the 10 corresponding to F, so F is the next vertex to be boxed.



We can now update E to 16, and box it because it now has the lowest unboxed label.



Finally, we update D to 18, and we are now sure that the lowest label is attached to the final destination. The algorithm stops, and its completed diagram is shown opposite:



To complete the route, we have to back-track from D to A using the final boxed labels. We have 18 units (and no more) to use, so we have to retrace steps back through E and F. From F, we can either return directly to A, or return via G and B. We therefore have the two solutions, each of weight 18, that were found by inspection:

A → B → G → F → E → D and A → F → E → D.

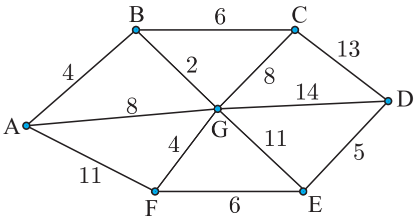
Note two unusual features of this example that do not occur in most problems:

- All vertices were considered. In general, the algorithm stops as soon as the destination vertex is boxed, irrespective of whether all other vertices have been considered. This is because a vertex is only boxed when we are sure it has the *minimum* cumulative weight.
- The minimum weight path from A to F was the same either via the intermediate vertices B and G or directly along the incident edge. This does not in general occur, but if it does, either path is equally valid.

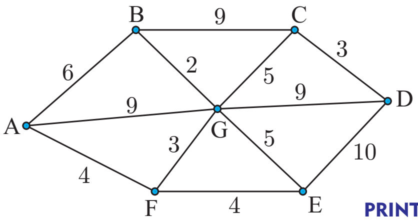
EXERCISE 2E.4

1 Find the minimum connector from A to D for the networks below:

a



b

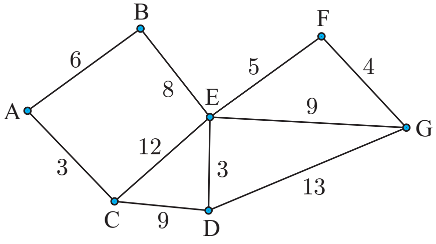


PRINTABLE DIAGRAMS

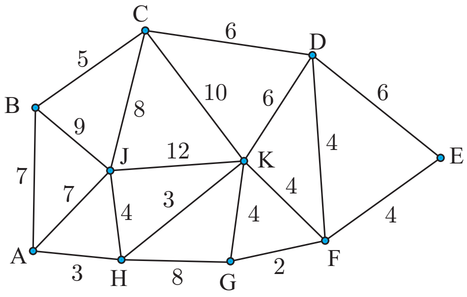
2 Solve the **Opening Problem d ii** on page **90** using Dijkstra's algorithm.

3 Find the shortest path from A to G on the graph below:

a



b



F THE CHINESE POSTMAN PROBLEM (CPP)

The Chinese mathematician **Kwan Mei-Ko** posed the question that given a weighted connected graph, what is the minimum weight closed walk that covers each edge *at least once*?

If all the vertices of the graph have even degree, the graph is Eulerian and there exists an Eulerian circuit that traverses every edge exactly once. The Chinese Postman Problem (CPP) is therefore trivial for an Eulerian graph, and the solution is any Eulerian circuit for the graph.

If a graph is not Eulerian, some of the edges must be walked twice to solve the CPP. The task is to minimise the total weight of the edges we walk twice.

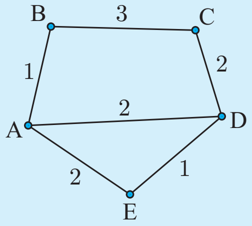
For non-Eulerian graphs, vertices with odd degree exist in pairs. We therefore need to walk twice over some edges between pairs of odd vertices. We work out how to do this most efficiently either by inspection or by using Dijkstra's algorithm.

By pairing vertices of odd degree in any graph G, we can add a "new edge" between each such pair and thus obtain a new graph H with all even vertices. H is an Eulerian graph, and any Eulerian circuit for H can be converted to a possible solution to the CPP for G by replacing each "new edge" in the circuit by the minimum connector path in G between the two odd vertices. These minimum connector paths are found by inspection or by using Dijkstra's algorithm.

If there are more than two odd vertices, we must consider each possible pairing of the vertices. We solve the CPP by applying Dijkstra's algorithm for each case. We then compare the results to find the closed walk of minimum weight.

Example 7

Solve the Chinese Postman Problem for the weighted graph shown.



The graph is not Eulerian since vertices A and D have odd degree.

We therefore need to walk twice between these vertices.

The possible paths from A to D are:

$$\begin{aligned} A \to B \to C \to D &\quad \text{with weight} \quad 1+3+2=6 \\ A \to D &\quad \text{with weight} \quad 2 \\ A \to E \to D &\quad \text{with weight} \quad 2+1=3 \end{aligned}$$

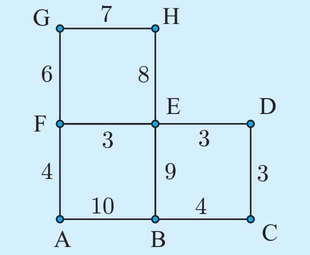
The most efficient way is therefore to traverse the edge AD twice.

A minimum weight closed walk that covers every edge at least once will have weight equal to the sum of the weights of all the edges, plus the weight of edge AD again. The total is $11+2=13$.

An example solution is $A \to B \to C \to D \to A \to E \to D \to A$.

Example 8

Use Dijkstra's algorithm to help solve the Chinese Postman Problem for the weighted graph shown.

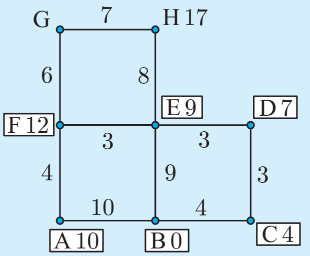


The graph is not Eulerian since vertices B and F are odd.

We therefore need to walk twice between these vertices, and we use Dijkstra's algorithm to do this in the most efficient way:

By Dijkstra, the minimum weight path from B to F is B → E → F.

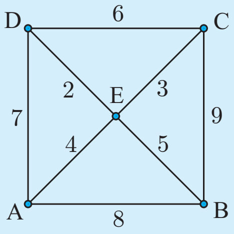
The solution will have total weight equal to the weight of all edges, counting the weights of BE and EF twice. The total weight is 69.



An example solution is
B → C → D → E → H → G → F → E → B → A → F → E → B.

Example 9

Solve the Chinese Postman Problem for the weighted graph shown.



The graph is not Eulerian since vertices A, B, C, and D are all odd.

There are three possible pairings of these vertices: AB and CD, AC and BD, AD and BC.

For each case we find the minimum weight connector path between the vertices, either by inspection or using Dijkstra's algorithm.

	Minimum Weight Connector		*Combination's Total Minimum Weight*
Pairing	*Path*	*Weight*	
AB CD	A → B C → E → D	8 5	13
AC BD	A → E → C B → E → D	7 7	14
AD BC	A → E → D B → E → C	6 8	14

The combination of pairs with the overall minimum weight is AB and CD.

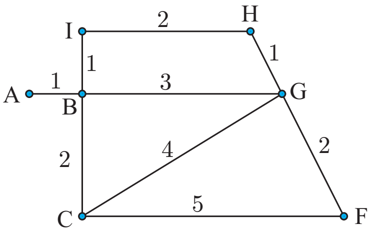
Hence the most efficient way is to construct a closed walk which traverses all edges, and traverses both routes A → B and C → E → D twice each.

An example solution is

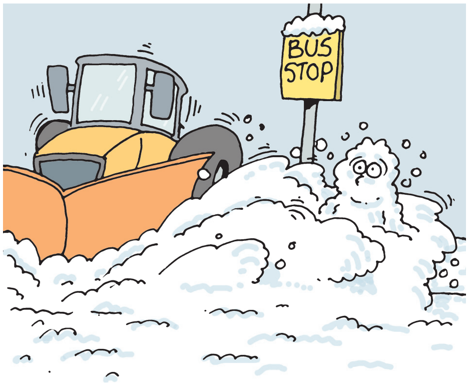
A → E → B → A → B → C → E → D → C → E → D → A of total weight 57.

EXERCISE 2F

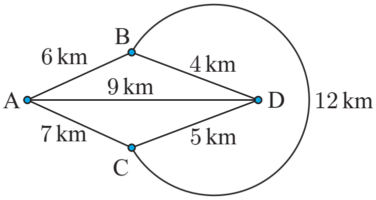
1 A snowplough must clear snow by driving along all of the roads shown in the graph, starting and finishing at the garage A. All distances shown are in km.



Explain why the shortest distance the snowplough must travel is 24 km.



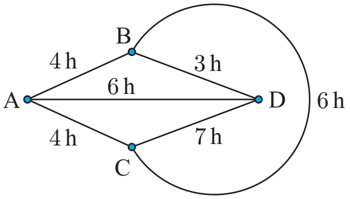
2 A network of paths connects four mountain tops as shown in the figure. A keen rambler wishes to walk along all of the paths linking the peaks, and return to the starting point.



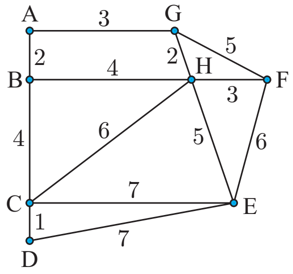
a Explain why the rambler will have to repeat some sections of the track. How many sections will have to be repeated?

b Considering all possible combinations of pairs, find the minimum distance that the rambler must travel to cover every section of track, starting and finishing at A. Suggest a possible route that achieves this minimum distance.

c After some careful thought, the rambler realises that because of the terrain, he would be better off considering the time required to walk the paths instead of the distances. The map with the times for each section of track is shown alongside. If the ramber wants to minimise the total time on route, what should his strategy be?



3 A roadsweeper based at A must clean all of the roads shown at least once, and return to A.



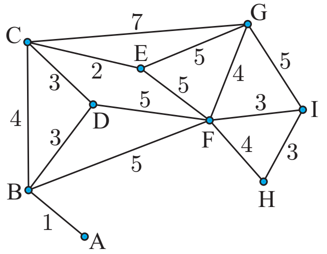
a Explain why:

i some of the roads will have to be swept twice

ii the shortest possible distance the roadsweeper must travel is 63 units.

b Find a route by which the roadsweeper can achieve this minimum.

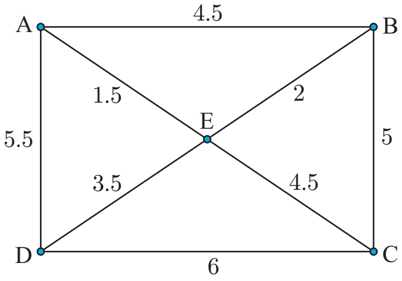
4



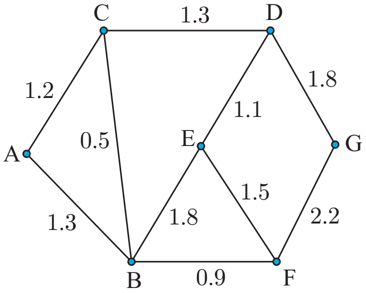
The graph opposite shows the roads in Postman Peter's mailing route. If the Post Office where Peter starts and finishes his round is at A, how should Peter minimise the distance he must walk? Find this minimum distance.

5 A carnival procession wishes to march down each of the roads shown, and return to its starting point. All lengths are shown in kilometres.

- **a** List the three different ways in which the four odd vertices can be paired.
- **b** Find the shortest distance that the procession has to travel if they are to start and finish at E.



6



The graph opposite is a schematic drawing of an oil field. The vertices are oil wells, and the edges are the pipelines which connect them.

The cost of inspecting each pipeline (in tens of thousands of dollars) by means of a robotic device, is shown. Once the robot is on a pipeline, it must inspect all of it.

Find the least cost solution for completing the inspection, given that at the end of the inspection, the robot must return to its starting point.

G THE TRAVELLING SALESMAN PROBLEM (TSP)

We have seen how the vertices of a weighted connected graph can represent cities, oilwells, or delivery destinations, and the weights of the edges can represent travel distance, time, or connection cost.

For the Chinese Postman Problem we considered the most efficient way to travel along *all edges* of a graph and return to our starting point.

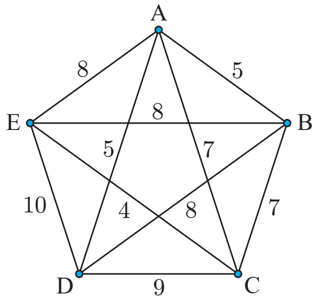
For the Travelling Salesman Problem (TSP) we consider the most efficient way to visit *all vertices* of a graph and return to our starting point.

We have seen that a Hamiltonian cycle is a cycle containing every vertex in a connected graph. A graph which contains a Hamiltonian cycle is called **Hamiltonian**. Note that any complete graph is Hamiltonian.

A **closed spanning walk** in a connected graph is a closed walk which visits every vertex in the graph at least once.

Since a closed spanning walk can have repeated edges and/or repeated vertices, a Hamiltonian cycle is necessarily a closed spanning walk, but a closed spanning walk is not necessarily a Hamiltonian cycle.

Consider the complete weighted graph G:



Two examples of Hamiltonian cycles in G are: C_1: ABCEDA of weight $\text{wt}(C_1) = 31$
C_2: ABCDEA of weight $\text{wt}(C_2) = 39$

Note that C_1 has a lower weight than C_2.

Some examples of closed spanning walks in G are: Any Hamiltonian cycle in G,
W_1: ABCEDECBA and $\text{wt}(W_1) = 52$
W_2: ABCEDBA and $\text{wt}(W_2) = 39$

Note that W_2 has a much lower weight than W_1, but not as low as C_1.

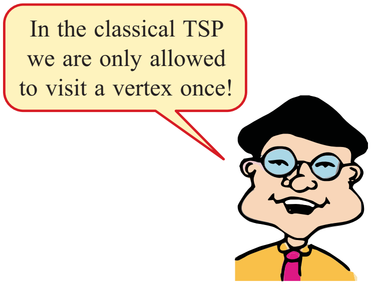
For this graph G it appears that the most efficient way to visit all vertices and return to our starting point, is by the Hamiltonian cycle C_1. However, there are two different statements for the TSP:

Classical Travelling Salesman Problem (TSP):

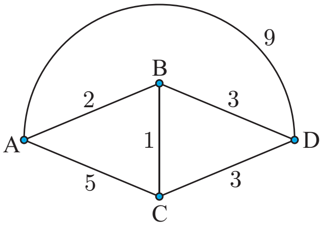
For a given weighted *complete* graph, find a Hamiltonian cycle of least weight.

Practical Travelling Salesman Problem (TSP):

For a given weighted connected graph, find a closed spanning walk of least weight.


In the classical TSP we are only allowed to visit a vertex once!

Consider the weighted complete graph H:



The solution to the classical TSP is the Hamiltonian cycle ABDCA of weight 13.

The solution to the practical TSP is the closed spanning walk ABDCBA of weight 11.

$\therefore$ for the practical TSP, the solution is not necessarily a Hamiltonian cycle.

A weighted complete graph is called **Euclidean** if, for all triples V, W, U of distinct vertices,

$$\text{wt}\{\text{VW}\} \leqslant \text{wt}\{\text{VU}\} + \text{wt}\{\text{UW}\} \quad \text{(triangle equality)}$$

where wt{VW} is the weight of edge VW.

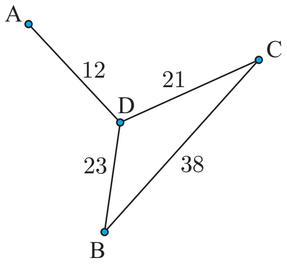
For example, graph G above is Euclidean, but graph H is not. We see for the triangle ABC in H that $\text{wt}\{\text{AC}\} \nleqslant \text{wt}\{\text{AB}\} + \text{wt}\{\text{BC}\}$.

If a weighted complete graph is Euclidean, then the practical TSP and the classical TSP are equivalent problems, and both are solvable by a minimum weight Hamiltonian cycle.

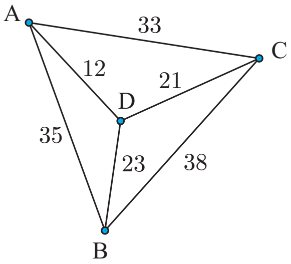
Note that if a weighted connected graph satisfies the triangle inequality but is not complete, it can be made complete by the addition of edges of weight equal to the shortest path between the two given vertices.

For example, consider the graph G on the left below. We can transform it into a complete graph K_G as follows:

G:



K_G:



Since K_G is weighted, complete, and Euclidean, to solve the TSP we need only consider Hamiltonian cycles in K_G. We arbitrarily choose vertex A as the starting point, and find all Hamiltonian cycles in K_G starting and finishing at A.

ABCDA:	$35 + 38 + 21 + 12 = 106$	ACDBA:	$33 + 21 + 23 + 35 = 112$
ABDCA:	$35 + 23 + 21 + 33 = 112$	ADBCA:	$12 + 23 + 38 + 33 = 106$
ACBDA:	$33 + 38 + 23 + 12 = 106$	ADCBA:	$12 + 21 + 38 + 35 = 106$

The three cycles on the right are simply those on the left in reverse order, so they can be discarded. We see that the solution to the TSP is a Hamiltonian cycle of weight 106, for example ABCDA of minimum weight 106. We interpret from this that the solution to the practical TSP for the original graph G is given by the closed spanning walk ADBCDA of weight 106.

From here on, **we consider the TSP only for weighted complete graphs which are Euclidean**.

Solving the TSP therefore reduces to finding a minimum weight Hamiltonian cycle.

It is not always easy to directly find a minimum weight Hamiltonian cycle. We now explore methods to find upper and lower bounds for the TSP, which are upper and lower bounds for the minimum weight m of the Hamiltonian cycle solution to the TSP.

FINDING AN UPPER BOUND

Let G be a Euclidean, weighted complete graph.

Let m be the weight of the minimum weight Hamiltonian cycle in G.

1 Kruskal's algorithm can be used to find a minimum weight spanning tree T for G. The branches of T can be used to construct a minimum weight spanning walk of weight $2 \times \text{wt}(T)$.
Hence an upper bound for m is

$$m \leqslant 2 \times \text{wt}(T) \quad \text{for } T \text{ any minimum weight spanning tree in } G.$$

2 If we can find any Hamiltonian cycle C in G then $\text{wt}(C)$ provides an upper bound for m.

$$m \leqslant \text{wt}(C) \quad \text{for } C \text{ any Hamiltonian cycle in } G.$$

A Hamiltonian cycle in G can be found by inspection or by using the **nearest neighbour algorithm** below.

NEAREST NEIGHBOUR ALGORITHM

This is a **greedy** algorithm, which means that at each stage the optimal strategy is taken, regardless of the consequences. The algorithm therefore delivers a Hamiltonian cycle of low, but not necessarily minimum weight, for a complete weighted graph G. If G is Euclidean, the weight of the resulting Hamiltonian cycle provides an upper bound for the TSP.

Step 1: Start with the vertices only of a weighted complete graph G.

Step 2: Choose a starting vertex, A. Label A as visited, and set A as the current vertex.

Step 3: Find the edge of least weight connecting the current vertex to an unvisited vertex V. Add this edge to the graph.

Step 4: Label V as visited, and set V as the current vertex.

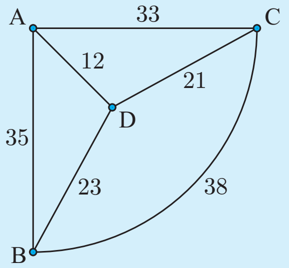
Step 5: If all vertices in the graph are visited, then return to vertex A by adding the corresponding edge. Otherwise, return to *Step 3*.

The sequence of visited vertices is a Hamiltonian cycle.

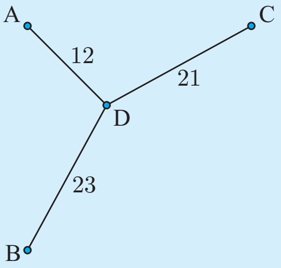
Example 10

a Find a minimum weight spanning tree and hence find an upper bound for the TSP.

b Find a Hamiltonian cycle which improves the upper bound found in **a**.



a T:



$\text{wt}(T) = 12 + 21 + 23 = 56$

$\therefore$ $m \leqslant 2 \times 56 = 112$ where m is the minimum weight solution to the TSP.

b The Hamiltonian cycle ADBCA has weight $= 106$

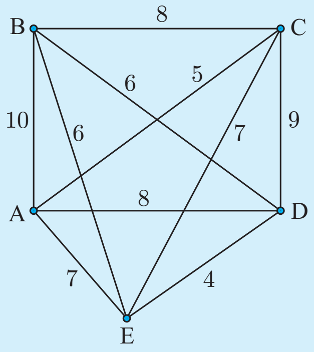
$\therefore$ $m \leqslant 106$.

Example 11

a Find a minimum weight spanning tree and hence find an upper bound for the TSP.

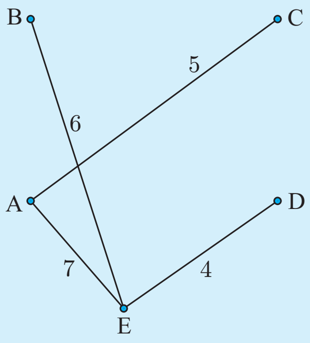
b Use the nearest neighbour algorithm starting at A, to find a Hamiltonian cycle for the graph. Hence improve the upper bound found in **a**.

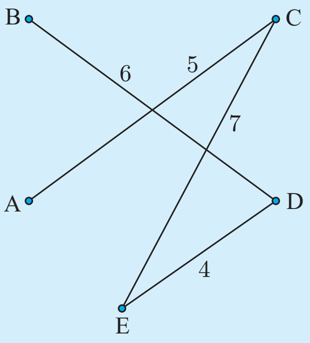
c Does the Hamiltonian cycle in **b** solve the TSP? Explain your answer.

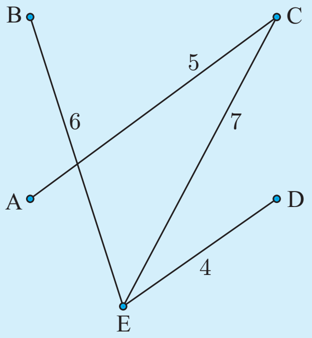


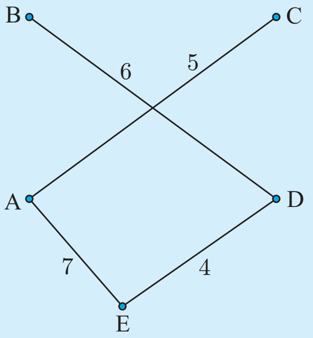
a Let m be the least weight solution to the TSP.

Using Kruskal's algorithm, there are four possible minimum weight spanning trees each of weight $4 + 5 + 6 + 7 = 22$.









$\therefore \quad m \leqslant 2 \times 22 = 44.$

b Start at A.

The nearest vertex is C, so we add edge AC and set C as the current vertex.

The nearest unvisited vertex to C is E, so we add edge CE and set E as the current vertex.

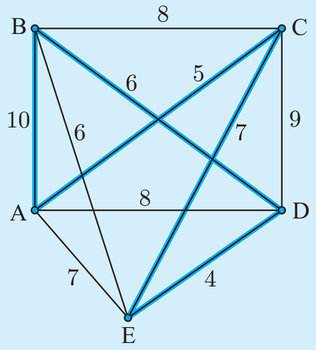
Continuing this process, we choose ED, then DB.

All vertices have now been visited, so we add BA to complete a Hamiltonian cycle.

The Hamiltonian cycle is ACEDBA with

$$\begin{aligned}\text{weight} &= 5 + 7 + 4 + 6 + 10\\ &= 32\end{aligned}$$

$\therefore \quad m \leqslant 32.$



c No. For example, the spanning tree BDEAC from **a** completes to the Hamiltonian cycle BDEACB of weight $= 6 + 4 + 7 + 5 + 8 = 30$

FINDING A LOWER BOUND

Let G be a Euclidean, weighted, complete graph on the n vertices $V_1, V_2, ..., V_n$.

Suppose $V_1 \longrightarrow V_2 \longrightarrow .... \longrightarrow V_n \longrightarrow V_1$ is a minimum weight Hamiltonian cycle in G of minimum weight m, that is a solution to the TSP for G.

Then $m = \text{wt}\{V_1V_2\} + \text{wt}\{V_1V_n\} + (\text{weight of the path } V_2 \longrightarrow V_3 \longrightarrow .... \longrightarrow V_n)$.

Consider the graph G_{V_1} on vertices $V_2, V_3, ..., V_n$ which is G with vertex V_1 removed and all edges incident on V_1 removed. Graph G_{V_1} is a complete graph on the $n-1$ vertices $V_2, V_3, ..., V_n$.

The path $V_2 \longrightarrow V_3 \longrightarrow .... \longrightarrow V_n$ is a spanning tree of G_{V_1}

$\therefore \quad \text{wt(path } V_2 \longrightarrow V_3 \longrightarrow .... \longrightarrow V_n) \geqslant \text{wt(a minimum weight spanning tree of } G_{V_1})$

$\therefore \quad m \geqslant \text{wt}\{V_1V_2\} + \text{wt}\{V_1V_n\} + \text{wt(a minimum weight spanning tree of } G_{V_1})$

This observation is the basis for the following method which gives a lower bound for the TSP.

DELETED VERTEX ALGORITHM

Step 1: Delete a vertex, together with all incident edges, from the original graph.

Step 2: Find the minimum spanning tree for the remaining graph.

Step 3: Add to the length of the minimum spanning tree, the lengths of the two shortest deleted edges.

The resulting value is a lower bound for m, the minimum weight for the solution to the TSP.

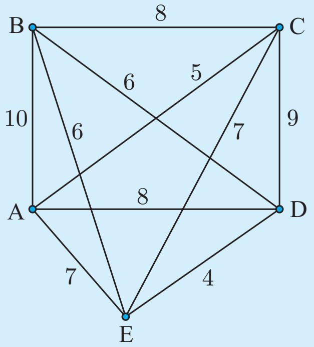
Note that the bound obtained depends on which vertex is chosen to be the deleted vertex. For each choice of vertex to be deleted, the algorithm yields possibly different lower bounds. The *largest* such bound provides the best lower bound for the TSP.

The value returned by the algorithm will only equal m in the solution to the TSP if there is a minimum length spanning tree with only two end vertices *and* if the minimum lengths deleted are incident to these end vertices.

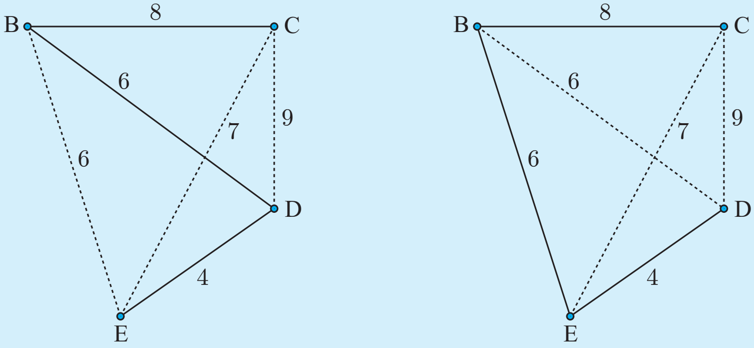
Example 12

a Apply the deleted vertex algorithm by deleting vertex A.
Hence obtain a lower bound for the TSP.

b Find, if possible, a Hamiltonian cycle which meets the bound found in **a**.



a There are two minimum spanning trees for the graph with vertex A deleted and all edges incident with A deleted:



The minimum spanning trees each have weight 18.

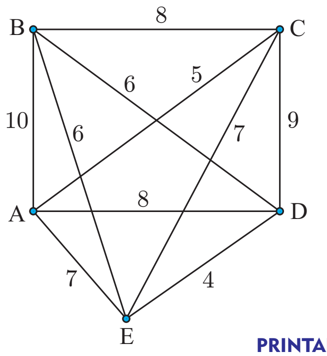
The two edges of least weight incident with A have weights 5 and 7.

$\therefore$ if m is the minimum weight in the solution to the TSP, then $m \geqslant 18 + 5 + 7 = 30$.

b ACBDEA and ACBEDA both have weight 30.

EXERCISE 2G

1 Consider again the graph in **Examples 11** and **12**.



PRINTABLE DIAGRAMS

a Find an upper bound for the TSP using the nearest neighbour algorithm beginning at:

i vertex B **ii** vertex C

iii vertex D **iv** vertex E.

Which is the best bound found?

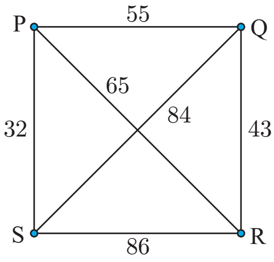
b Find a lower bound for the TSP using the deleted vertex algorithm and deleting:

i vertex B **ii** vertex C

iii vertex D **iv** vertex E.

Which is the best bound found?

2 **a** Find a minimum spanning tree for the given graph. Hence find an upper bound for the TSP.



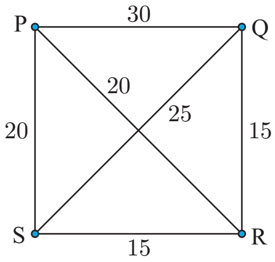
b Complete the tree to a Hamiltonian cycle, and hence find a better upper bound.

c By deleting each vertex in turn, use the deleted vertex algorithm to find a set of lower bounds.

d Use the nearest neighbour algorithm, starting at P, to find an upper bound for the TSP.

e Solve the TSP problem for this graph.

3



a Find two minimum spanning trees for the given graph.

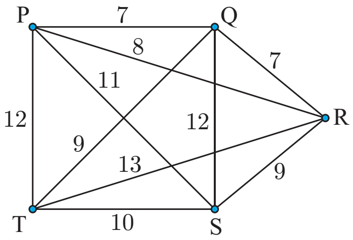
b Complete one of these to a Hamiltonian cycle, and hence find an upper bound for the TSP.

c By deleting each vertex in turn, use the deleted vertex algorithm to find a set of lower bounds.

d Use the nearest neighbour algorithm, starting at P, to find an upper bound for the TSP.

e Solve the TSP problem for this graph.

4 **a** Find a minimum spanning tree for the given graph. Hence find an upper bound for the TSP.



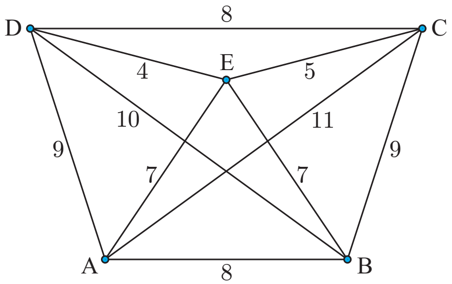
b Find a Hamiltonian cycle, and hence find a better upper bound.

c By deleting the vertices in turn, use the deleted vertex algorithm to find a set of lower bounds.

d Use the nearest neighbour algorithm, starting at P, to find an upper bound for the TSP.

e Solve the TSP problem for this graph.

5 Consider the TSP for the given graph.



a Apply the deleted vertex algorithm with A, B, C, D, and E in turn to find a lower bound.

b Apply the nearest neighbour algorithm with A as the initial vertex to find an upper bound and a Hamiltonian cycle.

c Suppose the network represented five towns.

i At which town would you choose to base yourself to minimise travel amongst the towns? Explain your answer.

ii Apply the nearest neighbour algorithm using this vertex initially to find an upper bound and a Hamiltonian cycle.

6 A hygiene inspector lives in Town A and has to visit hawkers centres in towns B, C, D, E, and F. Use the nearest neighbour algorithm on the distance data below to recommend a route for him.

	A	B	C	D	E	F
A	–	16	13	11	7	8
B	16	–	10	5	12	10
C	13	10	–	4	7	9
D	11	5	4	–	6	7
E	7	12	7	6	–	9
F	8	10	9	7	9	–

7 The table below shows the distances, in km, between towns in France. Twice per year, a company representative must visit each town in turn, and then return home.

Bordeaux								
870	Calais							
641	543	Dijon						
550	751	192	Lyons					
649	1067	507	316	Marseille				
457	421	297	445	761	Orléans			
247	625	515	431	733	212	Poitiers		
519	803	244	59	309	392	421	St-Etienne	
244	996	726	535	405	582	435	582	Toulouse

a Use the nearest neighbour algorithm to find a Hamiltonian cycle between all of the towns, beginning and ending at Toulouse.

b Use the nearest neighbour algorithm to find a Hamiltonian cycle between all of the towns, beginning and ending at Calais.

c Which town, Toulouse or Calais, would be the preferred home town for the representative in order to minimise travel?

THEORY OF KNOWLEDGE — NP PROBLEMS

A **Turing machine** is an imaginary device invented by **Alan Turing** in 1936 as a hypothetical representation of a computer. It is designed to help computer scientists understand the limits of mechanical computation. In particular, they are used to consider the time a computer would require to perform the operations necessary to solve a problem.

Suppose we are solving the TSP for n nodes. The most direct solution would be to try all $\frac{(n-1)!}{2}$ ordered combinations of nodes. An algorithm checking every possibility is therefore said to have order $n!$, written $O(n!)$.

We can show that any factorial or exponential will grow faster than any polynomial, since $\lim\limits_{n\to\infty} \frac{n^k}{n!} = \lim\limits_{n\to\infty} \frac{n^k}{e^n} = 0$ for all k. This means that problems with factorial or exponential order require increasingly more computations than problems with polynomial order.

In 2006, the TSP was solved for visiting 85 900 nodes, using a group of computers taking a total of 136 CPU-years.

1 How long would it take a computer to test all Hamiltonian cycles in a complete, weighted graph with 30 vertices?

A computer algorithm can only be efficient if it can run in **polynomial time** on a Turing machine, which means it must have polynomial order $O(n^k)$. Computer scientists can hence sort problems into a number of classes, including:

- a problem which can be solved in polynomial time on a deterministic Turing machine belong to the **complexity class P**
- a problem for which a given solution can be verified as correct in polynomial time belong to the **complexity class NP**
- a problem which requires at least as much computational time to solve as the hardest problem in NP, is said to be **NP-hard**
- a problem which is in NP and which is NP-hard, is said to be **NP-complete**.

For example:

- The Chinese Postman Problem (CPP) is a P problem.
- The Travelling Salesman Problem (TSP) is an NP-complete problem.
- The New York Street Sweeper Problem (NYSSP) is a variant of the Chinese Postman Problem (CPP) in which the edges of the graph are *directed*. This means they can only be travelled in one direction. The NYSSP is an NP-complete problem.

2 Is it reasonable that a simply posed solvable problem should not be solvable in polynomial time?

3 Why should extra constraints on a problem make it harder to solve? For example, consider the NYSSP and the CPP.

4 How can a problem be categorised as NP-hard?

Given the huge time and cost of finding guaranteed optimal solutions to the TSP, a huge amount of research has been done on approximate solutions, or solutions which are within a given bound of being optimal. In 1976, Nicos Christofides of Imperial College, London, developed an algorithm which produces routes guaranteed to be at most 50% longer than the shortest route. It then took a further 35 years before an improvement was made, and that was so extraordinarily tiny as to have no practical benefit. Around the world, mathematicians and computer scientists continue to work on this problem, hoping to find more powerful results.

5 Is there benefit in pursuing exact solutions to problems like the TSP if approximate solutions are far easier to obtain?

6 At what point should we consider an approximate solution "good enough"?

The **P = NP problem** posed by **Stephen Cook** in 1971 is one of the most important unsolved problems in computer science. It questions whether the classes P and NP are equivalent, or in other words whether problems whose solutions can be easily verified by a computer, can also be easily solved by a computer. If there exists a polynomial algorithm for any NP-complete problem, then there exist polynomial algorithms for all NP-complete problems.

It is reasonably well thought that P $\neq$ NP. However, on the assumption that P = NP:

7 How can a polynomial algorithm for one NP problem assist in finding algorithms for the rest?

8 What ramifications are there for mathematical research in the future?

REVIEW SET A

1 Use the Principle of Mathematical Induction to prove that $7^n + 3^n + 2$ is divisible by 4 for all $n \in \mathbb{N}$.

2 Find a closed form solution for the recurrence relation $a_{n+1} = \frac{n+2}{n+1}a_n$, $n \geqslant 0$, $a_0 = 1$. Prove your result by induction.

3 Consider the recurrence relation $a_0 = 3$, $a_n = 4a_{n-1} - 8$, $n \geqslant 1$.

a Calculate the first five terms of the sequence.

b Find a closed form solution, proving your result by induction.

4 A radioactive isotope decays by 2.2% every week. Initially there are a_0 grams of the substance in a sample.

a Write, in terms of a_0, the quantity of isotope remaining after:

i 1 week **ii** 5 weeks.

b Find and solve a recurrence relation for the amount of isotope remaining after n weeks.

c What initial mass would be necessary for 1.7 g to be remaining after 10 weeks?

5 Find the closed form solution for each recurrence relation:

a $a_n = 4a_{n-1} - 3a_{n-2}$, $n \geqslant 2$ with $a_0 = 1$, $a_1 = -1$

b $a_n = 4a_{n-1} - 4a_{n-2}$, $n \geqslant 2$ with $a_0 = 1$, $a_1 = -1$

c $a_n = 4a_{n-1} - 5a_{n-2}$, $n \geqslant 2$ with $a_0 = 0$, $a_1 = 1$.

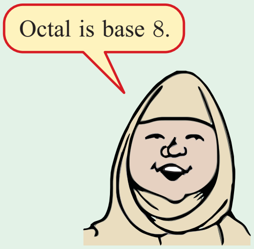
6 Consider $a, b \in \mathbb{Z}^+$. Show that if $3 \mid (a^2 + b^2)$ then $3 \mid a$ and $3 \mid b$, but if $5 \mid (a^2 + b^2)$ then 5 need not necessarily divide either a or b.

7 **a** Prove that any integer of the form $6m + 5$, $m \in \mathbb{Z}$, is also of the form $3n + 2$, $n \in \mathbb{Z}$.

b Provide a counter example to show that the converse of **a** is not true.

8 Convert 144_5 from base 5 into:

a binary **b** octal.



9 Prove that the product of any five consecutive integers is divisible by 120.

10 **a** Use the Euclidean algorithm to find the greatest divisor of 552 and 208.

b Hence or otherwise, find two integers m and n such that $552m - 208n = 8$.

11 **a** Let $n \in \mathbb{Z}^+$, $n \geqslant 2$, and let $m = (n+1)!+2$. Show that m is even and that $3 \mid (m+1)$.

b Let $n \in \mathbb{Z}^+$, $n \geqslant 3$, and let $m = (n+2)!+2$. Show that m is even and that $3 \mid (m+1)$ and $4 \mid (m+2)$.

c Prove that there is a sequence of n numbers that are all composite.

12 Find the prime factorisation of:

a 1040 **b** 18 360 **c** 19 845

13 Find:

a $23^{12} \pmod 5$ **b** $\sum_{k=1}^{30} k! \pmod{20}$

14 Prove that for any prime $p \geqslant 5,\; 12 \mid p^2 - 1$.

15 If a and b are relatively prime, show that for any $c \in \mathbb{Z}^+,\; \gcd(a,\, bc) = \gcd(a,\, c)$.

16 **a** Consider a three-digit number of the form (bba). If the sum of its digits is divisible by 12, show that the number itself is divisible by 12.

b Consider a three-digit number of the form (bab). If the number itself *and* the sum of its digits is divisible by $k \in \mathbb{Z}^+,\; k > 1$, show that the only possible values of k less than 10 are 3 and 9, or a common divisor of a and b.

17 Solve: $57x \equiv 20 \pmod{13}$.

18 **a** Given $n \not\equiv 0 \pmod 5$, show that $n^2 \equiv \pm 1 \pmod 5$.

b Hence, prove that $n^5 + 5n^3 + 4n$ is divisible by 5 for all $n \in \mathbb{Z}^+$.

19 Solve this system using the Chinese Remainder Theorem: $x \equiv 2 \pmod 4,\; x \equiv 4 \pmod 5$.

20 Show that if $\sqrt{6}$ can be written in the form $\sqrt{6} = \dfrac{a}{b}$ where $a,\, b \in \mathbb{Z}^+$ are both relatively prime, then a must be an even number.

Hence prove that $\sqrt{6}$ is irrational.

21 Use FLT to find the remainder when $11^{87} + 3$ is divided by 17.

22 Consider a rectangular garden 36 m wide and 44 m long, planted with 100 trees. Prove there exists a 4 m by 4 m square area in the garden which contains at least two trees.

23 If x, y, z, and t are any four distinct integers, prove that

$$(x-y)(x-z)(x-t)(y-z)(y-t)(z-t) \equiv 0 \pmod 3.$$

24 For which values of m are the following graphs bipartite?

a K_m **b** C_m **c** W_m

25 Let G be a graph with v vertices and e edges. Let M be the maximum degree of the vertices and let m be the minimum degree of the vertices. Show that $m \leqslant \dfrac{2e}{v} \leqslant M$.

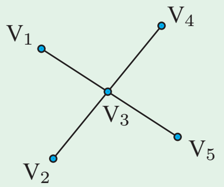
26 How many edges does the complement of W_n have?

27 For each of the following graphs:

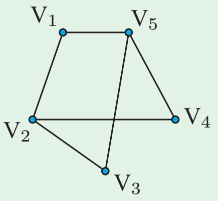
i Construct an adjacency table.

ii State whether the graph is bipartite. If it is, draw it as clearly bipartite.

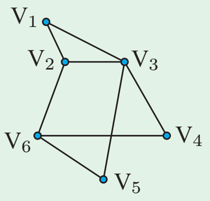
a



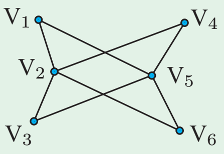
b



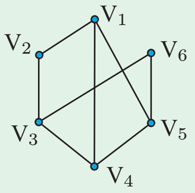
c



d



e



28 Find the number of paths between two given different vertices in K_5, which have length:

a 2 **b** 3 **c** 4.

29 A simple bipartite graph G has an odd number of vertices.
Prove that it cannot be Hamiltonian.

30 Determine whether there exist simple graphs with 12 vertices and 28 edges in which the degree of each vertex is:

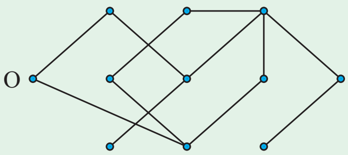
a either 3 or 4 **b** either 5 or 6.

31 Suppose that a connected planar simple graph with v vertices and e edges contains no cycles of length 4 or less. Show $e \leqslant \dfrac{5v-10}{3}$.

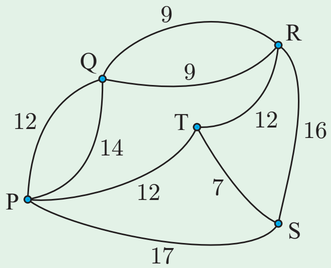
32 A connected planar graph has 8 vertices, each of degree 3. How many faces does it have?

33 Use the breadth first search starting at O to find a spanning tree for the graph alongside:

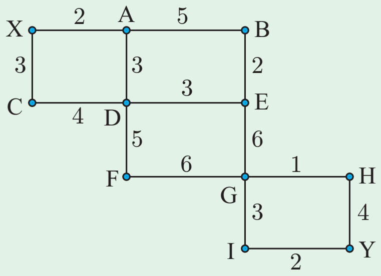
PRINTABLE DIAGRAMS



34 Find a minimum weight spanning tree for the graph shown using Kruskal's algorithm.



35 Find the minimum weight path (minimum connector) from X to Y using Dijkstra's algorithm.



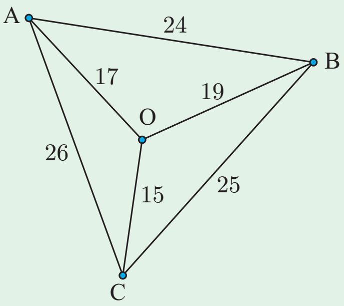
36 The graph alongside is to be solved for the Travelling Salesman Problem.

a Find a minimum spanning tree for the graph and hence find an upper bound for the TSP.

b Improve the upper bound by finding a Hamiltonian cycle.

c Delete each vertex in turn, and hence find the best lower bound.

d Solve the TSP.



REVIEW SET B

1 Use the Principle of Mathematical Induction to prove that $2^n < n!$ for $n \geqslant 4$, $n \in \mathbb{Z}^+$.

2 Consider the recurrence relation $L_{k+2} = L_{k+1} + L_k$ with $L_1 = 1$ and $L_2 = 2$.

- **a** Write down the first 10 terms of the sequence.
- **b** Determine $\sum\limits_{k=1}^{n} L_k$ for $n = 1, 2, 3, 4, 5$, and postulate a closed form solution for $\sum\limits_{k=1}^{n} L_k$ in terms of other L_j.
- **c** Prove your result in **b** by induction.

3 A savings account has €4000 balance. The account earns 5% per annum compounded monthly, and at the end of each month an additional €100 is added to the account.
Let a_n be the amount in the account after n months.

- **a** Find a_0, a_1, a_2, and a_3.
- **b** Find and solve a recurrence relation for a_n, $n \in \mathbb{N}$.
- **c** Calculate the amount in the account after 2.5 years.
- **d** How long will it take for the investment to reach €10 000?

4 Consider the third-degree homogeneous recurrence relation with constant coefficients:

$$a_0 = 0,\ \ a_1 = 0,\ \ a_2 = 2,\ \ a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} = 0,\ \ n \geqslant 3.$$

- **a** Calculate a_3, a_4, a_5, and a_6.
- **b** Conjecture a closed form solution for a_n, $n \in \mathbb{N}$.
- **c** Use strong induction to prove your conjecture.

5 Find the closed form solution for the recurrence relation $a_{n+2} = 2a_{n+1} - 3a_n$, $n \in \mathbb{N}$ with $a_0 = 2$, $a_1 = 2$.

6 Prove that $3 \mid (a^3 + 5a)$ for all $a \in \mathbb{Z}^+$.

7 Prove or disprove: If n^2 is divisible by 12, then so is n.

8 Prove that $n^2 - 1$ is either divisible by 4, or is of the form $4k + 3$.

9 Let a and b be integers such that $\gcd(a, b) = 1$. Find the possible values of:

- **a** $\gcd(a + b, a + 2b)$
- **b** $\gcd(2a + b, a + 2b)$.

10 Using Euclid's algorithm, find all integer pairs x and y such that $17x + 31y = 1$.

11 Find, where possible, all $x, y \in \mathbb{Z}$ such that:

- **a** $12x - 15y = 42$
- **b** $32x + 24y = 144$
- **c** $18x + 11y = 196$

12 Convert $7\,203\,842_9$ from base 9 to base 3.

13 Show that $30 \mid (n^5 - n)$ for all $n \in \mathbb{Z}^+$.

14 Show that the modular equation $22x \equiv 41 \pmod{17}$ has a unique solution modulo 17.
Find the solution.

15 Find the smallest positive integer n such that $n \equiv 3 \pmod{19}$ and $n \equiv 2 \pmod{11}$.

16 Find the smallest integer $a > 2$ such that $2 \mid a$, $3 \mid (a + 2)$, $5 \mid (a + 3)$, and $7 \mid (a + 4)$.

17 Is $4^{35}(47) - 50$ divisible by 3?

18 Consider the statement $a^2 \equiv b^2 \pmod{n} \;\Rightarrow\; a \equiv b \pmod{n}$.

- **a** Show that the statement is false by providing a counter example.
- **b** Is the converse statement true?
- **c** Is the statement $a^2 \equiv b^2 \pmod{n} \;\Rightarrow\; a \equiv b \pmod{n}$ true when n is a prime number?

19 If $ab \equiv 0 \pmod{n}$, what are the conditions on n which require that either $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$?

20 Prove that for all $n \in \mathbb{Z}^+$, $n^5 - 37n^3 + 36n$ is divisible by 4.

21 Use FLT to find the value of $\sum\limits_{k=1}^{p-1} k^p \pmod{p}$ where p is an odd prime.

22 Prove that in a hand of five cards taken from a standard pack of 52, there will be at least two cards of the same suit.

23 Nine distinct points lie in the interior of the unit square. No three of the points are collinear. Prove that there is a triangle formed by 3 of the points which has an area of not more than $\frac{1}{8}$.

24 State the size and order of each of the following graphs:

a K_m **b** C_m **c** W_m **d** $K_{m,\,n}$

25 Colin and Bridget invited three other couples out to dinner. On arrival at the restaurant some people shook hands. No one shook hands with themselves or their partner, and no-one shook hands with anyone more than once.

Colin asked everyone how many hands they shook, and received seven different answers.

How many hands did:

a Bridget shake **b** Colin shake?

26 Represent the following graphs by their adjacency tables:

a K_4 **b** $K_{1,\,4}$ **c** $K_{2,\,3}$

27 A self-complementary graph is a graph which is its own complement.
Find a self-complementary graph with:

a 4 vertices **b** 5 vertices.

28 How many paths are there between (any) two *adjacent* vertices in $K_{3,\,3}$, which have length:

a 2 **b** 3 **c** 4?

29 **a** For which values of m, n does $K_{m,\,n}$ have:

i a Hamiltonian cycle **ii** an Eulerian circuit **iii** both?

b Give an example for the case in **a iii**.

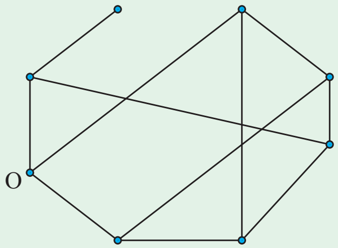
30 Find the fewest number of vertices required to construct a simple connected graph with at least 500 edges.

31 How many faces does a 4-regular connected planar graph with 6 vertices have?

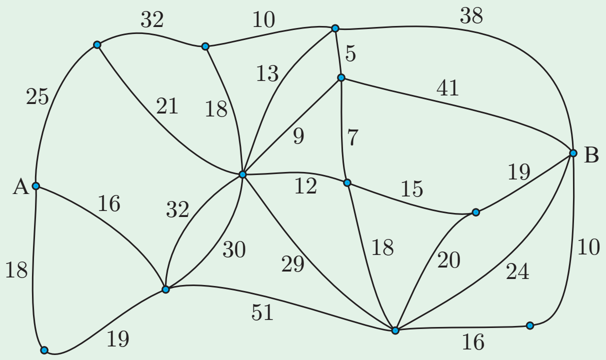
32 Given a simple connected 3-regular graph G is planar, find a relationship between the faces of G and its order. Verify that K_4 satisfies this relationship.

33 Use the breadth first search starting at O to find a spanning tree for the graph shown.

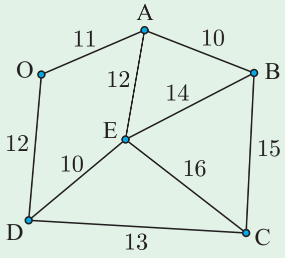
PRINTABLE DIAGRAMS



34 The network alongside shows the connecting roads between towns A and B. The weights on the edges represent distances in kilometres. Find the length of the shortest path from A to B using Dijkstra's algorithm.



35 Solve the Chinese Postman Problem for the graph shown. Assume the postman starts and finishes at O.



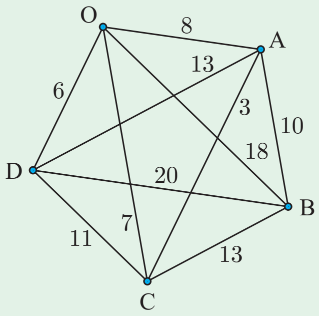
36 The graph alongside is to be solved for the Travelling Salesman Problem.

a Find a minimum spanning tree for the graph and hence find an upper bound for the TSP.

b Improve the upper bound by finding a Hamiltonian cycle.

c Delete each vertex in turn, and hence find the best lower bound.

d Solve the TSP.



REVIEW SET C

1 Consider the recurrence relation $a_n = a_{n-1} + n - 2$, $n \in \mathbb{Z}^+$, $a_0 = 2$.

a Find the first five terms of the sequence described by the recurrence relation.

b Conjecture a closed form solution.

c Use induction to prove your conjecture.

d Find a_{20}.

2 Prove by induction that the $(n+1)$th member of the Fibonacci sequence is given by $f_{n+1} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}$, where $\left\lfloor \frac{n}{2} \right\rfloor$ is the greatest integer less than or equal to $\frac{n}{2}$.

Hint: You may need to consider the cases of odd n and even n separately.

3 A home loan of £120 000 is taken out with fixed interest rate 4.9% p.a. compounded monthly. The loan is to be repaid with regular monthly repayments. The first repayment is due one month after the loan is taken out, after the first amount of interest is calculated and added to the loan. Let a_n be the outstanding value of the loan after n months.

a Suppose the loan is repaid with £1000 every month.

i Calculate a_0, a_1, a_2, and a_3.

ii Write a_n in terms of a_{n-1}, $n \geqslant 1$, and state an appropriate initial condition for the recurrence relation.

iii Find a closed form solution for the recurrence relation.

iv How long will it take for the loan to be repaid?

v Find the total interest paid on the loan.

b Now suppose instead that the loan is to be repaid over 10 years.

i Calculate the regular monthly repayment.

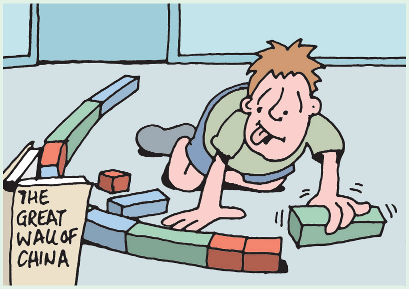
ii Find the total interest paid on the loan.

4 Find a closed form solution for $a_0 = 1$, $a_n = na_{n-1} + n!3^n$, $n \in \mathbb{Z}^+$.

5 A child is playing with a set of coloured blocks, placing them end to end to form a long line. There are three types of blocks: red blocks have length 1 unit, blue blocks have length 2 units, and green blocks have length 3 units.

a Find a recurrence relation for the number of different lines of blocks of length n units.

b How many different block arrangements of length 10 units are there?



6 For $n \in \mathbb{Z}^+$, prove that if n^2 is divisible by 5, then so is n.

7 Suppose $n \in \mathbb{Z}^+$.

a Prove that $n(7n^2 - 1)$ is even.

b Prove that $3 \mid n(7n^2 - 1)$.

c Hence, prove that $6 \mid n(7n^2 - 1)$.

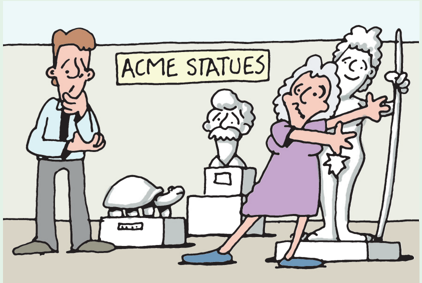
d Prove the result in **c** directly, by considering six exhaustive cases for the form of n.

8 Suppose $p \in \mathbb{Z}^+$. Prove that if p^2 has 7 as a factor, then p has 7 as a factor. Hence prove that the real number $\sqrt{7}$ is irrational.

9 Suppose $d = \gcd(378,\ 168)$. Use Euclid's algorithm to find d, and hence find one pair of integers x and y such that $d = 378x + 168y$.

10 Prove that $a \times b = \gcd(a,\ b) \times \operatorname{lcm}(a,\ b)$ for any positive integers a and b.

11 I wish to buy 50 statues for the botanical gardens. Small statues cost \$40 each, medium statues cost \$100 each, and large statues cost \$250 each. I have \$11 240 to spend. If I spend all of the allocated money, how many statues of each size do I buy?



12 Given that p is prime, prove that:

a $p \mid a^3 \ \Rightarrow\ p^3 \mid a^3$

b $p \mid a^3 \ \Rightarrow\ p \mid a$

13 Prove by induction that for $n \in \mathbb{Z}^+$, $6^n \equiv 1 + 5n \pmod{25}$.

14 Determine, with reasons, the number of incongruent solutions modulo 51 to the equation $165x \equiv 105 \pmod{51}$. Find the solutions.

15 Determine a divisibility test for 36.
Is $14\,975\,028\,526\,645\,824$ divisible by 36?

16 Use the Chinese Remainder Theorem to solve $19x \equiv 99 \pmod{260}$.

17 Solve: $14x + 17 \equiv 27 \pmod{6}$.

18 What is the units digit of 3^{2014}?

19 Suppose N_k is the kth repunit, so $N_1 = 1$, $N_2 = 11$, $N_3 = 111$, and so on.
If $m, n \in \mathbb{Z}^+$ are such that $m < n$ and $m \mid n$, deduce that $N_m \mid N_n$.
Hint: N_m and N_n can be written as geometric series.

20 Determine whether each of these integers is divisible by, 3, 7, 11, or 13.

a $2\,504\,304$

b $1\,703\,702$

21 Use FLT to find the last digit of the base 11 expansion of 7^{80}.

22 Prove that if 51 distinct numbers are chosen from the first 100 positive integers, then at least two of the numbers are consecutive.

23 A set A contains fifteen distinct positive integers, each less than 200. Prove that A contains two *distinct* subsets whose elements sum to the same total.

24 If G is a simple graph with 17 edges and its complement, G', has 11 edges, how many vertices does G have?

25 Show that if G is a bipartite simple graph with v vertices and e edges then $e \leqslant \dfrac{v^2}{4}$.

26 Let G be a simple graph on 6 vertices.

a Give an example which shows that "if G does not contain a 3-cycle, then its complement G' does".

b Assuming the statement in **a** is true, show that in any group of six people, there will always be three who are mutually known to each other, or else are mutual strangers.

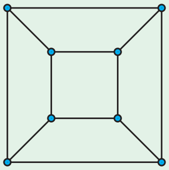
27 If G is a simple graph with at least two vertices, prove that G has two or more vertices of the same degree.

28 Classify the following graphs as

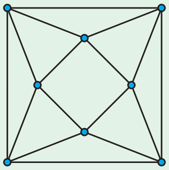
i Eulerian, semi-Eulerian, or neither

ii Hamiltonian, semi-Hamiltonian but not Hamiltonian, or neither:

a K_5 **b** $K_{2,\,3}$ **c**



d



29 A simple graph G with v vertices and e edges has the same number of edges as its complement G'.

a Find e in terms of v.

b Hence show that either $v \equiv 0 \pmod 4$ or $v \equiv 1 \pmod 4$.

c Find all possible values of the order v and corresponding size e of G with $1 \leqslant v \leqslant 20$.

d Draw such a graph G with v and e the smallest of the values found in **c**.
Draw also the complement G'.

30 Prove that $v + f - e = 2$ for G a graph which is:

a a tree **b** a connected planar graph.

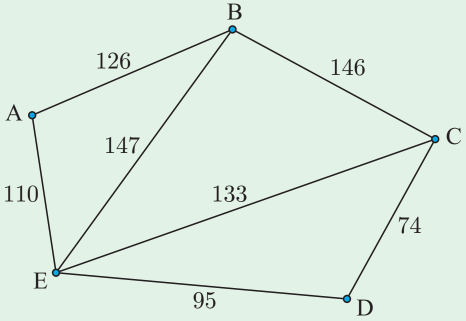
31 Let G be any simple connected planar graph with $v \geqslant 3$ vertices, f faces, and e edges.

a Explain why $3f \leqslant 2e$ and hence explain why $e \leqslant 3v - 6$.

b If $v = 11$, determine whether or not it is possible for the complement G' to also be planar.

32 Given that both a simple graph G and its complement G' are trees, what is the order of G? Sketch the graphs.

33 A sewerage network graphed alongside needs to have all of its tunnels inspected. The weights on the edges are their lengths in metres.



a If there are entrances at each of the nodes, where should the inspection start and finish so that it requires walking a minimum distance?

b State an inspection plan that covers each tunnel only once.

c Suppose the inspector must start and finish his inspection at A.

i Which tunnel will be covered twice for him to travel the minimum distance?

ii What is the minimum distance that he must walk in this case?

APPENDIX: METHODS OF PROOF

Greek mathematicians more than 2000 years ago realised that progress in mathematical thinking could be brought about by conscious formulation of the methods of **abstraction** and **proof**.

By considering a few examples, one might notice a certain common quality or pattern from which one could predict a rule or formula for the general case. In mathematics this prediction is known as a **conjecture**. Mathematicians love to find patterns, and try to understand why they occur.

Experiments and further examples might help to convince you that the conjecture is true. However, problems will often contain extra information which can sometimes obscure the essential detail, particularly in applied mathematics. Stripping this away is the process of **abstraction**.

For example, by considering the given table of values one may conjecture:

a	b	a^2	b^2
1	2	1	4
3	5	9	25
4	5	16	25
5	7	25	49
6	9	36	81

"If a and b are real numbers then $a < b$ implies that $a^2 < b^2$."

However, on observing that $-2 < 1$ but $(-2)^2 \not< 1^2$ we have a **counter example**.

In the light of this we reformulate and refine our conjecture:

"If a and b are *positive* real numbers then $a < b$ implies $a^2 < b^2$."

The difficulty is that this process might continue with reformulations, counter-examples, and revised conjectures indefinitely. At what point are we certain that the conjecture is true? A **proof** is a flawless logical argument which leaves no doubt that the conjecture is indeed a truth. If we have a proof then the conjecture can be called a **theorem**.

Mathematics has evolved to accept certain types of arguments as valid proofs. They include a mixture of both logic and calculation. Generally mathematicians like elegant, efficient proofs. It is common not to write every minute detail. However, when you write a proof you should be prepared to expand and justify every step if asked to do so.

We have already examined in the HL Core text, proof by **the principle of mathematical induction**. Now we consider other methods.

DIRECT PROOF

In a **direct proof** we start with a known truth and by a succession of correct deductions finish with the required result.

Example 1: Prove that if $a, b \in \mathbb{R}$ then $a < b \;\Rightarrow\; a < \dfrac{a+b}{2}$

Proof: $a < b \;\Rightarrow\; \dfrac{a}{2} < \dfrac{b}{2}$ {as we are dividing by 2 which is > 0}

$\Rightarrow\; \dfrac{a}{2} + \dfrac{a}{2} < \dfrac{a}{2} + \dfrac{b}{2}$ {adding $\dfrac{a}{2}$ to both sides}

$\Rightarrow\; a < \dfrac{a+b}{2}$

Sometimes it is not possible to give a direct proof of the full result and so the different possible cases (called **exhaustive cases**) need to be considered and proved separately.

Example 2: Prove the **geometric progression**: For $n \in \mathbb{Z},\ n \geqslant 0$,

$$1 + r^1 + r^2 + ... + r^n = \begin{cases} \dfrac{r^{n+1}-1}{r-1}, & r \neq 1 \\ n+1, & r = 1 \end{cases}$$

Proof: **Case $r = 1$:**

$$\begin{aligned} & 1 + r^1 + r^2 + ... + r^n \\ &= 1 + 1 + 1 + ... + 1 \qquad \{n+1 \text{ times}\} \\ &= n + 1 \end{aligned}$$

Case $r \neq 1$:

$$\begin{aligned} \text{Let} \quad S_n &= 1 + r^1 + r^2 + ... + r^n. \\ \text{Then} \quad rS_n &= r^1 + r^2 + r^3 + ... + r^{n+1} \\ \therefore \quad rS_n - S_n &= r^{n+1} - 1 \qquad \{\text{after cancellation of terms}\} \\ \therefore \quad (r-1)S_n &= r^{n+1} - 1 \\ \therefore \quad S_n &= \frac{r^{n+1}-1}{r-1} \qquad \{\text{dividing by } r-1 \text{ since } r \neq 1\} \end{aligned}$$

Example 3: Alice looks at Bob and Bob looks at Clare. Alice is married, but Clare is not. Prove that a married person looks at an unmarried person.

Proof: We do not know whether Bob is married or not, so we consider the different (exhaustive) cases:

Case: Bob is married. If Bob is married, then a married person (Bob) looks at an unmarried person (Clare).

Case: Bob is unmarried. If Bob is unmarried, then a married person (Alice) looks at an unmarried person (Bob).

Since we have considered all possible cases, the full result is proved.

EXERCISE

1 Let $I = \sqrt{2}$, which is irrational. Consider I^I and I^{I^I}, and hence prove that an irrational number to the power of an irrational number can be rational.

PROOF BY CONTRADICTION (AN INDIRECT PROOF)

In **proof by contradiction** we deliberately assume the opposite to what we are trying to prove. By a series of correct steps we show that this is impossible, our assumption is false, and hence its opposite is true.

Example 4: Consider **Example 1** again but this time use proof by contradiction:

Prove that if $a, b \in \mathbb{R}$ then $a < b \;\Rightarrow\; a < \dfrac{a+b}{2}$.

Proof (by contradiction):

For $a < b$, suppose that $a \geqslant \dfrac{a+b}{2}$

$$\begin{aligned} &\Rightarrow\; 2a \geqslant 2\left(\frac{a+b}{2}\right) && \{\text{multiplying both sides by } 2\} \\ &\Rightarrow\; 2a \geqslant a+b && \\ &\Rightarrow\; a \geqslant b && \{\text{subtracting } a \text{ from both sides}\} \end{aligned}$$

which is false.

Since the steps of the argument are correct, the supposition must be false and the alternative, $a < \dfrac{a+b}{2}$ must be true.

Example 5: Prove that the solution of $3^x = 8$ is irrational.

Proof (by contradiction):

Suppose the solution of $3^x = 8$ is rational, or in other words, that x is rational. Notice that $x > 0$.

$$\begin{aligned} &\Rightarrow\; x = \frac{p}{q} \quad \text{where } p, q \in \mathbb{Z},\; q \neq 0 \quad \{\text{and since } x > 0, \text{ integers } p, q > 0\} \\ &\Rightarrow\; 3^{\frac{p}{q}} = 8 \\ &\Rightarrow\; \left(3^{\frac{p}{q}}\right)^q = 8^q \\ &\Rightarrow\; 3^p = 8^q \end{aligned}$$

which is impossible since for the given possible values of p and q, 3^p is always odd and 8^q is always even. Thus, the assumption is false and its opposite must be true. Hence x is irrational.

Example 6: Prove that no positive integers x and y exist such that $x^2 - y^2 = 1$.

Proof (by contradiction):

Suppose $x, y \in \mathbb{Z}^+$ exist such that $x^2 - y^2 = 1$.

$$\begin{aligned} &\Rightarrow\; (x+y)(x-y) = 1 \\ &\Rightarrow\; \underbrace{x+y = 1 \text{ and } x-y = 1}_{\text{case 1}} \;\; \textbf{or} \;\; \underbrace{x+y = -1 \text{ and } x-y = -1}_{\text{case 2}} \\ &\Rightarrow\; x = 1,\; y = 0 \;\; (\text{from case 1}) \;\; \textbf{or} \;\; x = -1,\; y = 0 \;\; (\text{from case 2}) \end{aligned}$$

Both cases provide a contradiction to $x, y > 0$.
Thus, the supposition is false and its opposite is true.
There do *not* exist positive integers x and y such that $x^2 - y^2 = 1$.

Indirect proof often seems cleverly contrived, especially if no direct proof is forthcoming. It is perhaps more natural to seek a direct proof for the first attempt to prove a conjecture.

ERRORS IN PROOF

One must be careful not to make errors in algebra or reasoning. Examine carefully the following examples.

Example 7: Consider **Example 5** again: Prove that the solution of $3^x = 8$ is irrational.

Invalid argument:

$$\begin{aligned} & 3^x = 8 \\ \Rightarrow\quad & \log 3^x = \log 8 \\ \Rightarrow\quad & x\log 3 = \log 8 \\ \Rightarrow\quad & x = \frac{\log 8}{\log 3} \quad \text{where both } \log 8 \text{ and } \log 3 \text{ are irrational.} \\ \Rightarrow\quad & x \text{ is irrational.} \end{aligned}$$

The last step is not valid. The argument that an irrational divided by an irrational is always irrational is not correct. For example, $\frac{\sqrt{2}}{\sqrt{2}} = 1$, and 1 is rational.

Dividing by zero is *not* a valid operation. $\frac{a}{0}$ is not defined for any $a \in \mathbb{R}$, in particular $\frac{0}{0} \neq 1$.

Example 8: Invalid "proof" that $5 = 2$

$$\begin{aligned} & 0 = 0 \\ \Rightarrow\quad & 0 \times 5 = 0 \times 2 \\ \Rightarrow\quad & \frac{0 \times 5}{0} = \frac{0 \times 2}{0} \qquad \{\text{dividing through by } 0\} \\ \Rightarrow\quad & 5 = 2, \quad \text{which is clearly false.} \end{aligned}$$

This invalid step is not always obvious, as illustrated in the following example.

Example 9: Invalid "proof" that $0 = 1$:

$$\begin{aligned} \text{Suppose}\quad & a = 1 \\ \Rightarrow\quad & a^2 = a \\ \Rightarrow\quad & a^2 - 1 = a - 1 \\ \Rightarrow\quad & (a+1)(a-1) = a - 1 \\ \Rightarrow\quad & a + 1 = 1 \quad .... \ (*) \\ \Rightarrow\quad & a = 0 \\ \text{So,}\quad & 0 = 1 \end{aligned}$$

The invalid step in the argument is $(*)$ where we divide both sides by $a - 1$. Since $a = 1$, $a - 1 = 0$, and so we are dividing both sides by zero.

Another trap to be avoided is to begin by assuming the result we wish to prove is true. This readily leads to invalid circular arguments.

Example 10: Prove without decimalisation that $\sqrt{3} - 1 > \frac{1}{\sqrt{2}}$.

Invalid argument:

$$\begin{aligned} & \sqrt{3} - 1 > \tfrac{1}{\sqrt{2}} \\ \Rightarrow\ & (\sqrt{3} - 1)^2 > \left(\tfrac{1}{\sqrt{2}}\right)^2 && \{\text{both sides are } > 0, \text{ so we can square them}\} \\ \Rightarrow\ & 4 - 2\sqrt{3} > \tfrac{1}{2} \\ \Rightarrow\ & \tfrac{7}{2} > 2\sqrt{3} \\ \Rightarrow\ & 7 > 4\sqrt{3} \\ \Rightarrow\ & 7^2 > 48 && \{\text{squaring again}\} \\ \Rightarrow\ & 49 > 48 && \text{which is true.} \end{aligned}$$

Hence $\sqrt{3} - 1 > \frac{1}{\sqrt{2}}$ is true.

Although $\sqrt{3} - 1 > \frac{1}{\sqrt{2}}$ is in fact true, the above argument is invalid because we began by assuming the result.

A valid method of proof for $\sqrt{3} - 1 > \frac{1}{\sqrt{2}}$ can be found by either:

- reversing the steps of the above argument, or by
- using proof by contradiction (supposing $\sqrt{3} - 1 \leqslant \frac{1}{\sqrt{2}}$).

It is important to distinguish **errors in proof** from a **false conjecture**.

Consider the table alongside, which shows values of $n^2 - n + 41$ for various values of $n \in \mathbb{N}$.

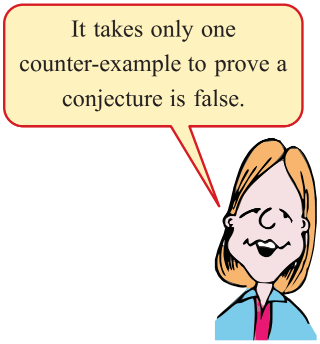
From the many examples given, one might conjecture:

> "For all natural numbers n, $n^2 - n + 41$ is prime."

This conjecture is in fact false.

For example, for $n = 41$, $n^2 - n + 41 = 41^2$ is clearly not prime.

n	$n^2 - n + 41$
1	41
2	43
3	47
4	53
5	61
6	71
7	83
8	97
9	113
10	131
11	151
12	173
13	197
...	...
30	911
...	...
99	9743
...	...


It takes only one counter-example to prove a conjecture is false.

IMPLICATIONS AND THEIR CONVERSE

If .... then ....

Many statements in mathematics take the form of an **implication** "If A then B", where A and B are themselves statements. The statement A is known as the **hypothesis**. The statement B is known as the **conclusion**.

Implications can be written in many forms in addition to "If A then B". For example, the following all have the same meaning:

$$A \left\{ \begin{array}{c} \text{implies} \\ \text{so} \\ \text{hence} \\ \text{thus} \\ \text{therefore} \end{array} \right\} B.$$

Given a statement of the form "If A then B", we can write a **converse** statement "If B then A".

If we know the truth, or otherwise, of a given statement, we can say nothing about the truth of the converse. It could be true or false.

A statement and its converse are said to be (logically) *independent*.

For example, suppose x is an integer.

- The statement "If x is odd, then $2x$ is even" is *true*, but its converse "If $2x$ is even, then x is odd" is *false*.
- The statement "If $2x$ is even, then x is odd" is *false*, but its converse "If x is odd, then $2x$ is even" is *true*.
- The statement "If $x > 1$, then $\ln x > 0$" is *true*, and its converse "If $\ln x > 0$, then $x > 1$" is also *true*.
- The statement "If $x = 5$, then $x^2 = 16$" is *false*, and its converse "If $x^2 = 16$, then $x = 5$" is also *false*.

EXERCISE

Prove or disprove:

1 If x is rational then $2^x \neq 3$.

2 If $2^x \neq 3$ then x is rational.

EQUIVALENCE

Some conjectures with two statements A and B involve **logical equivalence** or simply **equivalence**.

We say A *is equivalent to* B, or A is true *if and only if* B is true.

The phrase "if and only if" is often written as "iff" or $\Leftrightarrow$.

$A \Leftrightarrow B$ means $A \Rightarrow B$ *and* $B \Rightarrow A$

In order to prove an equivalence, we need to prove both implications: $A \Rightarrow B$ *and* $B \Rightarrow A$.

For example: $x^2 = 9 \;\Leftrightarrow\; x = 3$ is a false statement.

$x = 3 \;\Rightarrow\; x^2 = 9$ is true

but $x^2 = 9 \;\not\Leftarrow\; x = 3$ as x may be -3.

Example 11: Prove that $(n+2)^2 - n^2$ is a multiple of 8 $\Leftrightarrow$ n is odd.

Proof: $(\Rightarrow)$ $(n+2)^2 - n^2$ is a multiple of 8

$$\begin{aligned}
&\Rightarrow\; n^2 + 4n + 4 - n^2 = 8a \quad \text{for some integer } a\\
&\Rightarrow\; 4n + 4 = 8a\\
&\Rightarrow\; n + 1 = 2a\\
&\Rightarrow\; n = 2a - 1\\
&\Rightarrow\; n \text{ is odd.}
\end{aligned}$$

$(\Leftarrow)$ n is odd

$$\begin{aligned}
&\Rightarrow\; n = 2a - 1 \quad \text{for some integer } a\\
&\Rightarrow\; n + 1 = 2a\\
&\Rightarrow\; 4n + 4 = 8a\\
&\Rightarrow\; (n^2 + 4n + 4) - n^2 = 8a\\
&\Rightarrow\; (n+2)^2 - n^2 \quad \text{is a multiple of } 8.
\end{aligned}$$

In the above example the $(\Rightarrow)$ argument is clearly reversible to give the $(\Leftarrow)$ argument. However, this is not always the case.

Example 12: Prove that for all $x \in \mathbb{Z}^+$, x is not divisible by 3 $\Leftrightarrow$ $x^2 - 1$ is divisible by 3.

Proof: $(\Rightarrow)$ x is not divisible by 3

$$\begin{aligned}
&\Rightarrow\; \text{either } x = 3k + 1 \text{ or } x = 3k + 2 \quad \text{for some } k \in \mathbb{Z}^+ \cup \{0\}\\
&\Rightarrow\; x^2 - 1 = 9k^2 + 6k \quad \text{or} \quad 9k^2 + 12k + 3\\
&\qquad\qquad = 3(3k^2 + 2) \quad \text{or} \quad 3(3k^2 + 4k + 1)\\
&\Rightarrow\; x^2 - 1 \text{ is divisible by 3.}
\end{aligned}$$

$(\Leftarrow)$ $x^2 - 1$ is divisible by 3

$$\begin{aligned}
&\Rightarrow\; 3 \mid x^2 - 1\\
&\Rightarrow\; 3 \mid (x+1)(x-1)\\
&\Rightarrow\; 3 \mid (x+1) \quad \text{or} \quad 3 \mid (x-1) \quad \{\text{as 3 is a prime number}\}\\
&\Rightarrow\; 3 \nmid x
\end{aligned}$$

or in other words, x is not divisible by 3.

NEGATION

For any given statement A, we write not A or $\neg A$ to represent the negation of the statement A.

For example:

	A	$\neg A$
	$x > 0$	$x \leqslant 0$
	x is prime	x is not prime
	x is an integer	x is not an integer
For $x \in \mathbb{R}$:	x is rational	x is irrational
For $z \in \mathbb{C}$:	z is real	$z = a + bi,\ a, b \in \mathbb{R},\ b \neq 0$
For $x \in \mathbb{Z}^+ \cup \{0\}$:	x is a multiple of 3	x is not a multiple of 3 *or* $x = 3k+1$ or $3k+2$ for $k \in \mathbb{Z}^+ \cup \{0\}$

PROOF OF THE CONTRAPOSITIVE

To prove the statement "If A then B", we can provide a direct proof, or we can prove the logically equivalent **contrapositive** statement "If not B, then not A" which we can also write as "If $\neg B$, then $\neg A$".

For example, the statement "If it is Jon's bicycle, then it is blue"
is logically equivalent to "If that bicycle is not blue, then it is not Jon's".

Example 13: Prove that for $a, b \in \mathbb{R}$, "ab is irrational $\Rightarrow$ either a or b is irrational".

Proof using contrapositive:

a and b are both rational $\Rightarrow$ $a = \dfrac{p}{q}$ and $b = \dfrac{r}{s}$ where $p, q, r, s \in \mathbb{Z},\ q \neq 0,\ s \neq 0$

$\Rightarrow$ $ab = \left(\dfrac{p}{q}\right)\left(\dfrac{r}{s}\right) = \dfrac{pr}{qs}$ {where $qs \neq 0$, since $q, s \neq 0$}

$\Rightarrow$ ab is rational {since $pr, qs \in \mathbb{Z}$}

Thus ab is irrational $\Rightarrow$ either a or b is irrational.

Example 14: Prove that if n is a positive integer of the form $3k+2$, $k \geqslant 0$, $k \in \mathbb{Z}$, then n is not a square.

Proof using contrapositive:

If n is a square then
n has one of the forms $(3a)^2$, $(3a+1)^2$ or $(3a+2)^2$, where $a \in \mathbb{Z}^+ \cup \{0\}$.

$\Rightarrow$ $n = 9a^2,\ 9a^2 + 6a + 1$ or $9a^2 + 12a + 4$

$\Rightarrow$ $n = 3(3a^2),\ 3(3a^2 + 2a) + 1$ or $3(3a^2 + 4a + 1) + 1$

$\Rightarrow$ n has the form $3k$ or $3k+1$ only, where $k \in \mathbb{Z}^+ \cup \{0\}$

$\Rightarrow$ n does not have form $3k+2$.

Thus if n is a positive integer of the form $3k+2$, $k \geqslant 0$, $k \in \mathbb{Z}$, then n is not a square.

USING PREVIOUS RESULTS

In mathematics we build up collections of important and useful results, each depending on previously proven statements.

Example 15: Prove the conjecture:

"The recurring decimal $0.\overline{9} = 0.999\,999\,99....$ is exactly equal to 1".

Proof (by contradiction):

$$\begin{aligned}
\text{Suppose}\quad & 0.\overline{9} < 1 \\
\Rightarrow\quad & 0.\overline{9} < \frac{0.\overline{9}+1}{2} && \{\text{We proved earlier that } a < b \ \Rightarrow\ a < \tfrac{a+b}{2}\} \\
\Rightarrow\quad & 0.\overline{9} < \frac{1.\overline{9}}{2} && \left\{\text{Ordinary division:}\quad \begin{array}{r|l} 2 & 1.999\,999\,99.... \\ \hline & 0.999\,999\,99.... \end{array}\right\} \\
\Rightarrow\quad & 0.\overline{9} < 0.\overline{9} && \text{clearly a contradiction}
\end{aligned}$$

Therefore the supposition is false, and so $0.\overline{9} \geqslant 1$ is true.

Since, $0.\overline{9} > 1$ is absurd, $0.\overline{9} = 1$.

Proof (Direct Proof):

$$\begin{aligned}
0.\overline{9} &= 0.999\,999\,99.... \\
&= 0.9 + 0.09 + 0.009 + 0.0009 + ... \\
&= 0.9\left(1 + \tfrac{1}{10} + \tfrac{1}{100} + \tfrac{1}{1000} + ...\right) \\
&= \tfrac{9}{10}\left(\sum_{i=0}^{\infty}\left(\tfrac{1}{10}\right)^i\right) \\
&= \tfrac{9}{10}\left(\frac{1}{1-\frac{1}{10}}\right) && \{\text{Using the previously proved Geometric Series with } r = \tfrac{1}{10} \text{ and } \left|\tfrac{1}{10}\right| < 1\} \\
&= \tfrac{9}{10} \times \tfrac{10}{9} \\
&= 1
\end{aligned}$$

THEORY OF KNOWLEDGE AXIOMS AND OCCAM'S RAZOR

In order to understand complicated concepts, we often try to break them down into simpler components. But when mathematicians try to understand the foundations of a particular branch of the subject, they consider the question "What is the minimal set of assumptions from which all other results can be deduced or proved?" The assumptions they make are called **axioms**. Whether the axioms accurately reflect properties observed in the physical world is less important to pure mathematicians than the theory which can be developed and deduced from the axioms.

Occam's razor is a principle of economy that among competing hypotheses, the one that makes the fewest assumptions should be selected.

1 What value does Occam's razor have in understanding the long-held belief that the world was flat?

2 Is the simplest explanation to something always true?

3 Is it reasonable to construct a set of mathematical axioms under Occam's razor?

One of the most famous examples of a set of axioms is given by Euclid in his set of 13 books called *Elements*. He gives five axioms, which he calls "postulates", as the basis for his study of Geometry:

1. Any two points can be joined by a straight line.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one endpoint as centre.
4. All right angles are congruent.
5. **Parallel postulate**: If two lines intersect a third in such a way that the sum of the inner angles on one side is less than two right angles, then the two lines inevitably must intersect each other on that side if extended far enough.

4 Is the parallel postulate genuinely an axiom, or can it be proved from the others?

5 What happens if you change the list of axioms or do not include the parallel postulate?

6 What other areas of mathematics can we reduce to a concise list of axioms?

Worked Solutions

EXERCISE 1A.1

1 **a** **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$3^n \geqslant 7n$" for $n \geqslant 3,\ n \in \mathbb{Z}^+$.

(1) If $n = 3$, $3^3 \geqslant 7 \times 3 \Rightarrow 27 \geqslant 21$ which is true.

$\therefore$ P_3 is true.

(2) If P_k is true, then $3^k \geqslant 7k,\ k \geqslant 3$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & 3^{k+1} - 7(k+1)\\ &= 3 \times 3^k - 7k - 7\\ &\geqslant 3(7k) - 7k - 7 && \{\text{using } *\}\\ &= 21k - 7k - 7\\ &= 14k - 7\\ &= 7(2k-1)\\ &\geqslant 7(6-1) && \{\text{as } k \geqslant 3\}\\ &= 35\\ &\geqslant 0\end{aligned}$$

$\therefore$ $3^{k+1} \geqslant 7(k+1)$

Thus P_3 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for $n \geqslant 3,\ n \in \mathbb{Z}^+$.

b **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$n^n > n!$" for $n \geqslant 2,\ n \in \mathbb{Z}^+$.

(1) If $n = 2$, $2^2 > 2!$ is true $\{4 > 2\}$

$\therefore$ P_2 is true.

(2) If P_k is true, then $k^k > k!,\ k \geqslant 2$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & \frac{(k+1)^{k+1}}{(k+1)!}\\ &= \frac{(k+1)^k\cancel{(k+1)}}{\cancel{(k+1)}k!}\\ &> \frac{k^k}{k!} && \{\text{as } k+1 > k\}\\ &> 1 && \{\text{using } *\}\end{aligned}$$

$\therefore$ $(k+1)^{k+1} > (k+1)!$

Thus P_2 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for $n \geqslant 2,\ n \in \mathbb{Z}^+$.

c **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$3^n < n!$" for $n \geqslant 7,\ n \in \mathbb{Z}^+$.

(1) If $n = 7$, $3^7 < 7!$ is true as
$3^7 = 2187$ and $7! = 5040$

$\therefore$ P_7 is true.

(2) If P_k is true, then $3^k < k!,\ k \geqslant 7$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & (k+1)! - 3^{k+1}\\ &= (k+1)k! - 3^{k+1}\\ &> (k+1)3^k - 3^{k+1} && \{\text{using } *\}\\ &= 3^k(k+1-3)\\ &= 3^k(k-2)\\ &> 0 && \{\text{as } k \geqslant 7\}\end{aligned}$$

$\therefore$ $3^{k+1} < (k+1)!$

Thus P_7 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for $n \geqslant 7,\ n \in \mathbb{Z}^+$.

2 **a** **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$n^3 - 4n$ is divisible by 3" for all $n \geqslant 3$, $n \in \mathbb{Z}^+$.

(1) If $n = 3$, $3^3 - 4 \times 3 = 27 - 12 = 15 = 5 \times 3$

$\therefore$ P_3 is true.

(2) If P_k is true, then

$k^3 - 4k = 3A$ for some $A \in \mathbb{Z},\ k \geqslant 3$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & (k+1)^3 - 4(k+1)\\ &= \underline{k^3} + 3k^2 + 3k + 1 - \underline{4k} - 4\\ &= (k^3 - 4k) + (3k^2 + 3k - 3)\\ &= 3A + 3(k^2 + k - 1) && \{\text{using } *\}\\ &= 3[A + k^2 + k - 1] && \text{where } A,\ k \in \mathbb{Z}\end{aligned}$$

$\therefore$ $(k+1)^3 - 4(k+1)$ is divisible by 3.

Thus P_3 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for $n \geqslant 3,\ n \in \mathbb{Z}^+$.

b **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$5^{n+1} + 2(3^n) + 1$ is divisible by 8" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $5^2 + 2(3) + 1 = 25 + 6 + 1 = 32$ which is divisible by 8 $\{8 \times 4 = 32\}$ $\therefore$ P_1 is true.

(2) If P_k is true, then

$5^{k+1} + 2(3^k) + 1 = 8A$ for some $A \in \mathbb{Z}$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & 5^{[k+1]+1} + 2(3^{k+1}) + 1\\ &= 5 \times 5^{k+1} + 3 \times 2(3^k) + 1\\ &= 5[8A - 2(3^k) - 1] + 6(3^k) + 1 && \{\text{using } *\}\\ &= 40A - 10(3^k) - 5 + 6(3^k) + 1\\ &= 40A - 4(3^k) - 4\\ &= 8\left[5A - \frac{3^k+1}{2}\right]\end{aligned}$$

where $\dfrac{3^k+1}{2} \in \mathbb{Z}$ $\{$as 3^k is odd $\Rightarrow 3^k + 1$ is even
$\Rightarrow \dfrac{3^k+1}{2} \in \mathbb{Z}\}$

Thus $5A - \dfrac{3^k+1}{2} \in \mathbb{Z}$ and $5^{[k+1]+1} + 2(3^{k+1}) + 1$ is divisible by 8.

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

c **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$73 \mid (8^{n+2} + 9^{2n+1})$" for all $n \in \mathbb{Z}^+$.

$$\begin{aligned}\text{(1) If } n = 1,\quad & 8^{n+2} + 9^{2n+1}\\ &= 8^3 + 9^3\\ &= 1241\\ &= 73 \times 17 \qquad \therefore\ P_1 \text{ is true.}\end{aligned}$$

(2) If P_k is true, then

$8^{k+2} + 9^{2k+1} = 73A$ for some $A \in \mathbb{Z}$ .... $(*)$

$$\begin{aligned}\text{Now}\quad & 8^{[k+1]+2} + 9^{2[k+1]+1}\\ &= 8 \times 8^{k+2} + 81 \times 9^{2k+1}\\ &= 8 \times 8^{k+2} + 81(73A - 8^{k+2}) && \{\text{using } *\}\\ &= 81(73A) + 8^{k+2}(8 - 81)\\ &= 81(73A) - 73(8^{k+2})\\ &= 73(81A - 8^{k+2}) && \text{where } 81A - 8^{k+2} \in \mathbb{Z}\end{aligned}$$

$\therefore$ $73 \mid (8^{[k+1]+2} + 9^{2[k+1]+1})$

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

3 **a** The nth repunit is

$$\underbrace{11111....1}_{n \text{ of these}}$$

$= 1 + 10^1 + 10^2 + 10^3 + ... + 10^{n-1}$

which is a geometric series with $u_1 = 1$ and $r = 10$

$$= \frac{1(10^n - 1)}{10 - 1} \qquad \left\{ S_n = \frac{u_1(r^n - 1)}{r - 1} \right\}$$

$$= \frac{10^n - 1}{9}, \quad n \in \mathbb{Z}^+$$

b The first repunit is 1 which is not a composite. So, the statement is false.

c Ali's statement is true.
We use "if $\sim B \Rightarrow \sim A$, then $A \Rightarrow B$".
So we need to prove that:
"if a repunit does not have a prime number of digits then the repunit is not prime".

Proof:
Firstly 1 is not a prime.
If the nth repunit does not have a prime number of digits then $n = ab$ where $a, b > 1$.
Let the nth repunit be k.

$$\therefore\ k = \underbrace{\underbrace{111....1}_{a \text{ of them}}\ \underbrace{111....1}_{a \text{ of them}}\ ....\ \underbrace{111....1}_{a \text{ of them}}}_{b \text{ lots of } a}$$

$$\therefore\ k = (111....1)[1 + 10^a + 10^{2a} + ... + 10^{(b-1)a}]$$

$$\therefore\ k = \left(\frac{10^n - 1}{9}\right)\left(\frac{(10^a)^b - 1}{10^a - 1}\right)$$

$\therefore$ k is not a prime

d Joachim's claim is false as the third repunit is 111 and $111 = 3 \times 37$.

4 **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$3^n \geqslant 5n^2 - 6n$" for all $n \geqslant 3$, $n \in \mathbb{Z}^+$.

(1) If $n = 3$, $3^3 \geqslant 45 - 18$

$\therefore\ 27 \geqslant 27$

$\therefore$ P_3 is true.

(2) If P_k is true, then $3^k \geqslant 5k^2 - 6k$, $k \geqslant 3$ .... $(*)$

Now $3^{k+1} - (5[k+1]^2 - 6[k+1])$

$$\begin{aligned}
&= 3(3^k) - 5k^2 - 10k - 5 + 6k + 6 \\
&\geqslant 3(5k^2 - 6k) - 5k^2 - 4k + 1 \qquad \{\text{using } *\} \\
&= 10k^2 - 22k + 1 \\
&= 2k(5k - 11) + 1 \\
&\geqslant 2(3)(4) + 1 \qquad \{\text{as } k \geqslant 3\} \\
&= 25 \\
&\geqslant 0
\end{aligned}$$

$\therefore\ 3^{k+1} \geqslant 5[k+1]^2 - 6[k+1]$

Thus P_3 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for $n \geqslant 3$, $n \in \mathbb{Z}^+$.

EXERCISE 1A.2

1 **Proof:**

(By the Principle of Mathematical Induction (strong form))

P_n is that "if $a_1 = 1$, $a_2 = 2$ and $a_{n+2} = a_{n+1} + a_n$ for all $n \in \mathbb{Z}^+$, then $a_n \leqslant \left(\frac{5}{3}\right)^n$".

(1) If $n = 1$, $a_1 \leqslant \left(\frac{5}{3}\right)^1$, that is, $1 \leqslant \frac{5}{3}$ is true

$\therefore$ P_1 is true.

(2) Assume that $a_r \leqslant \left(\frac{5}{3}\right)^r$ is true for all $r \leqslant k$

$\therefore$ $a_r \leqslant \left(\frac{5}{3}\right)^r$ for $r = 1, 2, 3, ..., k$ .... $(*)$

Now $a_{k+1} = a_k + a_{k-1}$

$$\begin{aligned}
&\leqslant \left(\tfrac{5}{3}\right)^k + \left(\tfrac{5}{3}\right)^{k-1} \qquad \{\text{using } *\} \\
&= \left(\tfrac{5}{3}\right)^{k+1}\left[\tfrac{3}{5} + \tfrac{9}{25}\right] \\
&= \left(\tfrac{5}{3}\right)^{k+1}\left[\tfrac{24}{25}\right] \\
&\leqslant \left(\tfrac{5}{3}\right)^{k+1}
\end{aligned}$$

Thus P_1 is true, and the assumed result for $r = 1, 2, 3, ..., k \Rightarrow$ the same result for $r = k + 1$.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

2 **Proof:**

(By the Principle of Mathematical Induction (strong form))

P_n is that "if $b_1 = b_2 = 1$ and $b_n = 2b_{n-1} + b_{n-2}$ for all $n \geqslant 3$, $n \in \mathbb{Z}^+$, then b_n is odd".

(1) b_1 and b_2 are odd

$\therefore$ P_1 and P_2 are true.

(2) Assume that b_r is odd for all $r \leqslant k$

$\therefore$ b_r is odd for $r = 1, 2, 3, ..., k$ .... $(*)$

Now $b_{k+1} = 2b_k + b_{k-1}$

$$\begin{aligned}
\therefore\ b_{k+1} &= 2(\text{odd}) + \text{odd} \qquad \{\text{using } *\} \\
&= \text{even} + \text{odd} \\
&= \text{odd}
\end{aligned}$$

Thus P_1 is true, and the assumed result for $r = 1, 2, 3, ..., k \Rightarrow$ the same result for $r = k + 1$.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

3 $f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, $f_7 = 13$, $f_8 = 21$, $f_9 = 34$, $f_{10} = 55$, $f_{11} = 89$

If $S_n = \sum\limits_{k=1}^{n} f_k$ then

$$\begin{aligned}
S_1 &= f_1 = 1 \\
S_2 &= f_1 + f_2 = 2 \\
S_3 &= f_1 + f_2 + f_3 = 4 \\
S_4 &= f_1 + f_2 + f_3 + f_4 = 7 \\
S_5 &= 12 \\
S_6 &= 20 \\
S_7 &= 33
\end{aligned}$$

We notice that

$$\begin{aligned}
S_1 &= f_3 - 1 \\
S_2 &= f_4 - 1 \\
S_3 &= f_5 - 1 \\
S_4 &= f_6 - 1 \\
&\ \ \vdots \\
&\text{etc}
\end{aligned}$$

So, we postulate that $S_n = f_{n+2} - 1$ for all $n \in \mathbb{Z}^+$.

Proof:

(By the Principle of Mathematical Induction (strong form))

P_n is that "if $S_1 = 1$ and $S_{n+1} = S_n + f_{n+1}$ for all $n \in \mathbb{Z}^+$, then $S_n = f_{n+2} - 1$".

(1) If $n = 1$, $S_1 = 1$ and $f_3 - 1 = 2 - 1 = 1$ ✓

$\therefore$ P_1 is true.

(2) Assume that $S_r = f_{r+2} - 1$ is true for all $r \leqslant t$

$\therefore$ $S_r = f_{r+2} - 1$ for $r = 1, 2, 3, ..., t$ .... $(*)$

Now $S_{t+1} = S_t + f_{t+1}$

$$\begin{aligned}
&= f_{t+2} - 1 + f_{t+1} \qquad \{\text{using } *\} \\
&= (f_{t+2} + f_{t+1}) - 1
\end{aligned}$$

$$\begin{aligned} &= f_{t+3} - 1 \\ &= f_{[t+1]+2} - 1 \end{aligned}$$

Thus P_1 is true, and the assumed result for $r = 1, 2, 3, ..., t \Rightarrow$ the same result for $r = t+1$.

Thus P_n is true for all $n \in \mathbb{Z}^+$.

4 a Proof:

(By the Principle of Mathematical Induction (strong form))

P_n is that "if $f_1 = f_2 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for all $n \geqslant 3$, $n \in \mathbb{Z}^+$, then $\left(\frac{3}{2}\right)^{n-2} < f_n < 2^{n-2}$".

(1) If $n = 3$, $\left(\frac{3}{2}\right)^1 < f_3 \leqslant 2^1$

$\therefore$ $\frac{3}{2} < 2 \leqslant 2$ which is true

$\therefore$ P_3 is true.

(2) Consider first proving $f_n > \left(\frac{3}{2}\right)^{n-2}$, $n \geqslant 3$

Assume that $f_r > \left(\frac{3}{2}\right)^{r-2}$ for all $3 \leqslant r \leqslant k$

$\therefore$ $f_r > \left(\frac{3}{2}\right)^{r-2}$ for $r = 3, 4, 5, ..., k$ .... (1)

Now $f_{k+1} = f_k + f_{k-1}$

$$\begin{aligned} &> \left(\tfrac{3}{2}\right)^{k-2} + \left(\tfrac{3}{2}\right)^{k-3} \qquad \{\text{using (1)}\} \\ &= \left(\tfrac{3}{2}\right)^{k-1} \left[\tfrac{2}{3} + \tfrac{4}{9}\right] \\ &= \left(\tfrac{3}{2}\right)^{k-1} \left(\tfrac{10}{9}\right) \\ &> \left(\tfrac{3}{2}\right)^{k-1} \end{aligned}$$

Secondly we prove that $f_n \leqslant 2^{n-2}$, $n \geqslant 3$

Assume that $f_r \leqslant 2^{r-2}$ for all $3 \leqslant r \leqslant k$

$\therefore$ $f_r \leqslant 2^{r-2}$ for $r = 3, 4, 5, ..., k$ .... (2)

Now $f_{k+1} = f_k + f_{k-1}$

$$\begin{aligned} &\leqslant 2^{k-2} + 2^{k-3} \qquad \{\text{using (2)}\} \\ &= 2^{k-1} \left[\tfrac{1}{2} + \tfrac{1}{4}\right] \\ &= 2^{k-1} \left(\tfrac{3}{4}\right) \\ &\leqslant 2^{k-1} \end{aligned}$$

Thus P_3 is true, and the assumed result for $r = 3, 4, 5, ..., k \Rightarrow$ the result for $r = k+1$.

$\therefore$ P_n is true for all $n \geqslant 3$, $n \in \mathbb{Z}^+$.

b Proof:

(By the Principle of Mathematical Induction (strong form))

P_n is that "if $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for all $n \in \mathbb{Z}^+$, then $\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} < f_n$".

(1) If $n = 1$, $\left(\frac{1+\sqrt{5}}{2}\right)^{-1} < f_1$ is true

as $\text{LHS} = \frac{2}{1+\sqrt{5}} < 1 = \text{RHS}$

(2) Assume that $\left(\frac{1+\sqrt{5}}{2}\right)^{r-2} < f_r$ is true for all $r \leqslant k$

$\therefore$ $\left(\frac{1+\sqrt{5}}{2}\right)^{r-2} < f_r$ for $r = 1, 2, 3, ..., k$ .... $(*)$

Now f_{k+1}

$$\begin{aligned} &= f_k + f_{k-1} \\ &> \left(\frac{1+\sqrt{5}}{2}\right)^{k-2} + \left(\frac{1+\sqrt{5}}{2}\right)^{k-3} \qquad \{\text{using } *\} \\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} \left[\frac{2}{1+\sqrt{5}} + \frac{4}{(1+\sqrt{5})^2}\right] \\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} [1] \\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} \end{aligned}$$

Thus $\left(\frac{1+\sqrt{5}}{2}\right)^{[k+1]-2} < f_{k+1}$.

Thus P_1 is true, and the assumed result for $r = 1, 2, 3, ..., k \Rightarrow$ the same result for $r = k+1$.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

5 As $f_{n+2} = f_{n+1} + f_n$, then $f_n = f_{n+2} - f_{n+1}$

Thus, $\displaystyle\sum_{k=1}^{n} f_n$

$$\begin{aligned} &= f_1 + f_2 + f_3 + ... + f_n \\ &= (\cancel{f_3} - f_2) + (\cancel{f_4} - \cancel{f_3}) + (\cancel{f_5} - \cancel{f_4}) + ... \\ &\qquad + (\cancel{f_{n+1}} - \cancel{f_n}) + (f_{n+2} - \cancel{f_{n+1}}) \\ &= f_{n+2} - f_2 \\ &= f_{n+2} - 1 \end{aligned}$$

6 Consider $\displaystyle\sum_{k=1}^{n} f_{2k-1} = S_n$, say

$$\begin{aligned} S_1 &= f_1 = 1 &&= f_2 \\ S_2 &= f_1 + f_3 = 1 + 2 = 3 &&= f_4 \\ S_3 &= 3 + f_5 = 3 + 5 = 8 &&= f_6 \\ S_4 &= 8 + f_7 = 8 + 13 = 21 &&= f_8 \\ S_5 &= 21 + f_9 = 21 + 34 = 55 &&= f_{10} \end{aligned}$$

As it appears that $S_n = f_{2n}$ for all $n \geqslant 1$, we postulate that

$$S_n = \sum_{k=1}^{n} f_{2k-1} = f_{2n}, \quad n \in \mathbb{Z}^+.$$

Proof: (By the Principle of Mathematical Induction)

P_n is that "$S_n = f_{2n}$" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $\text{LHS} = f_1 = 1$

$\text{RHS} = f_2 = 1$

$\therefore$ P_1 is true.

(2) If P_t is true, then $S_t = f_{2t}$, $t \in \mathbb{Z}^+$ .... $(*)$

Now $S_{t+1} = S_t + f_{2t+1}$

$$\begin{aligned} &= f_{2t} + f_{2t+1} \qquad \{\text{using } *\} \\ &= f_{2t+2} \\ &= f_{2(t+1)} \end{aligned}$$

Thus P_1 is true, and P_{t+1} is true whenever P_t is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

7 Let $\displaystyle\sum_{k=1}^{n} {f_k}^2 = S_n$, say

$$\begin{aligned} S_1 &= {f_1}^2 = 1 \times 1 = 1 \\ S_2 &= S_1 + {f_2}^2 = 1 + 1^2 = 2 \\ S_3 &= S_2 + {f_3}^2 = 2 + 2^2 = 6 \\ S_4 &= S_3 + {f_4}^2 = 6 + 3^2 = 15 \\ S_5 &= S_4 + {f_5}^2 = 15 + 5^2 = 40 \end{aligned}$$

Thus,
$$\begin{aligned} S_1 &= 1 \times 1 = f_1 f_2 \\ S_2 &= 1 \times 2 = f_2 f_3 \\ S_3 &= 2 \times 3 = f_3 f_4 \\ S_4 &= 3 \times 5 = f_4 f_5 \\ S_5 &= 5 \times 8 = f_5 f_6 \end{aligned}$$

As it appears that $S_n = f_n f_{n+1}$ for all $n \geqslant 1$ we postulate that $S_n = \sum_{k=1}^{n} f_k{}^2 = f_n f_{n+1}$, $n \in \mathbb{Z}^+$.

Proof: (By the Principle of Mathematical Induction)

P_n is that "$S_n = f_n f_{n+1}$" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $\text{LHS} = 1^2 = 1$

$\text{RHS} = 1 \times 1 = 1$

$\therefore$ P_1 is true.

(2) If P_t is true, then $S_t = f_t f_{t+1}$ .... $(*)$

Now
$$\begin{aligned} S_{t+1} &= S_t + f_{t+1}^2 \\ &= f_t f_{t+1} + f_{t+1}^2 \qquad \{\text{using } *\} \\ &= f_{t+1}[f_t + f_{t+1}] \\ &= f_{t+1} f_{t+2} \end{aligned}$$

Thus P_1 is true, and P_{t+1} is true whenever P_t is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

8 **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$f_{n+1} f_{n-1} - f_n^2 = (-1)^n$", $n \geqslant 2$, $n \in \mathbb{Z}^+$.

(1) If $n = 2$,
$$\begin{aligned} \text{LHS} &= f_3 f_1 - f_2{}^2 \\ &= 2 \times 1 - 1^2 \\ &= 1 \\ &= (-1)^2 \\ &= \text{RHS} \end{aligned}$$

$\therefore$ P_1 is true.

(2) If P_k is true, then $f_{k+1} f_{k-1} - f_k{}^2 = (-1)^k$ .... $(*)$

Now
$$\begin{aligned} & f_{k+2} f_k - f_{k+1}^2 \\ &= (f_{k+1} + f_k) f_k - f_{k+1}^2 \\ &= f_{k+1} f_k + f_k{}^2 - f_{k+1}^2 \\ &= f_{k+1} f_k + \left[f_{k+1} f_{k-1} - (-1)^k\right] - f_{k+1}^2 \\ & \qquad\qquad\qquad\qquad \{\text{using } *\} \\ &= f_{k+1}(f_k + f_{k-1}) + (-1)^{k+1} - f_{k+1}^2 \\ &= \cancel{f_{k+1}^2} + (-1)^{k+1} - \cancel{f_{k+1}^2} \\ &= (-1)^{k+1} \end{aligned}$$

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for $n \geqslant 2$, $n \in \mathbb{Z}^+$.

9 Let $S_n = \sum_{k=1}^{n} f_{2k}$
$$\therefore \quad \begin{aligned} S_1 &= f_2 = 1 \\ S_2 &= S_1 + f_4 = 1 + 3 = 4 \\ S_3 &= S_2 + f_6 = 4 + 8 = 12 \\ S_4 &= S_3 + f_8 = 12 + 21 = 33 \\ S_5 &= S_4 + f_{10} = 33 + 55 = 88 \end{aligned}$$

$$\begin{aligned} S_1 + 1 &= 2 = f_3 \\ S_2 + 1 &= 5 = f_5 \\ S_3 + 1 &= 13 = f_7 \\ S_4 + 1 &= 34 = f_9 \\ S_5 + 1 &= 89 = f_{11} \end{aligned}$$

$\therefore$ we postulate that $S_n = \sum_{k=1}^{n} f_{2k} = f_{2n+1} - 1$

Proof: (By the Principle of Mathematical Induction)

P_n is that "$S_n = f_{2n+1} - 1$" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $S_1 = 1$ and
$$\begin{aligned} f_{2n+1} - 1 &= f_3 - 1 \\ &= 2 - 1 \\ &= 1 \end{aligned}$$

$\therefore$ P_1 is true.

(2) If P_t is true, then $S_t = f_{2t+1} - 1$ .... $(*)$
$$\therefore \quad \begin{aligned} S_{t+1} &= S_t + f_{2t+2} \\ &= f_{2t+1} - 1 + f_{2t+2} \qquad \{\text{using } *\} \\ &= (f_{2t+1} + f_{2t+2}) - 1 \\ &= f_{2t+3} - 1 \\ &= f_{2(t+1)+1} - 1 \end{aligned}$$

Thus P_1 is true, and P_{t+1} is true whenever P_t is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

10 Let $S_n = \sum_{k=1}^{2n-1} f_k f_{k+1}$
$$\therefore \quad \begin{aligned} S_1 &= f_1 f_2 = 1 \times 1 = 1 \\ S_2 &= f_1 f_2 + f_2 f_3 + f_3 f_4 = 1 + 2 + 6 = 9 \\ S_3 &= f_1 f_2 + f_2 f_3 + f_3 f_4 + f_4 f_5 + f_5 f_6 \\ &= 9 + 15 + 40 \\ &= 64 \end{aligned}$$

As
$$\begin{aligned} S_1 &= 1^2 = f_2{}^2 \\ S_2 &= 3^2 = f_4{}^2 \\ S_3 &= 8^2 = f_6{}^2, \end{aligned}$$
we postulate that
$$S_n = \sum_{k=1}^{2n-1} f_k f_{k+1} = f_{2n}^2$$

Proof: (By the Principle of Mathematical Induction)

P_n is that "$S_n = (f_{2n})^2$" for all $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $S_1 = f_1 \times f_2 = 1 \times 1 = 1$ and $f_2{}^2 = 1^2 = 1$

$\therefore$ P_1 is true.

(2) If P_t is true then $S_t = (f_{2t})^2$ .... $(*)$

Now
$$\begin{aligned} S_{t+1} &= S_t + f_{2t} f_{2t+1} + f_{2t+1} f_{2t+2} \\ &= (f_{2t})^2 + f_{2t} f_{2t+1} + f_{2t+1}(f_{2t+1} + f_{2t}) \\ & \qquad\qquad\qquad\qquad\qquad\qquad \{\text{using } *\} \\ &= (f_{2t})^2 + 2(f_{2t} f_{2t+1}) + (f_{2t+1})^2 \\ &= (f_{2t} + f_{2t+1})^2 \\ &= (f_{2t+2})^2 \\ &= (f_{2(t+1)})^2 \end{aligned}$$

Thus P_1 is true, and P_{t+1} is true whenever P_t is true.

$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

11
$$\begin{aligned} & (f_n)^2 - (f_{n-1})^2 + (-1)^n \\ &= (f_n + f_{n-1})(f_n - f_{n-1}) + (-1)^n \\ &= f_{n+1}(f_n - f_{n-1}) + (-1)^n \\ &= f_n f_{n+1} - f_{n+1} f_{n-1} + (-1)^n \\ &= f_n f_{n+1} - \left[(f_n)^2 + (-1)^n\right] + (-1)^n \qquad \{\text{from } \mathbf{8}\} \\ &= f_n f_{n+1} - f_n^2 - \cancel{(-1)^n} + \cancel{(-1)^n} \\ &= f_n(f_{n+1} - f_n) \\ &= f_n f_{n-1} \qquad \{f_{n-1} + f_n = f_{n+1}\} \end{aligned}$$

Suppose f_{n-1} and f_n have some common factor $k > 1$.

$\therefore$ $k \mid f_{n-1}$ and $k \mid f_n$

$\therefore$ $k^2 \mid f_n \times f_{n-1}$ .... (1)

Also, $k^2 \mid (f_n)^2-(f_{n-1})^2$

$\therefore\ \ k^2 \nmid (f_n)^2-(f_{n-1})^2+(-1)^n$ for $k>1$ .... (2)

But (1) and (2) are contradictions since

$f_n \times f_{n-1} = (f_n)^2-(f_{n-1})^2+(-1)^n$

$\therefore$ f_{n-1} and f_n have no common factor besides 1.

12 **a** **Proof:**

(By the Principle of Mathematical Induction (strong form))

P_n is that

"if $f_1=f_2=1$ and $f_{n+2}=f_{n+1}+f_n$ for all $n\in\mathbb{Z}^+$,

then $f_n = a_n = \dfrac{1}{\sqrt5}\left(\dfrac{1+\sqrt5}{2}\right)^n - \dfrac{1}{\sqrt5}\left(\dfrac{1-\sqrt5}{2}\right)^n$".

(1) If $n=1$,

$$a_1 = \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right) - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)$$

$$= \frac{\cancel{1}+\sqrt5-\cancel{1}+\sqrt5}{2\sqrt5}$$

$$= \frac{2\sqrt5}{2\sqrt5} = 1 \quad \text{and} \quad f_1 = 1 \qquad \therefore\ P_1 \text{ is true.}$$

If $n=2$,

$$a_2 = \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^2 - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^2$$

$$= \frac{1}{4\sqrt5}\Big[(1+\sqrt5)+(1-\sqrt5)\Big]\Big[(1+\sqrt5)-(1-\sqrt5)\Big]$$

$$= \frac{1}{4\sqrt5}(2)(2\sqrt5) = 1 \quad \text{and} \quad f_2 = 1 \qquad \therefore\ P_2 \text{ is true.}$$

(2) Assume that

$$f_r = a_r = \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^r - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^r$$

is true for all $r \leqslant k$

$$\therefore\ \ f_r = \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^r - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^r$$

for $r = 1, 2, 3, ..., k$ .... $(*)$

Now

$$f_{k+1}$$

$$= f_k + f_{k-1}$$

$$= \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^k - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^k$$

$$+ \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^{k-1} - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^{k-1}$$

$\{$using $*\}$

$$= \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^{k+1}\left[\frac{2}{1+\sqrt5}+\left(\frac{2}{1+\sqrt5}\right)^2\right]$$

$$- \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^{k+1}\left[\frac{2}{1-\sqrt5}+\left(\frac{2}{1-\sqrt5}\right)^2\right]$$

where

$$\frac{2}{1+\sqrt5}+\left(\frac{2}{1+\sqrt5}\right)^2 \quad \text{and} \quad \frac{2}{1-\sqrt5}+\left(\frac{2}{1-\sqrt5}\right)^2$$

$$= \frac{2(1+\sqrt5)}{(1+\sqrt5)^2}+\frac{4}{(1+\sqrt5)^2} \qquad = \frac{2(1-\sqrt5)}{(1-\sqrt5)^2}+\frac{4}{(1-\sqrt5)^2}$$

$$= \frac{6+2\sqrt5}{(1+\sqrt5)^2} \qquad = \frac{6-2\sqrt5}{(1-\sqrt5)^2}$$

$$= \frac{6+2\sqrt5}{6+2\sqrt5} = 1 \qquad = 1 \text{ also}$$

$$\therefore\ \ f_{k+1} = \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^{k+1} - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^{k+1}$$

Thus P_1 (and P_2) are true, and the assumed result for $r = 1, 2, 3, ..., k \Rightarrow$ the same result for $r=k+1$.

Thus P_n is true for all $n\in\mathbb{Z}^+$.

b The strong form.

13 **Proof:** (By the Principle of Mathematical Induction)

P_n is that "f_{4n} is a multiple of 3" for all $n\in\mathbb{Z}^+$.

(1) If $n=1$, $f_{4n}=f_4=3$ which is a multiple of 3.

$\therefore$ P_1 is true.

(2) If P_k is true, then $f_{4k}=3A,\ A\in\mathbb{Z}$ .... $(*)$

Now
$$\begin{aligned}
f_{4(k+1)} &= f_{4k+4}\\
&= f_{4k+3}+f_{4k+2}\\
&= f_{4k+2}+f_{4k+1}+f_{4k+2}\\
&= 2f_{4k+2}+f_{4k+1}\\
&= 2\,[f_{4k+1}+f_{4k}]+f_{4k+1}\\
&= 3f_{4k+1}+2f_{4k}\\
&= 3f_{4k+1}+6A \qquad \{\text{using } *\}\\
&= 3\,[f_{4k+1}+2A]
\end{aligned}$$

where $f_{4k+1}+2A\in\mathbb{Z}$

$\therefore$ $f_{4(k+1)}$ is a multiple of 3.

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for all $n\in\mathbb{Z}^+$.

14 **a** $f_0=0$, $f_5=5$, and $f_{10}=55$

b **Proof:** (By the Principle of Mathematical Induction)

P_t is that "f_{5t} is a multiple of 5" for all $t\geqslant 0$.

(1) $f_0=0$ is a multiple of 5.

$\therefore$ P_0 is true.

(2) If P_k is true, then $f_{5k}=5A,\ A\in\mathbb{Z}$ .... $(*)$

Now
$$\begin{aligned}
f_{5(k+1)} &= f_{5k+5}\\
&= f_{5k+4}+f_{5k+3}\\
&= f_{5k+3}+f_{5k+2}+f_{5k+3}\\
&= 2f_{5k+3}+f_{5k+2}\\
&= 2\,[f_{5k+2}+f_{5k+1}]+f_{5k+2}\\
&= 3f_{5k+2}+2f_{5k+1}\\
&= 3\,[f_{5k+1}+f_{5k}]+2f_{5k+1}\\
&= 5f_{5k+1}+3f_{5k}\\
&= 5f_{5k+1}+3(5A) \qquad \{\text{from } *\}\\
&= 5\,[f_{5k+1}+3A]
\end{aligned}$$

where $f_{5k+1}+3A\in\mathbb{Z}$

$\therefore$ $f_{5(k+1)}$ is a multiple of 5.

Thus P_0 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_t is true for all $t\geqslant 0$.

EXERCISE 1B.1

1 **a** **i** $a_n=a_{n-1}+2$ for $n\geqslant 1$ and $a_0=12$.

$a_0=12$

$a_1=a_0+2=14$

$a_2=a_1+2=16$

$a_3=a_2+2=18$

$a_4=a_3+2=20$

Conjecture: $a_n=2n+12,\ n\in\mathbb{N}$.

ii For $n = 0,\ a_0 = 2(0) + 12 = 12$ ✓

If $a_k = 2k + 12$ then
$$\begin{aligned} a_{k+1} &= a_k + 2 \\ &= 2k + 12 + 2 \\ &= 2[k+1] + 12 \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = 2n + 12$ for all $n \in \mathbb{N}$.

b **i** $a_n = 3a_{n-1}$ for $n \geqslant 1$ and $a_0 = 10$.

$$\begin{aligned} a_0 &= 10 &&= 10 \times 3^0 \\ a_1 &= 3a_0 = 30 &&= 10 \times 3^1 \\ a_2 &= 3a_1 = 90 &&= 10 \times 3^2 \\ a_3 &= 3a_2 = 270 &&= 10 \times 3^3 \\ a_4 &= 3a_3 = 810 &&= 10 \times 3^4 \end{aligned}$$

Conjecture: $a_n = 10 \times 3^n,\ n \in \mathbb{N}$.

ii For $n = 0,\ a_0 = 10 \times 3^0 = 10$ ✓

If $a_k = 10 \times 3^k$ then
$$\begin{aligned} a_{k+1} &= 3a_k \\ &= 3 \times 10 \times 3^k \\ &= 10 \times 3^{k+1} \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = 10 \times 3^n$ for all $n \in \mathbb{N}$.

c **i** $a_{n+1} = 3a_n$ for $n \geqslant 1$ and $a_1 = 10$.

$$\begin{aligned} a_1 &= 10 &&= 10 \times 3^0 \\ a_2 &= 3a_1 = 30 &&= 10 \times 3^1 \\ a_3 &= 3a_2 = 90 &&= 10 \times 3^2 \\ a_4 &= 3a_3 = 270 &&= 10 \times 3^3 \\ a_5 &= 3a_4 = 810 &&= 10 \times 3^4 \end{aligned}$$

Conjecture: $a_n = 10 \times 3^{n-1},\ n \in \mathbb{Z}^+$.

ii For $n = 1,\ a_1 = 10 \times 1 = 10$ ✓

If $a_k = 10 \times 3^{k-1}$ then
$$\begin{aligned} a_{k+1} &= 3a_k \\ &= 3 \times 10 \times 3^{k-1} \\ &= 10 \times 3^k \\ &= 10 \times 3^{[k+1]-1} \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction,

$a_n = 10 \times 3^{n-1}$ for all $n \in \mathbb{Z}^+$.

d **i** $a_n = 2a_{n-1} + 10$ for $n \geqslant 1$ and $a_0 = 1$.

$$a_1 = 2a_0 + 10 = \underline{2 + 10} = 12$$

$$\begin{aligned} a_2 &= 2a_1 + 10 \\ &= 2(2 + 10) + 10 \\ &= \underline{2^2 + 2 \times 10 + 10} \\ &= 34 \end{aligned}$$

$$\begin{aligned} a_3 &= 2a_2 + 10 \\ &= 2(2^2 + 2 \times 10 + 10) + 10 \\ &= \underline{2^3 + 2^2 \times 10 + 2 \times 10 + 10} \\ &= 78 \end{aligned}$$

$$\begin{aligned} a_4 &= 2a_3 + 10 \\ &= 2(2^3 + 2^2 \times 10 + 2 \times 10 + 10) + 10 \\ &= \underline{2^4 + 2^3 \times 10 + 2^2 \times 10 + 2 \times 10 + 10} \\ &= 166 \end{aligned}$$

From the under-scored lines we conjecture that

$$a_n = 2^n + [2^{n-1} + 2^{n-2} + 2^{n-3} + \dots . + 2 + 1]10$$

$$\therefore\ a_n = 2^n + 10\left(\frac{2^n - 1}{2 - 1}\right) \qquad \{\text{sum of GS}\}$$

$$\therefore\ a_n = 2^n + 10(2^n - 1)$$

$$\therefore\ a_n = 11 \times 2^n - 10,\ n \in \mathbb{N}$$

ii For $n = 0,\ a_0 = 11 \times 2^0 - 10 = 1$ ✓

If $a_k = 11 \times 2^k - 10$

then
$$\begin{aligned} a_{k+1} &= 2a_k + 10 \\ &= 2[11 \times 2^k - 10] + 10 \\ &= 11 \times 2^{k+1} - 20 + 10 \\ &= 11 \times 2^{[k+1]} - 10 \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction,

$a_n = 11 \times 2^n - 10$ for all $n \in \mathbb{N}$.

e **i** $a_n = a_{n-1} + k$ for $n \geqslant 1$ and $a_0 = 0$.

$$\begin{aligned} a_0 &= 0 &&= 0k \\ a_1 &= a_0 + k = 0 + k &&= k \\ a_2 &= a_1 + k = k + k &&= 2k \\ a_3 &= a_2 + k = 2k + k &&= 3k \\ a_4 &= a_3 + k = 3k + k &&= 4k \end{aligned}$$

Conjecture: $a_n = nk,\ n \in \mathbb{N}$.

ii For $n = 0,\ a_0 = 0(k) = 0$ ✓

If $a_t = tk$

then
$$\begin{aligned} a_{t+1} &= a_t + k \\ &= tk + k \\ &= [t+1]k \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = nk$ for all $n \in \mathbb{N}$.

f **i** $a_n = ka_{n-1}$ for $n \in \mathbb{Z}^+$ and $a_0 = 1$.

$$\begin{aligned} a_0 &= 1 &&= k^0 \\ a_1 &= ka_0 = k \times 1 &&= k \\ a_2 &= ka_1 = k \times k &&= k^2 \\ a_3 &= ka_2 = k \times k^2 &&= k^3 \\ a_4 &= ka_3 = k \times k^3 &&= k^4 \end{aligned}$$

Conjecture: $a_n = k^n,\ n \in \mathbb{N}$.

ii For $n = 0,\ a_0 = k^0 = 1$ ✓

If $a_t = k^t$

then
$$\begin{aligned} a_{t+1} &= ka_t \\ &= k \times k^t \\ &= k^{t+1} \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = k^n$ for all $n \in \mathbb{N}$.

g **i** $a_n = na_{n-1},\ n \in \mathbb{Z}^+,\ n \geqslant 2$ and $a_1 = 1$.

$$\begin{aligned} a_1 &= 1 &&&&= 1! \\ a_2 &= 2a_1 = 2 \times 1 &&= 2 &&= 2! \\ a_3 &= 3a_2 = 3 \times 2 &&= 6 &&= 3! \\ a_4 &= 4a_3 = 4 \times 6 &&= 24 &&= 4! \\ a_5 &= 5a_4 = 5 \times 24 &&= 120 &&= 5! \end{aligned}$$

Conjecture: $a_n = n!$ for all $n \in \mathbb{Z}^+$.

ii For $n = 1,\ a_1 = 1! = 1$ ✓

If $a_k = k!$

then
$$\begin{aligned} a_{k+1} &= (k+1)a_k \\ &= (k+1)k! \\ &= (k+1)! \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = n!$ for all $n \in \mathbb{Z}^+$.

h **i** $x_{n+1} = x_n + (2n+3)$ for $n \in \mathbb{Z}^+$ and $x_0 = 1$.

$$\begin{aligned} x_0 &= 1 && = 1^2 \\ x_1 &= x_0 + 3 = 1 + 3 = 4 && = 2^2 \\ x_2 &= x_1 + 5 = 4 + 5 = 9 && = 3^2 \\ x_3 &= x_2 + 7 = 9 + 7 = 16 && = 4^2 \end{aligned}$$

Conjecture: $x_n = (n+1)^2$ for all $n \in \mathbb{N}$.

ii For $n = 0$, $x_0 = 1^2 = 1$ ✓

If $x_k = (k+1)^2$

then
$$\begin{aligned} x_{k+1} &= x_k + (2k+3) \\ &= (k+1)^2 + 2k + 3 \\ &= k^2 + 2k + 1 + 2k + 3 \\ &= k^2 + 4k + 4 \\ &= (k+2)^2 \\ &= ([k+1]+1)^2 \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $x_n = (n+1)^2$ for all $n \in \mathbb{N}$.

2 **a** 5, 7, 9, 11, ...

Recurrence relationship

$$a_n = a_{n-1} + 2 \quad \text{for} \quad n \in \mathbb{Z}^+ \quad \text{and} \quad a_0 = 5.$$

Closed form

$$a_n = 2n + 5, \quad n \in \mathbb{N}.$$

b 5, 6, 9, 14, 21, 30, ...

$$\begin{aligned} a_0 &= 5 \\ a_1 &= a_0 + 1 = 6 \\ a_2 &= a_1 + 3 = 9 \\ a_3 &= a_2 + 5 = 14 \\ a_4 &= a_3 + 7 = 21 \\ a_5 &= a_4 + 9 = 30 \end{aligned}$$

Recurrence relationship

$$a_n = a_{n-1} + (2n-1) \quad \text{for} \quad n \in \mathbb{Z}^+ \quad \text{and} \quad a_0 = 5.$$

$$\begin{aligned} a_0 &= 5 \\ a_1 &= 5 + 1 \\ a_2 &= 5 + 4 \\ a_3 &= 5 + 9 \\ a_4 &= 5 + 16 \\ a_5 &= 5 + 25 \end{aligned}$$

Closed form

$$a_n = 5 + n^2, \quad n \in \mathbb{N}.$$

c 5, 10, 20, 40, 80, ...

$$\begin{aligned} a_0 &= 5 \\ a_1 &= 2 \times 5 = 2a_0 \\ a_2 &= 2 \times a_1 \\ a_3 &= 2 \times a_2 \\ a_4 &= 2 \times a_3 \end{aligned}$$

Recurrence relationship

$$a_n = 2a_{n-1} \quad \text{for} \quad n \in \mathbb{Z}^+ \quad \text{and} \quad a_0 = 5.$$

Also
$$\begin{aligned} a_0 &= 5 \\ a_1 &= 2 \times 5 \\ a_2 &= 2^2 \times 5 \\ a_3 &= 2^3 \times 5 \\ a_4 &= 2^4 \times 5 \end{aligned}$$

Closed form

$$a_n = 5 \times 2^n, \quad n \in \mathbb{N}.$$

d 2, 8, 24, 64, 160, ...

$$\begin{aligned} a_0 &= 2 = 2 \times 1 \\ a_1 &= 8 = 2^2 \times 2 \\ a_2 &= 24 = 2^3 \times 3 \\ a_3 &= 64 = 2^4 \times 4 \\ a_4 &= 160 = 2^5 \times 5 \end{aligned}$$

Recurrence relationship

$$\frac{a_1}{a_0} = 2 \times \frac{2}{1}$$
$$\frac{a_2}{a_1} = 2 \times \frac{3}{2}$$
$$\frac{a_3}{a_2} = 2 \times \frac{4}{3}$$
$$\frac{a_4}{a_3} = 2 \times \frac{5}{4} \qquad \text{suggests} \quad \frac{a_n}{a_{n-1}} = 2 \times \frac{n+1}{n}$$

$$\therefore \quad a_n = 2\left(\frac{n+1}{n}\right) a_{n-1} \quad \text{for} \quad n \geqslant 1, \quad \text{and} \quad a_0 = 2.$$

Closed form $\quad a_n = 2^{n+1}(n+1), \quad n \in \mathbb{N}.$

e This is the Fibonacci sequence with

Recurrence relationship

$$a_{n+2} = a_{n+1} + a_n, \quad a_0 = a_1 = 1, \quad n \in \mathbb{N}.$$

Closed form (previously found)

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n, \quad n \in \mathbb{N}.$$

3 **a** $a_n = a_{n-1} + 2n - 1, \quad n \in \mathbb{Z}^+, \quad a_0 = 0.$

i
$$\begin{aligned} a_1 &= a_0 + 1 = 0 + 1 = 1 && = 1^2 \\ a_2 &= a_1 + 3 = 1 + 3 = 4 && = 2^2 \\ a_3 &= a_2 + 5 = 4 + 5 = 9 && = 3^2 \\ a_4 &= a_3 + 7 = 9 + 7 = 16 && = 4^2 \end{aligned}$$

Conjecture: $a_n = n^2$ for all $n \in \mathbb{N}$

ii For $n = 0$, $a_0 = 0^2 = 0$ ✓

If $a_k = k^2$ then
$$\begin{aligned} a_{k+1} &= a_k + 2(k+1) - 1 \\ &= k^2 + 2k + 2 - 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = n^2$ for all $n \in \mathbb{N}$.

iii $a_{100} = 100^2 = 100\,000$

b $a_n = a_{n-1} + 2n + 1, \quad n \in \mathbb{Z}^+, \quad a_0 = 1.$

i
$$\begin{aligned} a_1 &= a_0 + 3 = 1 + 3 && = 4 && = 2^2 \\ a_2 &= a_1 + 5 = 4 + 5 && = 9 && = 3^2 \\ a_3 &= a_2 + 7 = 9 + 7 && = 16 && = 4^2 \\ a_4 &= a_3 + 9 = 16 + 9 && = 25 && = 5^2 \end{aligned}$$

Conjecture: $a_n = (n+1)^2, \quad n \in \mathbb{N}$

ii For $n = 0$, $a_0 = 1^2 = 1$ ✓

If $a_k = (k+1)^2$

then
$$\begin{aligned} a_{k+1} &= a_k + 2(k+1) + 1 \\ &= (k+1)^2 + 2k + 3 \\ &= k^2 + 2k + 1 + 2k + 3 \\ &= k^2 + 4k + 4 \\ &= (k+2)^2 = ([k+1]+1)^2 \end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = (n+1)^2$ for all $n \in \mathbb{N}$.

iii $a_{100} = (101)^2 = 10\,201$

c $a_n = a_{n-1} + n$ for $n \in \mathbb{Z}^+$ and $a_0 = 0$.

i
$$\begin{aligned}
a_0 &= 0 && = \frac{0 \times 1}{2}\\
a_1 &= a_0 + 1 = 0 + 1 = 1 && = \frac{1 \times 2}{2}\\
a_2 &= a_1 + 2 = 1 + 2 = 3 && = \frac{2 \times 3}{2}\\
a_3 &= a_2 + 3 = 3 + 3 = 6 && = \frac{3 \times 4}{2}\\
a_4 &= a_3 + 4 = 6 + 4 = 10 && = \frac{4 \times 5}{2}
\end{aligned}$$

Conjecture: $a_n = \dfrac{n(n+1)}{2}$ for $n \in \mathbb{N}$

ii For $n = 0$, $a_0 = \dfrac{0 \times 1}{2} = 0$ $\checkmark$

If $a_k = \dfrac{k(k+1)}{2}$

then
$$\begin{aligned}
a_{k+1} &= a_k + (k+1)\\
&= \frac{k(k+1)}{2} + (k+1)\left(\frac{2}{2}\right)\\
&= \frac{k+1}{2}[k+2]\\
&= \frac{(k+1)([k+1]+1)}{2}
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction,

$a_n = \dfrac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

iii $a_{100} = \dfrac{100 \times 101}{2} = 5050$

d $a_n = a_{n-1} + n + 1$ for $n \in \mathbb{Z}^+$ and $a_0 = 1$.

i
$$\begin{aligned}
a_0 &= 1 && = \frac{1 \times 2}{2}\\
a_1 &= a_0 + 2 = 1 + 2 = 3 && = \frac{2 \times 3}{2}\\
a_2 &= a_1 + 3 = 3 + 3 = 6 && = \frac{3 \times 4}{2}\\
a_3 &= a_2 + 4 = 6 + 4 = 10 && = \frac{4 \times 5}{2}\\
a_4 &= a_3 + 5 = 10 + 5 = 15 && = \frac{5 \times 6}{2}
\end{aligned}$$

Conjecture: $a_n = \dfrac{(n+1)(n+2)}{2}$, $n \in \mathbb{N}$

ii For $n = 0$, $a_0 = \dfrac{1 \times 2}{2} = 1$ $\checkmark$

If $a_k = \dfrac{(k+1)(k+2)}{2}$

then
$$\begin{aligned}
a_{k+1} &= a_k + k + 2\\
&= \frac{(k+1)(k+2)}{2} + (k+2)\left(\frac{2}{2}\right)\\
&= \frac{k+2}{2}[k+1+2]\\
&= \frac{(k+2)(k+3)}{2}\\
&= \frac{([k+1]+1)([k+1]+2)}{2}
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction,

$a_n = \dfrac{(n+1)(n+2)}{2}$ for all $n \in \mathbb{N}$.

iii $a_{100} = \dfrac{101 \times 102}{2} = 5151$

e $a_n = a_{n-1} + n^3$ for $n \in \mathbb{Z}^+$, $a_0 = 0$.

i
$$\begin{aligned}
a_0 &= 0 && && = 0^2\\
a_1 &= a_0 + 1^3 = 0 + 1 && = 1 && = 1^2\\
a_2 &= a_1 + 2^3 = 1 + 8 && = 9 && = 3^2\\
a_3 &= a_2 + 3^3 = 9 + 27 && = 36 && = 6^2\\
a_4 &= a_3 + 4^3 = 36 + 64 && = 100 && = 10^2
\end{aligned}$$

Conjecture: Using **c**, $a_n = \left[\dfrac{n(n+1)}{2}\right]^2$, $n \in \mathbb{N}$

ii For $n = 0$, $a_0 = \left[\dfrac{0 \times 1}{2}\right]^2 = 0$ $\checkmark$

If $a_k = \left[\dfrac{k(k+1)}{2}\right]^2$

then
$$\begin{aligned}
a_{k+1} &= a_k + (k+1)^3\\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3\left(\frac{4}{4}\right)\\
&= \frac{(k+1)^2[k^2+4k+4]}{4}\\
&= \frac{(k+1)^2(k+2)^2}{4}\\
&= \left[\frac{(k+1)([k+1]+1)}{2}\right]^2
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction,

$a_n = \left[\dfrac{n(n+1)}{2}\right]^2$ for all $n \in \mathbb{N}$.

iii $a_{100} = \left[\dfrac{100 \times 101}{2}\right]^2 = 25\,502\,500$

f $a_n = (n+1)a_{n-1}$ for $n \in \mathbb{Z}^+$ and $a_0 = 1$.

i
$$\begin{aligned}
a_0 &= 1 && = 1!\\
a_1 &= 2a_0 = 2 \times 1 && = 2!\\
a_2 &= 3a_1 = 3 \times 2 \times 1 && = 3!\\
a_3 &= 4a_2 = 4 \times 3 \times 2 \times 1 && = 4!
\end{aligned}$$

Conjecture: $a_n = (n+1)!$, $n \in \mathbb{N}$

ii For $n = 0$, $a_0 = 1! = 1$ $\checkmark$

If $a_k = (k+1)!$

then
$$\begin{aligned}
a_{k+1} &= (k+2)a_k\\
&= (k+2)(k+1)!\\
&= (k+2)!\\
&= ([k+1]+1)!
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = (n+1)!$ for all $n \in \mathbb{N}$.

iii $a_{100} = 101!$

4 $a_0 = c$ and $a_n = ra_{n-1}$, $n \in \mathbb{Z}^+$

a
$$\begin{aligned}
a_0 &= c\\
a_1 &= ra_0 = rc\\
a_2 &= ra_1 = r(rc) = r^2c\\
a_3 &= ra_2 = r(r^2c) = r^3c
\end{aligned}$$

b *Conjecture*: $a_n = cr^n$, $n \in \mathbb{N}$.

5 $a_0 = c$ and $a_n = a_{n-1} + b$, $n \in \mathbb{Z}^+$

a
$$\begin{aligned}
a_0 &= c\\
a_1 &= a_0 + b = c + b
\end{aligned}$$

$a_2 = a_1 + b = c + b + b = c + 2b$

$a_3 = a_2 + b = c + 2b + b = c + 3b$

b *Conjecture*: $a_n = c + nb, \; n \in \mathbb{N}.$

6 $a_0 = c, \; a_n = ra_{n-1} + b, \; n \in \mathbb{Z}^+$

a $a_0 = c$

$a_1 = ra_0 + b = rc + b$

$a_2 = ra_1 + b = r(rc + b) + b$

$\quad = r^2c + rb + b$

$a_3 = ra_2 + b = r(r^2c + rb + b) + b$

$\quad = r^3c + r^2b + rb + b$

$a_4 = ra_3 + b = r(r^3c + r^2b + rb + b) + b$

$\quad = r^4c + r^3b + r^2b + rb + b$

b *Conjecture*:

$a_n = r^nc + r^{n-1}b + r^{n-2}b + ... + rb + b$

$\therefore \; a_n = r^nc + b(r^{n-1} + r^{n-2} + ... + r + 1)$

That is, $a_n = r^nc + b\left(\dfrac{r^n - 1}{r - 1}\right), \; n \in \mathbb{N}$

{using sum of a GS}

7 $a_n = a_{n-1} + a_{n-2} - a_{n-3}, \; n \geqslant 3, \; n \in \mathbb{Z}$

a No, as initial values of a_0, a_1, and a_2 are needed.

b If $a_n = c, \; n \in \mathbb{N}$ then for $n \geqslant 3$,

$a_{n-3} = a_{n-2} = a_{n-1} = c.$

$\therefore \quad a_{n-1} + a_{n-2} - a_{n-3}$

$= c + c - c$

$= c$

$= a_n$

$\therefore \; a_n = c$ for $n \in \mathbb{N}$ is a closed form solution.

c If $a_n = cn + d, \; n \in \mathbb{N}$ then for $n \geqslant 3$

$a_{n-1} = c(n-1) + d$

$a_{n-2} = c(n-2) + d$

$a_{n-3} = c(n-3) + d$

$\therefore \quad a_{n-1} + a_{n-2} - a_{n-3}$

$= cn - \cancel{c} + d + \cancel{cn} - \cancel{2c} + \cancel{d} - \cancel{cn} + \cancel{3c} - \cancel{d}$

$= cn + d$

$= a_n$

$\therefore \; a_n = cn + d$ for $n \in \mathbb{N}$ is a closed form solution.

8 $a_0 = c, \; a_n = a_{n-1} + n^2, \; n \in \mathbb{Z}^+$

$a_1 = a_0 + 1^2 = c + 1^2$

$a_2 = a_1 + 2^2 = c + 1^2 + 2^2$

$a_3 = a_2 + 3^2 = c + 1^2 + 2^2 + 3^2$

$a_4 = a_3 + 4^2 = c + 1^2 + 2^2 + 3^2 + 4^2$

$\vdots$

$a_n = c + 1^2 + 2^2 + 3^2 + ... + (n-1)^2 + n^2$

$$\therefore \; a_n = c + \sum_{i=1}^{n} i^2$$

$$\therefore \; a_n = c + \frac{n(n+1)(2n+1)}{6}, \; n \in \mathbb{N}.$$

EXERCISE 1B.2

1 **a** homogeneous with constant coefficients

$\therefore \; a_n = r^nc$ where $c = 0, \; r = 100$

$\therefore \; a_n = 100^n \times 0$

$\therefore \; a_n = 0, \; n \in \mathbb{N}$

b homogeneous with constant coefficients

$\therefore \; a_n = r^nc$ where $c = 3, \; r = 100 = 10^2$

$\therefore \; a_n = (10^2)^n \times 3$

$\therefore \; a_n = 3 \times 10^{2n}, \; n \in \mathbb{N}$

c homogeneous with constant coefficients

$\therefore \; a_n = r^{n-1}c$ where $c = 500, \; r = 10$

{exponent is $n - 1$ since the initial term is a_1}

$\therefore \; a_n = 10^{n-1} \times 500$

$\therefore \; a_n = 5 \times 10^{n+1}, \; n \in \mathbb{Z}^+$

d inhomogeneous with constant coefficient of 1

$\therefore \; a_n = c + nb$ where $c = 3, \; b = -5$

$\therefore \; a_n = 3 + n \times -5$

$\therefore \; a_n = 3 - 5n, \; n \in \mathbb{N}$

e inhomogeneous with constant coefficient of 1

$\therefore \; a_n = c + nb$ where $c = 0, \; b = 1$

$\therefore \; a_n = 0 + n \times 1$

$\therefore \; a_n = n, \; n \in \mathbb{N}$

f inhomogeneous with constant coefficient of 1

$\therefore \; a_n = c + (n-2)b$ where $c = -17, \; b = -4$

{coefficient of b is $n - 2$ since the initial term is a_2}

$\therefore \; a_n = -17 + (n-2)(-4)$

$\therefore \; a_n = -9 - 4n, \; n \in \mathbb{Z}^+, \; n \geqslant 2$

g inhomogeneous with constant coefficient $r \neq 1$

$\therefore \; a_n = r^nc + b\left(\dfrac{r^n - 1}{r - 1}\right)$

where $c = 1, \; r = 3, \; b = 5$

$\therefore \; a_n = 3^n \times 1 + 5\left(\dfrac{3^n - 1}{3 - 1}\right)$

$\therefore \; a_n = 3^n + 5\left(\dfrac{3^n - 1}{2}\right)$

$\therefore \; a_n = 3^n + \frac{5}{2}3^n - \frac{5}{2}$

$\therefore \; a_n = \left(\frac{7}{2}\right)3^n - \frac{5}{2}$

or $a_n = \dfrac{7(3^n) - 5}{2}, \; n \in \mathbb{N}$

h inhomogeneous with constant coefficient $r \neq 1$

$\therefore \; a_n = r^nc + b\left(\dfrac{r^n - 1}{r - 1}\right)$

where $c = 3, \; r = -2, \; b = 6$

$\therefore \; a_n = 3(-2)^n + 6\left(\dfrac{(-2)^n - 1}{-2 - 1}\right)$

$\therefore \; a_n = 3(-2)^n - 2[(-2)^n - 1]$

$\therefore \; a_n = 3(-2)^n - 2(-2)^n + 2$

$\therefore \; a_n = (-2)^n + 2, \; n \in \mathbb{N}$

i inhomogeneous with constant coefficient $r \neq 1$

$\therefore \; a_n = r^nc + b\left(\dfrac{r^n - 1}{r - 1}\right)$

where $c = 0, \; r = 5, \; b = 3$

$\therefore \; a_n = 5^n(0) + 3\left(\dfrac{5^n - 1}{4}\right)$

$\therefore \; a_n = \frac{3}{4}(5^n - 1), \; n \in \mathbb{N}$

2 **a** $a_n = 3a_{n-1}, \; n \in \mathbb{Z}^+$

b $a_n = 3^n \times a_0$

$\therefore \; a_n = a_0(3^n), \; n \in \mathbb{N}$

c **i**
$$\begin{aligned} a_6 &= 20\,000 \\ \therefore\ a_0 \times 3^6 &= 20\,000 \\ \therefore\ a_0 &= \frac{20\,000}{3^6} \approx 27.4 \\ \therefore\ a_0 &= 27 \text{ cells} \end{aligned}$$

ii
$$\begin{aligned} a_{24} &= 27 \times 3^{24} \\ &\approx 7.63 \times 10^{12} \text{ cells} \end{aligned}$$

iii If $a_n = 51\,000\,000$, then
$$\begin{aligned} 27 \times 3^n &= 51\,000\,000 \\ \therefore\ 3^n &\approx 1.888\,89 \times 10^6 \\ \therefore\ n \ln 3 &\approx \ln(1.888\,89 \times 10^6) \\ \therefore\ n &\approx \frac{14.451....}{1.0986....} \\ \therefore\ n &\approx 13.15 \text{ hours} \\ \therefore\ n &\approx 13 \text{ hours } 9.259 \text{ min} \\ \therefore\ n &\approx 13 \text{ hours } 10 \text{ min} \end{aligned}$$

3
$a_0 = 1$ {the empty string is unique}

$a_1 = 2$ {0, 1}

$a_2 = 4$ {00, 01, 10, 11}

$a_3 = 8$ {000, 100, 010, 001, 110, 101, 011, 111}

$a_n = 2a_{n-1}$ for $n \in \mathbb{Z}^+$ and $a_0 = 1$

$\therefore\ a_n = 2^n,\ n \in \mathbb{N}$

4 **a**
$$\begin{aligned} a_0 &= 500 \\ a_1 &= 500 \times 1.1 = 550 \\ a_2 &= 500 \times 1.1^2 = 605 \\ a_3 &= 500 \times 1.1^3 = 665.50 \end{aligned}$$

b $a_n = a_{n-1} \times 1.1,\ a_0 = 500$

c $a_n = 500 \times (1.1)^n,\ n \in \mathbb{N}$

d
$$\begin{aligned} a_{10} &= 500 \times (1.1)^{10} \\ &\approx 1296.87 \end{aligned}$$

$\therefore$ the investment is worth $\approx$ \$1296.87 .

e When $a_n = 1000$
$$\begin{aligned} (1.1)^n &= 2 \\ \therefore\ n \ln(1.1) &= \ln 2 \\ \therefore\ n &= \frac{\ln 2}{\ln 1.1} \\ \therefore\ n &\approx 7.2725 \end{aligned}$$

$\therefore$ the initial value will be doubled in 7 years and 100 days.

5 **a**
$$\begin{aligned} a_n &= ra_{n-1},\ n \geqslant 1 \\ \therefore\ a_n &= r^n a_0,\ n \in \mathbb{N} \end{aligned}$$

b **i** $r = 100\% + 12\% = 112\% = 1.12$

ii $r = 100\% + \frac{12\%}{4} = 103\% = 1.03$

iii $r = 100\% + \frac{12\%}{12} = 101\% = 1.01$

c **i** $a_3 = (1.12)^3 \times 10\,500 \approx 14\,751.74$

$\therefore$ the investment is worth $\approx$ \$14 751.74 .

ii 3 years corresponds to $3 \times 4 = 12$ compounding periods.

$a_{12} = (1.03)^{12} \times 10\,500 \approx 14\,970.49$

$\therefore$ the investment is worth $\approx$ \$14 970.49 .

iii 3 years corresponds to $3 \times 12 = 36$ compounding periods.

$a_{36} = (1.01)^{36} \times 10\,500 \approx 15\,023.07$

$\therefore$ the investment is worth $\approx$ \$15 023.07 .

6 **a**
$$\begin{aligned} a_n &= 85\% \text{ of } a_{n-1}, \quad a_0 = \text{initial mass} \\ \therefore\ a_n &= 0.85a_{n-1}, \quad a_0 = \text{initial mass} \\ \therefore\ a_n &= (0.85)^n \times a_0,\ n \in \mathbb{N} \end{aligned}$$

b But when $n = 7,\ a_7 = 80$
$$\begin{aligned} \therefore\ 80 &= (0.85)^7 \times a_0 \\ \therefore\ a_0 &= \frac{80}{(0.85)^7} \\ \therefore\ a_0 &\approx 249.55 \end{aligned}$$

$\therefore$ an initial mass of $\approx$ 250 g is necessary.

7 **a** **i** $a_0 = 1000$

ii
$$\begin{aligned} a_1 &= 1000 \times 1.048 + 100 \\ &= 1148 \end{aligned}$$

iii
$$\begin{aligned} a_2 &= a_1 \times 1.048 + 100 \\ &\approx 1303.10 \end{aligned}$$

iv
$$\begin{aligned} a_3 &= a_2 \times 1.048 + 100 \\ &\approx 1465.65 \end{aligned}$$

b $a_n = a_{n-1} \times 1.048 + 100$ for $n \in \mathbb{Z}^+,\ a_0 = 1000$

which has $c = 1000,\ r = 1.048,\ b = 100$

$$\therefore\ a_n = (1.048)^n \times 1000 + 100\left(\frac{1.048^n - 1}{1.048 - 1}\right),\ n \in \mathbb{N}$$

c If the investment doubles, $a_n = 2000$.

If $(1.048)^n 1000 + 100\left(\dfrac{1.048^n - 1}{1.048 - 1}\right) = 2000$

then $n \approx 5.9914$

{using technology}

$\therefore$ 6 years are needed to reach \$2000.

8 **a**
$$\begin{aligned} a_0 &= 800 \\ a_1 &= 800 \times 2 \\ a_2 &= a_1 \times 2 = 800 \times 2^2 \end{aligned}$$

$a_n = 2a_{n-1}$ for $n \in \mathbb{Z}^+$ and $a_0 = 800$

$\therefore\ a_n = 2^n \times 800,\ n \in \mathbb{N}$.

b In one day $n = 8$

and
$$\begin{aligned} a_8 &= 2^8 \times 800 \\ &= 204\,800 \end{aligned}$$

$\therefore$ 204 800 bacteria are present after 1 day.

c We need to solve $a_n = 1\,000\,000$
$$\begin{aligned} 2^n \times 800 &= 1\,000\,000 \\ \therefore\ 2^n &= 1250 \\ \therefore\ n &= \frac{\ln 1250}{\ln 2} \\ \therefore\ 3n &= \frac{3 \ln 1250}{\ln 2} \\ \therefore\ 3n &= 30.863.... \end{aligned}$$

$\therefore$ 31 hours are needed.

9 **a**
$$\begin{aligned} a_0 &= 2000 - 1600 = 400 \\ a_1 &= a_0 + 2000 \times 1.01 - 1600 \\ a_2 &= a_1 + 2000 \times 1.01^2 - 1600 \\ &\ \vdots \end{aligned}$$

$a_n = a_{n-1} + 2000 \times 1.01^n - 1600,\ n \in \mathbb{Z}^+$

Now
$$\begin{aligned} a_n - \cancel{a_{n-1}} &= 2000(1.01^n) - 1600 \\ \cancel{a_{n-1}} - \cancel{a_{n-2}} &= 2000(1.01^{n-1}) - 1600 \\ \cancel{a_{n-2}} - \cancel{a_{n-3}} &= 2000(1.01^{n-2}) - 1600 \\ &\ \vdots \\ \cancel{a_2} - \cancel{a_1} &= 2000(1.01^2) - 1600 \\ \cancel{a_1} - a_0 &= 2000(1.01) - 1600 \end{aligned}$$

Adding vertically

$$a_n - a_0 = 2000 \times 1.01[1 + 1.01 + 1.01^2 + ... + 1.01^{n-1}] - n \times 1600$$

$$\therefore \quad a_n - 400 = 2020\left(\frac{1.01^n - 1}{1.01 - 1}\right) - 1600n$$

$$\therefore \quad a_n = 202\,000(1.01^n - 1) - 1600n + 400, \quad n \in \mathbb{N}.$$

b **i** $a_{12} = 202\,000(1.01^{12} - 1) - 1600 \times 12 + 400$

≈ 6819

∴ the amount of steel held in stock after 12 months is ≈ 6819 tonnes.

ii $a_{24} = 202\,000(1.01^{24} - 1) - 1600 \times 24 + 400$

$\approx 16\,486$

∴ the amount of steel held in stock after 2 years is ≈ 16 486 tonnes.

c If $202\,000(1.01^n - 1) - 1600n + 400 = 30\,000$

then $n \approx 36.14$ {using technology}

∴ it will take about 37 months to reach 30 000 tonnes.

10 **a** $a_0 = 5000$

$a_1 = 5000 \times 1.0075 + 40 \qquad \left\{ \begin{array}{l} r = 1 + \frac{0.09}{12} \\ \quad = 1.0075 \end{array} \right\}$

≈ 5077.50

$a_2 = a_1 \times 1.0075 + 40$

≈ 5155.58

$a_3 = a_2 \times 1.0075 + 40$

≈ 5234.25

b $a_n = a_{n-1} \times 1.0075 + 40$, for $n \in \mathbb{Z}^+$ and $a_0 = 5000$ which has $c = 5000$, $r = 1.0075$, $b = 40$

$$\therefore \quad a_n = 5000(1.0075)^n + 40\left(\frac{1.0075^n - 1}{1.0075 - 1}\right), \quad n \in \mathbb{N}$$

c After 4 years, $n = 4 \times 12 = 48$ months

$$\text{and} \quad a_{48} = 5000(1.0075)^{48} + 40\left(\frac{1.0075^{48} - 1}{1.0075 - 1}\right)$$

∴ $a_{48} \approx 9457.86$

∴ after 4 years the investment is worth ≈ £9457.86 .

d If $5000(1.0075)^n + 40\left(\frac{1.0075^n - 1}{1.0075 - 1}\right) = 15\,000$

then $n \approx 90.59$ {using technology}

∴ it will take ≈ 7 years and 7 months to reach £15 000.

11 **a** $a_0 = 3000$

$a_1 = 3000 \times 1.02 - 200 \approx 2860 \qquad \left\{ \begin{array}{l} r = 1 + \frac{0.24}{12} \\ \quad = 1.02 \end{array} \right\}$

$a_2 = a_1 \times 1.02 - 200 \approx 2717.20$

$a_3 = a_2 \times 1.02 - 200 \approx 2571.54$

b $a_n = 1.02 \times a_{n-1} - 200$, $n \in \mathbb{Z}^+$ and $a_0 = 3000$ which has $c = 3000$, $r = 1.02$, $b = -200$

$$a_n = 3000(1.02)^n - 200\left(\frac{1.02^n - 1}{0.02}\right)$$

$$\therefore \quad a_n = 3000(1.02)^n - 10\,000(1.02^n - 1)$$

$$\therefore \quad a_n = 10\,000 - 7000(1.02)^n, \quad n \in \mathbb{N}$$

c $10\,000 - 7000(1.02)^n = 0$

$$\therefore \quad (1.02)^n = \tfrac{10\,000}{7000} = \tfrac{10}{7}$$

$$\therefore \quad n = \frac{\ln\left(\frac{10}{7}\right)}{\ln(1.02)}$$

$$\therefore \quad n \approx 18.011$$

∴ the loan would take 18 months to repay with a very small additional repayment at the end of the 19th month.

12 **a** $a_0 = a_0$

$a_1 = ra_0 - p$

$a_2 = ra_1 - p$

$a_3 = ra_2 - p$ and in general

$a_n = ra_{n-1} - p$ for $n \in \mathbb{Z}^+$, $a_0 = a_0$

b $c = a_0$, $r = r$, $b = -p$

$$\therefore \quad a_n = r^n a_0 - p\left(\frac{r^n - 1}{r - 1}\right), \quad n \in \mathbb{N}.$$

13 **a** First interest added

$= \frac{13\%}{26} \times \$20\,000$

$= \$\left(\frac{0.13}{26} \times 20\,000\right)$

$= \$100$

So, to reduce the loan amount, a fortnightly repayment of more than $100 must be made.

b **i** $a_0 = 20\,000$

$a_1 = 20\,000 \times 1.005 - 200 \qquad \{r = 1 + \frac{0.13}{26} = 1.005\}$

$= 19\,900$

$a_2 = a_1 \times 1.005 - 200$

$= 19\,799.50$

$a_3 = a_2 \times 1.005 - 200$

$\approx 19\,698.50$

ii The recurrence relationship is $a_n = a_{n-1} \times 1.005 - 200$ for $n \in \mathbb{Z}^+$ and $a_0 = 20\,000$.

iii $c = 20\,000$, $r = 1.005$, $b = -200$

$$\therefore \quad a_n = (1.005^n)20\,000 - 200\left(\frac{1.005^n - 1}{1.005 - 1}\right)$$

$$\therefore \quad a_n = 20\,000(1.005^n) - 40\,000(1.005^n - 1)$$

$$\therefore \quad a_n = 40\,000 - 20\,000(1.005^n), \quad n \in \mathbb{N}$$

iv 2 years corresponds to

$2 \times 26 = 52$ fortnightly repayments

$a_{52} = 40\,000 - 20\,000(1.005^{52}) \approx 14\,078.20$

∴ the outstanding debt is about $14 078.20 .

v $40\,000 - 20\,000(1.005^n) = 0$

$$\therefore \quad 1.005^n = \frac{40\,000}{20\,000} = 2$$

$$\therefore \quad n = \frac{\ln 2}{\ln(1.005)}$$

$$\therefore \quad n \approx 138.975....$$

∴ 139 fortnights are needed or 5 years, 18 weeks.

vi The total cost ≈ 139 payments of $200

≈ $27 800

∴ total interest paid ≈ $27 800 − $20 000

≈ $7800

c **i** 4 years corresponds to

$4 \times 26 = 104$ fortnightly repayments.

$$1.005^{104} \times 20\,000 - p\left(\frac{1.005^{104} - 1}{1.005 - 1}\right) = 0$$

$$\therefore \quad p\left(\frac{1.005^{104} - 1}{0.005}\right) = 20\,000 \times 1.005^{104}$$

$$\therefore \quad p = \frac{20\,000 \times 1.005^{104} \times 0.005}{1.005^{104} - 1}$$

$$\therefore \quad p \approx 247.091$$

∴ to pay off the loan in 4 years, a fortnightly repayment of $247.10 is needed.

ii Total cost $\approx \$247.10 \times 104$

$\approx \$25\,700$

$\therefore$ total interest $\approx \$25\,700 - \$20\,000$

$\approx \$5700$

EXERCISE 1B.3

1 **a** $a_0 = 0,\ \ a_1 = 1,\ \ a_2 = 2$

$a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3},\ \ n \geqslant 3$

$$\begin{aligned}\therefore\ \ a_3 &= 3a_2 - 3a_1 + a_0\\ &= 3(2) - 3(1) + 0\\ &= 3\\ a_4 &= 3a_3 - 3a_2 + a_1\\ &= 3(3) - 3(2) + 1\\ &= 4\\ a_5 &= 3a_4 - 3a_3 + a_2\\ &= 3(4) - 3(3) + 2\\ &= 5\\ a_6 &= 3a_5 - 3a_4 + a_3\\ &= 3(5) - 3(4) + 3\\ &= 6\\ a_7 &= 3a_6 - 3a_5 + a_4\\ &= 3(6) - 3(5) + 4\\ &= 7\end{aligned}$$

b $a_n = n$ for all $n \in \mathbb{N}$.

c $a_0 = 0,\ \ a_1 = 1,\ \ a_2 = 2$ ✓

If $a_k = k$ for $k \geqslant 0$

$$\begin{aligned}\text{then}\quad a_{k+1} &= 3a_k - 3a_{k-1} + a_{k-2}\\ &= 3k - 3(k-1) + (k-2)\\ &= \cancel{3k} - \cancel{3k} + 3 + k - 2\\ &= (k+1)\end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = n,\ \ n \in \mathbb{N}$.

2 **a** $a_0 = 0,\ \ a_1 = 1,\ \ a_2 = 4$

$a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3},\ \ n \geqslant 3$

$$\begin{aligned}\therefore\ \ a_3 &= 3a_2 - 3a_1 + a_0\\ &= 3(4) - 3(1) + 0\\ &= 9\\ a_4 &= 3a_3 - 3a_2 + a_1\\ &= 3(9) - 3(4) + 1\\ &= 16\\ a_5 &= 3a_4 - 3a_3 + a_2\\ &= 3(16) - 3(9) + 4\\ &= 25\\ a_6 &= 3a_5 - 3a_4 + a_3\\ &= 3(25) - 3(16) + 9\\ &= 36\\ a_7 &= 3a_6 - 3a_5 + a_4\\ &= 3(36) - 3(25) + 16\\ &= 49\end{aligned}$$

b $a_n = n^2,\ \ n \in \mathbb{N}$.

c $a_0 = 0^2,\ \ a_1 = 1^2,\ \ a_2 = 2^2$ ✓

If $a_k = k^2$ for $k \geqslant 0$

$$\begin{aligned}\text{then}\quad a_{k+1} &= 3a_k - 3a_{k-1} + a_{k-2}\\ &= 3k^2 - 3(k-1)^2 + (k-2)^2\\ &= 3k^2 - 3k^2 + 6k - 3 + k^2 - 4k + 4\\ &= k^2 + 2k + 1\\ &= (k+1)^2\end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = n^2,\ \ n \in \mathbb{N}$.

3 **a** $a_0 = 1,\ \ a_1 = 2,\ \ a_2 = 4$

$a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3},\ \ n \geqslant 3$

$$\begin{aligned}\therefore\ \ a_3 &= 7a_2 - 16a_1 + 12a_0\\ &= 7(4) - 16(2) + 12(1)\\ &= 8\\ a_4 &= 7a_3 - 16a_2 + 12a_1\\ &= 7(8) - 16(4) + 12(2)\\ &= 16\end{aligned}$$

Conjecture: $a_n = 2^n,\ \ n \in \mathbb{N}$

$a_0 = 2^0,\ \ a_1 = 2^1,\ \ a_2 = 2^2$ ✓

If $a_k = 2^k$

$$\begin{aligned}\text{then}\quad a_{k+1} &= 7a_k - 16a_{k-1} + 12a_{k-2}\\ &= 7(2^k) - 16(2^{k-1}) + 12(2^{k-2})\\ &= 2^k\left(7 - \tfrac{16}{2} + \tfrac{12}{4}\right)\\ &= 2^k(2)\\ &= 2^{k+1}\end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = 2^n,\ \ n \in \mathbb{N}$.

b $a_0 = 0,\ \ a_1 = 2,\ \ a_2 = 8$

$a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3},\ \ n \geqslant 3$

$$\begin{aligned}\therefore\ \ a_3 &= 7a_2 - 16a_1 + 12a_0\\ &= 7(8) - 16(2) + 0\\ &= 24\\ a_4 &= 7a_3 - 16a_2 + 12a_1\\ &= 7(24) - 16(8) + 12(2)\\ &= 64\\ a_5 &= 7a_4 - 16a_3 + 12a_2\\ &= 7(64) - 16(24) + 12(8)\\ &= 160\end{aligned}$$

$$\begin{aligned}a_0 &= 0 \times 2^0\\ a_1 &= 1 \times 2^1\\ a_2 &= 2 \times 2^2\\ a_3 &= 3 \times 2^3\\ a_4 &= 4 \times 2^4\\ a_5 &= 5 \times 2^5\end{aligned}$$

Conjecture: $a_n = n2^n,\ \ n \in \mathbb{N}$

$a_0 = 0 \times 2^0,\ \ a_1 = 1 \times 2^1,\ \ a_2 = 2 \times 2^2$ ✓

If $a_k = k2^k$

$$\begin{aligned}\text{then}\quad a_{k+1} &= 7a_k - 16a_{k-1} + 12a_{k-2}\\ &= 7(k)2^k - 16(k-1)2^{k-1} + 12(k-2)2^{k-2}\\ &= 2^k[7k - 8(k-1) + 3(k-2)]\\ &= 2^k(7k - 8k + 8 + 3k - 6)\\ &= 2^k(2k+2)\end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = n2^n,\ \ n \in \mathbb{N}$.

c $a_0 = 1,\ \ a_1 = 3,\ \ a_2 = 9$

$a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3},\ \ n \geqslant 3$

$$\begin{aligned}\therefore\ \ a_3 &= 7a_2 - 16a_1 + 12a_0\\ &= 7(9) - 16(3) + 12(1)\\ &= 27\end{aligned}$$

$$\begin{aligned} a_4 &= 7a_3 - 16a_2 + 12a_1 \\ &= 7(27) - 16(9) + 12(3) \\ &= 81 \end{aligned}$$

$a_0 = 3^0,\ \ a_1 = 3^1,\ \ a_2 = 3^2,\ \ a_3 = 3^3,\ \ a_4 = 3^4$

Conjecture: $a_n = 3^n,\ \ n \in \mathbb{N}$

$a_0 = 3^0,\ \ a_1 = 3^1,\ \ a_2 = 3^2$ ✓

If $a_k = 3^k$

then
$$\begin{aligned} a_{k+1} &= 7a_k - 16a_{k-1} + 12a_{k-2} \\ &= 7(3^k) - 16(3^{k-1}) + 12(3^{k-2}) \\ &= 3^k\left(7 - \tfrac{16}{3} + \tfrac{12}{9}\right) \\ &= 3^k(3) \\ &= 3^{k+1} \end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = 3^n,\ \ n \in \mathbb{N}$.

4 $a_0 = 0,\ \ a_n = a_{n-1} + 2n(2n+1)(n-2) + 8n - 1$

a
$$\begin{aligned} a_1 &= a_0 + (2)(3)(-1) + 8 - 1 \\ &= 0 - 6 + 7 \\ &= 1 \\ a_2 &= a_1 + (4)(5)(0) + 16 - 1 \\ &= 1 + 15 \\ &= 16 \\ a_3 &= a_2 + (6)(7)(1) + 24 - 1 \\ &= 16 + 42 + 23 \\ &= 81 \\ a_4 &= a_3 + (8)(9)(2) + 32 - 1 \\ &= 81 + 144 + 31 \\ &= 256 \end{aligned}$$

$\therefore\ \ a_0 = 0^4,\ \ a_1 = 1^4,\ \ a_2 = 2^4,\ \ a_3 = 3^4,\ \ a_4 = 4^4$

b $a_n = n^4,\ \ n \in \mathbb{N}$

c $a_0 = 0^4$ ✓

If $a_k = k^4$

then
$$\begin{aligned} a_{k+1} &= a_k + 2(k+1)(2k+3)(k-1) \\ &\quad + 8(k+1) - 1 \\ \therefore\ \ a_{k+1} &= k^4 + 2(k+1)(2k^2 + k - 3) + 8k + 8 - 1 \\ &= k^4 + 4k^3 + 6k^2 - 4k - 6 + 8k + 7 \\ &= k^4 + 4k^3 + 6k^2 + 4k + 1 \\ &= (k+1)^4 \qquad \{\text{binomial theorem}\} \end{aligned}$$

$\therefore$ by the Principle of Mathematical Induction, $a_n = n^4,\ \ n \in \mathbb{N}$.

5 **a** $a_0 = 1,\ \ a_1 = 2,\ \ a_n = 3a_{n-1} - 2a_{n-2}$

$$\begin{aligned} a_2 &= 3a_1 - 2a_0 \\ &= 3(2) - 2(1) \\ &= 4 \\ a_3 &= 3a_2 - 2a_1 \\ &= 3(4) - 2(2) \\ &= 8 \\ a_4 &= 3a_3 - 2a_2 \\ &= 3(8) - 2(4) \\ &= 16 \end{aligned}$$

Conjecture: $a_n = 2^n$

$a_0 = 2^0,\ \ a_1 = 2^1$ ✓

If $a_k = 2^k$ then
$$\begin{aligned} a_{k+1} &= 3a_k - 2a_{k-1} \\ &= 3(2^k) - 2(2^{k-1}) \\ &= 2^k\left(3 - \tfrac{2}{2}\right) \\ &= 2^k(2) \\ &= 2^{k+1} \end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = 2^n,\ \ n \in \mathbb{N}$.

b $a_0 = 1,\ \ a_1 = 3,\ \ a_n = 4a_{n-1} - 3a_{n-2}$

$$\begin{aligned} \therefore\ \ a_2 &= 4a_1 - 3a_0 \\ &= 4(3) - 3(1) \\ &= 9 \\ a_3 &= 4a_2 - 3a_1 \\ &= 4(9) - 3(3) \\ &= 27 \\ a_4 &= 4a_3 - 3a_2 \\ &= 4(27) - 3(9) \\ &= 81 \end{aligned}$$

Conjecture: $a_n = 3^n,\ \ n \in \mathbb{N}$

$a_0 = 3^0,\ \ a_1 = 3^1$ ✓

If $a_k = 3^k$ then
$$\begin{aligned} a_{k+1} &= 4a_k - 3a_{k-1} \\ &= 4(3^k) - 3(3^{k-1}) \\ &= 3^k\left(4 - \tfrac{3}{3}\right) \\ &= 3^k(3) \\ &= 3^{k+1} \end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction, $a_n = 3^n,\ \ n \in \mathbb{N}$.

6 **a** $a_0 = 1,\ \ a_n = na_{n-1} + n!,\ \ n \in \mathbb{Z}^+$

$$\begin{aligned} \therefore\ \ a_1 &= 1a_0 + 1! \\ &= 1 + 1 \\ &= 2 \qquad = 2! \\ a_2 &= 2a_1 + 2! \\ &= 2(2) + 2 \\ &= 6 \qquad = 3! \\ a_3 &= 3a_2 + 3! \\ &= 3(6) + 6 \\ &= 24 \qquad = 4! \\ a_4 &= 3a_3 + 4! \\ &= 4(24) + 24! \\ &= 120 \qquad = 5! \end{aligned}$$

Conjecture: $a_n = (n+1)!,\ \ n \in \mathbb{N}$

$a_0 = 1 = (0+1)!$ ✓

If $a_k = (k+1)!$

then
$$\begin{aligned} a_{k+1} &= (k+1)a_k + (k+1)! \\ &= (k+1)(k+1)! + (k+1)! \\ &= (k+1)![k+1+1] \\ &= (k+2)(k+1)! \\ &= (k+2)! \end{aligned}$$

$\therefore$ by the Principle of Mathematical Induction, $a_n = (n+1)!,\ \ n \in \mathbb{N}$.

b $a_0 = 1,\ \ a_n = 2na_{n-1} + n!2^n,\ \ n \in \mathbb{Z}^+$

$$\begin{aligned} a_1 &= 2a_0 + 1!2^1 \\ &= 2(1) + 2 \\ &= 4 \end{aligned}$$

$$\begin{aligned} a_2 &= 4a_1 + 2!2^2 \\ &= 16+8 \\ &= 24 \\ a_3 &= 6a_2 + 3!2^3 \\ &= 6(24) + 6\times 8 \\ &= 192 \\ a_4 &= 8a_3 + 4!2^4 \\ &= 8(192) + 24\times 16 \\ &= 1920 \end{aligned}$$

$$\begin{aligned} a_0 &= 2^0 \times 1! \\ a_1 &= 2\times 2 &&= 2\times 2! \\ a_2 &= 2^2 \times 6 &&= 2^2\times 3! \\ a_3 &= 2^3\times 24 &&= 2^3 \times 4! \\ a_4 &= 2^4 \times 120 &&= 2^4\times 5! \end{aligned}$$

Conjecture: $a_n = 2^n(n+1)!,\ n \in \mathbb{N}$

$a_0 = 2^0(1!) = 1$ ✓

If $a_k = 2^k(k+1)!$

then
$$\begin{aligned} a_{k+1} &= 2(k+1)a_k + (k+1)!\,2^{k+1} \\ &= 2(k+1)\times 2^k(k+1)! + (k+1)!\,2^{k+1} \\ &= 2^{k+1}(k+1)![k+1+1] \\ &= 2^{k+1}(k+1)!(k+2) \\ &= 2^{k+1}(k+2)! \end{aligned}$$

$\therefore$ by the Principle of Mathematical Induction,
$a_n = 2^n(n+1)!,\ n\in\mathbb{N}$.

EXERCISE 1B.4

1 **a** $a_n = a_{n-1} + 12a_{n-2},\ n \geqslant 2$ with $a_0 = 12,\ a_1 = 24$

As $a_n - a_{n-1} - 12a_{n-2} = 0$, the characteristic equation is $\lambda^2 - \lambda - 12 = 0$

$\therefore\ (\lambda-4)(\lambda+3) = 0$

$\therefore\ \lambda = 4, -3$, distinct real roots.

$\therefore$ the general solution is $a_n = c_1(4)^n + c_2(-3)^n,\ n\in\mathbb{N}$.

Using the initial conditions:

$a_0 = 12 \quad \therefore\ c_1 + c_2 = 12 \quad .... (1)$

and $a_1 = 24 \quad \therefore\ 4c_1 - 3c_2 = 24 \quad .... (2)$

Solving (1) and (2) simultaneously, $c_1 = \frac{60}{7}$ and $c_2 = \frac{24}{7}$.

$\therefore\ a_n = \frac{60}{7}(4^n) + \frac{24}{7}(-3)^n,\ n\in\mathbb{N}$.

b $a_n - 3a_{n-1} + 2a_{n-2} = 0,\ n\geqslant 2$ with $a_0 = 2,\ a_1 = 3$

The characteristic equation is

$\lambda^2 - 3\lambda + 2 = 0$

$\therefore\ (\lambda - 1)(\lambda-2) = 0$

$\therefore\ \lambda = 1, 2$, distinct real roots.

$\therefore$ the general solution is $a_n = c_1(1)^n + c_2(2)^n,\ n\in\mathbb{N}$.

Using the initial conditions:

$a_0 = 2 \quad \therefore\ c_1 + c_2 = 2 \quad .... (1)$

and $a_1 = 3 \quad \therefore\ c_1 + 2c_2 = 3 \quad .... (2)$

Solving (1) and (2) simultaneously, $c_1 = 1$ and $c_2 = 1$.

$\therefore\ a_n = 1 + 2^n,\ n\in\mathbb{N}$.

c $x_{n+2} - x_{n+1} - 2x_n = 0,\ n\in\mathbb{N}$ with $x_0 = 1,\ x_1 = 1$

$\therefore\ x_n - x_{n-1} - 2x_{n-2} = 0$ and has characteristic equation

$\lambda^2 - \lambda - 2 = 0$

$\therefore\ (\lambda-2)(\lambda+1) = 0$

$\therefore\ \lambda = 2, -1$, distinct real roots.

$\therefore$ the general solution is $x_n = c_1(2)^n + c_2(-1)^n,\ n\in\mathbb{N}$.

Using the initial conditions:

$x_0 = 1 \quad \therefore\ c_1 + c_2 = 1 \quad .... (1)$

and $x_1 = 1 \quad \therefore\ 2c_1 - c_2 = 1 \quad .... (2)$

Solving (1) and (2) simultaneously, $c_1 = \frac{2}{3},\ c_2 = \frac{1}{3}$.

$\therefore\ x_n = \frac{2}{3}(2)^n + \frac{1}{3}(-1)^n,\ n\in\mathbb{N}$.

d $a_n - a_{n-1} - 2a_{n-2} = 0,\ n\geqslant 2$ with $a_0 = 7,\ a_1 = 11$.

The characteristic equation is

$\lambda^2 - \lambda - 2 = 0$

$\therefore\ (\lambda-2)(\lambda+1) = 0$

$\therefore\ \lambda = 2, -1$, distinct real roots.

$\therefore$ the general solution is $a_n = c_1(2)^n + c_2(-1)^n,\ n\in\mathbb{N}$.

Using the initial conditions:

$a_0 = 7 \quad \therefore\ c_1 + c_2 = 7 \quad .... (1)$

and $a_1 = 11 \quad \therefore\ 2c_1 - c_2 = 11 \quad .... (2)$

Solving (1) and (2) simultaneously, $c_1 = 6$ and $c_2 = 1$.

$\therefore\ a_n = 6(2)^n + (-1)^n,\ n\in\mathbb{N}$.

e $a_n = 5a_{n-1} - 6a_{n-2},\ n\geqslant 2$ with $a_0 = 3,\ a_1 = 5$.

The characteristic equation is

$\lambda^2 - 5\lambda + 6 = 0$

$\therefore\ (\lambda-2)(\lambda-3) = 0$

$\therefore\ \lambda = 2, 3$, distinct real roots.

$\therefore$ the general solution is $a_n = c_1(2)^n + c_2(3)^n,\ n\in\mathbb{N}$.

Using the initial conditions:

$a_0 = 3 \quad \therefore\ c_1 + c_2 = 3 \quad .... (1)$

and $a_1 = 5 \quad \therefore\ 2c_1 + 3c_2 = 5 \quad .... (2)$

Solving (1) and (2) simultaneously, $c_1 = 4$ and $c_2 = -1$.

$\therefore\ a_n = 4(2^n) - 3^n$ or $a_n = 2^{n+2} - 3^n,\ n\in\mathbb{N}$.

2 $a_n = a_{n-1} + a_{n-2}$ for $n\geqslant 1$ and $a_0 = 0,\ a_1 = 1$.

The characteristic equation is

$\lambda^2 - \lambda - 1 = 0$

$$\therefore\ \lambda = \frac{1\pm\sqrt{1-4(1)(-1)}}{2} = \frac{1\pm\sqrt{5}}{2}$$

$\therefore$ the general solution is

$$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n,\quad n\in\mathbb{N}.$$

Using initial conditions:

$a_0 = 0 \quad \therefore\ c_1 + c_2 = 0 \quad .... (1)$

and $a_1 = 1 \quad \therefore\ c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) = 1 \quad .... (2)$

Solving (1) and (2), $c_2 = -c_1$.

$$\therefore\ c_1\left(\frac{1+\sqrt{5}}{2}\right) - c_1\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

$$\therefore\ \frac{\cancel{c_1} + c_1\sqrt{5} - \cancel{c_1} + c_1\sqrt{5}}{2} = 1$$

$\therefore\ 2c_1\sqrt{5} = 2$

$\therefore\ c_1 = \frac{1}{\sqrt{5}}$

Hence $c_2 = -\frac{1}{\sqrt{5}}$

$$\text{Thus}\quad a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n,\quad n\in\mathbb{N}.$$

3 **a** $a_n = 2a_{n-1} - a_{n-2},\ n\geqslant 2$ with $a_0 = a_1 = 2$

The characteristic equation is

$\lambda^2 - 2\lambda + 1 = 0$

$\therefore\ (\lambda-1)^2 = 0$

$\therefore\ \lambda = 1$, a repeated root

$\therefore$ the general solution is $a_n = (c_1 + nc_2)(1)^n$, $n \in \mathbb{N}$.

$\therefore \quad a_n = c_1 + nc_2$

Using the initial conditions:

$a_0 = 2 \qquad \therefore \quad c_1 = 2$

and $a_1 = 2 \quad \therefore \quad c_1 + 2c_2 = 2$

$\therefore \quad c_2 = 0$

$\therefore$ $a_n = 2$ for all $n \in \mathbb{N}$.

b $a_n - 10a_{n-1} + 25a_{n-2} = 0, \ n \geqslant 2$

with $a_0 = 7, \ a_1 = 4$.

The characteristic equation is

$\lambda^2 - 10\lambda + 25 = 0$

$\therefore \quad (\lambda - 5)^2 = 0$

$\therefore \quad \lambda = 5$, a repeated root

$\therefore$ the general solution is $a_n = (c_1 + nc_2)(5)^n$, $n \in \mathbb{N}$

Using the initial conditions:

$a_0 = 7 \qquad \therefore \quad c_1 5^0 = 7$

and $a_1 = 4 \quad \therefore \quad (c_1 + c_2)5^1 = 4$

Thus $c_1 = 7$ and $7 + c_2 = \frac{4}{5}$

$\therefore \quad c_2 = -\frac{31}{5}$

$\therefore \quad a_n = (7 - \frac{31}{5}n)5^n, \ n \in \mathbb{N}$.

c $a_{n+2} + 4a_{n+1} + 4a_n = 0, \ n \in \mathbb{N}$

with $a_0 = 2, \ a_1 = -2$

$\therefore \quad a_n + 4a_{n-1} + 4a_{n-2} = 0$

which has characteristic equation

$\lambda^2 + 4\lambda + 4 = 0$

$\therefore \quad (\lambda + 2)^2 = 0$

$\therefore \quad \lambda = -2$, a repeated root

$\therefore$ the general solution is $a_n = (c_1 + nc_2)(-2)^n$, $n \in \mathbb{N}$.

Using the initial conditions:

$a_0 = 2 \qquad \therefore \quad c_1 = 2$

and $a_1 = -2 \quad \therefore \quad (c_1 + c_2)(-2) = -2$

$\therefore \quad c_1 + c_2 = 1$

$\therefore \quad c_2 = -1$

$\therefore$ $a_n = (2 - n)(-2)^n$ for all $n \in \mathbb{N}$.

d $x_{n+2} + 8x_{n+1} + 16x_n = 0, \ n \in \mathbb{N}$ with $x_0 = 2, \ x_1 = 0$.

The characteristic equation is

$\lambda^2 + 8\lambda + 16 = 0$

$\therefore \quad (\lambda + 4)^2 = 0$

$\therefore \quad \lambda = -4$, a repeated root

$\therefore$ the general solution is $x_n = (c_1 + nc_2)(-4)^n$, $n \in \mathbb{N}$.

Using the initial conditions:

$x_0 = c_1 = 2$ and

$x_1 = (c_1 + c_2)(-4) = 0$

$\therefore \quad c_1 + c_2 = 0$

$\therefore \quad c_2 = -2$

$\therefore \quad x_n = (2 - 2n)(-4)^n$

$\therefore \quad x_n = 2(1 - n)(-1)^n \, 2^{2n}$

$\therefore \quad x_n = (-1)^n \, 2^{2n+1}(1 - n), \ n \in \mathbb{N}$.

e $x_{n+2} - 2x_{n+1} + 2x_n = 0, \ n \in \mathbb{N}$ with $x_0 = x_1 = 2$.

The characteristic equation is

$\lambda^2 - 2\lambda + 2 = 0$

$$\therefore \quad \lambda = \frac{2 \pm \sqrt{4 - 4(1)(2)}}{2}$$

$$\therefore \quad \lambda = \frac{2 \pm 2i}{2}$$

$\therefore \quad \lambda = 1 \pm i$, complex conjugate roots.

$\therefore$ the general solution is

$x_n = c_1(1 + i)^n + c_2(1 - i)^n, \ n \in \mathbb{N}$.

Using the initial conditions:

$x_0 = 2 \qquad \therefore \quad c_1 + c_2 = 2 \quad .... (1)$

and $x_1 = 2 \quad \therefore \quad c_1(1 + i) + c_2(1 - i) = 2$

$\therefore \quad (c_1 + c_2) + i(c_1 - c_2) = 2 \quad .... (2)$

Solving (1) and (2) simultaneously, $c_1 = c_2$

Hence $c_1 = c_2 = 1$

$\therefore \quad x_n = (1 + i)^n + (1 - i)^n, \ n \in \mathbb{N}$

$= (\sqrt{2}\operatorname{cis}\frac{\pi}{4})^n + (\sqrt{2}\operatorname{cis}(-\frac{\pi}{4}))^n$

$= 2^{\frac{n}{2}} \left[\operatorname{cis}(\frac{n\pi}{4}) + \operatorname{cis}(\frac{-n\pi}{4})\right]$

$\therefore \quad x_n = 2^{\frac{n}{2}} \times 2\cos(\frac{n\pi}{4}) \qquad \{\operatorname{cis}\theta + \operatorname{cis}(-\theta) = 2\cos\theta\}$

$\therefore \quad x_n = 2^{\frac{n}{2}+1} \cos(\frac{n\pi}{4}), \ n \in \mathbb{N}$.

f $a_{n+2} - 2a_{n+1} + 5a_n = 0, \ n \in \mathbb{N}$ with $a_0 = 4 = a_1$.

The characteristic equation is

$\lambda^2 - 2\lambda + 5 = 0$

$$\therefore \quad \lambda = \frac{2 \pm \sqrt{4 - 4(1)(5)}}{2}$$

$$\therefore \quad \lambda = \frac{2 \pm 4i}{2}$$

$\therefore \quad \lambda = 1 \pm 2i$

$\therefore$ the general solution is

$a_n = c_1(1 + 2i)^n + c_2(1 - 2i)^n, \ n \in \mathbb{N}$.

Using the initial conditions:

$a_0 = 4 \qquad \therefore \quad c_1 + c_2 = 4$

and $a_1 = 4 \quad \therefore \quad c_1(1 + 2i) + c_2(1 - 2i) = 4$

$\therefore \quad (c_1 + c_2) + (2c_1 - 2c_2)i = 4$

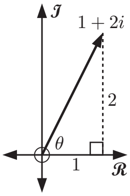
$\therefore \quad 2(c_1 - c_2)i = 0$

$\therefore \quad c_1 = c_2 = 2$

$\therefore \quad a_n = 2(1 + 2i)^n + 2(1 - 2i)^n, \ n \in \mathbb{N}$.

Now $1 + 2i = \sqrt{5}\operatorname{cis}(\arctan 2)$

and $1 - 2i = \sqrt{5}\operatorname{cis}(-\arctan 2)$



$\therefore \quad a_n = 2(5^{\frac{n}{2}})\operatorname{cis}(n\arctan 2)$

$+ 2(5^{\frac{n}{2}})\operatorname{cis}(-n\arctan 2)$

$\therefore \quad a_n = 2(5^{\frac{n}{2}})2\cos(n\arctan 2)$

$\{\operatorname{cis}\theta + \operatorname{cis}(-\theta) = 2\cos\theta\}$

$\therefore \quad a_n = 4(5^{\frac{n}{2}})\cos(n\arctan 2), \ n \in \mathbb{N}$.

4 As a_0, a_1, a, and $b \in \mathbb{Z}$, $a_n = aa_{n-1} + ba_{n-2}$ is a sequence of integers.

$\therefore \quad a_0 = c_1\lambda_1^{\ 0} + c_2\lambda_2^{\ 0} = c_1 + c_2 \quad .... (1)$

and $a_1 = c_1\lambda_1 + c_2\lambda_2$

$\therefore \quad a_1 = c_1(x + iy) + c_2(x - iy)$

$\therefore \quad a_1 = (c_1 + c_2)x + (c_1 - c_2)iy$

$\therefore \quad (c_1 - c_2)y = 0 \qquad$ {equating imaginary parts}

$\therefore \quad c_1 = c_2 \qquad$ {y varies}

But from (1), $a_0 = c_1 + c_2 = 2c_1$ or $2c_2$

$$\therefore \quad c_1 = c_2 = \frac{a_0}{2}$$

5 **a** $a_n = -2a_{n-1} - 2a_{n-2}, \ n \geqslant 2$ with $a_0 = 2, \ a_1 = -2$.

As $a_n + 2a_{n-1} + 2a_{n-2} = 0$, the characteristic equation is $\lambda^2 + 2\lambda + 2 = 0$

$$\therefore \quad \lambda = \frac{-2 \pm \sqrt{4 - 4(1)(2)}}{2}$$
$$\therefore \quad \lambda = \frac{-2 \pm 2i}{2}$$
$$\therefore \quad \lambda = -1 \pm i$$

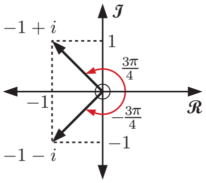
$\therefore$ the general solution is

$a_n = c_1(-1+i)^n + c_2(-1-i)^n, \ n \in \mathbb{N}$.

$c_1 = c_2 = \dfrac{a_0}{2}$ {using **4**}

$= \frac{2}{2} = 1$

Thus $a_n = (-1+i)^n + (-1-i)^n$



$$\therefore \quad a_n = \left[\sqrt{2}\operatorname{cis}\left(\tfrac{3\pi}{4}\right)\right]^n + \left[\sqrt{2}\operatorname{cis}\left(-\tfrac{3\pi}{4}\right)\right]^n$$
$$\therefore \quad a_n = 2^{\frac{n}{2}}\operatorname{cis}\left(\tfrac{3\pi n}{4}\right) + 2^{\frac{n}{2}}\operatorname{cis}\left(-\tfrac{3\pi n}{4}\right)$$
$$\therefore \quad a_n = 2^{\frac{n}{2}}\left[\operatorname{cis}\left(\tfrac{3\pi n}{4}\right) + \operatorname{cis}\left(-\tfrac{3\pi n}{4}\right)\right]$$
$$\therefore \quad a_n = 2^{\frac{n}{2}} \times 2\cos\left(\tfrac{3\pi n}{4}\right)$$

{$\operatorname{cis}\theta + \operatorname{cis}(-\theta) = 2\cos\theta$}

$$\therefore \quad a_n = 2^{\frac{n}{2}+1}\cos\left(\tfrac{3\pi n}{4}\right), \ n \in \mathbb{N}.$$

b $a_n + a_{n-1} + a_{n-2} = 0, \ n \geqslant 2$ with $a_0 = 4, \ a_1 = -2$.

The characteristic equation is

$\lambda^2 + \lambda + 1 = 0$

$$\therefore \quad \lambda = \frac{-1 \pm \sqrt{1 - 4(1)(1)}}{2}$$
$$\therefore \quad \lambda = \frac{-1 \pm i\sqrt{3}}{2}$$

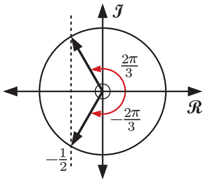
$\therefore$ the general solutions is

$$a_n = c_1\left(\frac{-1+i\sqrt{3}}{2}\right)^n + c_2\left(\frac{-1-i\sqrt{3}}{2}\right)^n, \ n \in \mathbb{N}.$$

$c_1 = c_2 = \dfrac{a_0}{2}$ {using **4**}

$= \frac{4}{2} = 2$

$$\therefore \quad a_n = 2\left(\frac{-1+i\sqrt{3}}{2}\right)^n + 2\left(\frac{-1-i\sqrt{3}}{2}\right)^n$$



$$\therefore \quad a_n = 2\left[\operatorname{cis}\left(\tfrac{2\pi}{3}\right)\right]^n + 2\left[\operatorname{cis}\left(-\tfrac{2\pi}{3}\right)\right]^n$$
$$\therefore \quad a_n = 2\left[\operatorname{cis}\left(\tfrac{2\pi n}{3}\right) + \operatorname{cis}\left(-\tfrac{2\pi n}{3}\right)\right]$$
$$\therefore \quad a_n = 2 \times 2\cos\left(\tfrac{2\pi n}{3}\right)$$
$$\therefore \quad a_n = 4\cos\left(\tfrac{2\pi n}{3}\right), \ n \in \mathbb{N}.$$

c $u_{n+2} + 4u_{n+1} + 5u_n = 0, \ n \in \mathbb{N}$ with $u_0 = 4, \ u_1 = -8$.

The characteristic equation is

$\lambda^2 + 4\lambda + 5 = 0$

$$\therefore \quad \lambda = \frac{-4 \pm \sqrt{16 - 4(1)(5)}}{2}$$
$$\therefore \quad \lambda = -2 \pm i$$

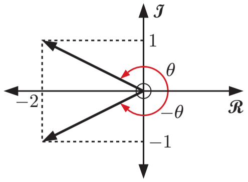
$\therefore$ the general solutions is

$u_n = c_1(-2+i)^n + c_2(-2-i)^n, \ n \in \mathbb{N}$.

$c_1 = c_2 = \dfrac{u_0}{2}$ {using **4**}

$= \frac{4}{2} = 2$

Thus $u_n = 2(-2+i)^n + 2(-2-i)^n, \ n \in \mathbb{N}$.



As $\theta = \pi - \arctan(\frac{1}{2}), \ r = \sqrt{5}$

$$\therefore \quad u_n = 2(\sqrt{5}\operatorname{cis}\theta)^n + 2(\sqrt{5}\operatorname{cis}(-\theta)^n)$$
$$\therefore \quad u_n = 2\left[5^{\frac{n}{2}}\operatorname{cis}(n\theta) + 5^{\frac{n}{2}}\operatorname{cis}(-n\theta)\right]$$
$$\therefore \quad u_n = 2 \times 5^{\frac{n}{2}}\left[\operatorname{cis}(n\theta) + \operatorname{cis}(-n\theta)\right]$$
$$\therefore \quad u_n = 2 \times 5^{\frac{n}{2}} \times 2\cos(n\theta)$$
$$\therefore \quad u_n = 4 \times 5^{\frac{n}{2}}\cos(n\theta),$$
$$\theta = \pi - \arctan(\tfrac{1}{2}), \ n \in \mathbb{N}.$$

d $a_n = 4a_{n-1} - 5a_{n-2}, \ n \geqslant 2$ with $a_0 = 6, \ a_1 = 12$.

The characteristic equation is

$\lambda^2 - 4\lambda + 5 = 0$

$$\therefore \quad \lambda = \frac{4 \pm \sqrt{16 - 4(1)(5)}}{2}$$
$$\therefore \quad \lambda = 2 \pm i$$

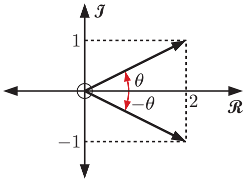
$\therefore$ the general solution is

$a_n = c_1(2+i)^n + c_2(2-i)^n, \ n \in \mathbb{N}$.

$c_1 = c_2 = \dfrac{a_0}{2}$ {using **4**}

$= \frac{6}{2} = 3$

$\therefore$ $a_n = 3(2+i)^n + 3(2-i)^n, \ n \in \mathbb{N}$.



$\theta = \arctan(\frac{1}{2}), \ r = \sqrt{5}$

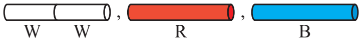
Thus $a_n = 3\left[\sqrt{5}\operatorname{cis}\theta\right]^n + 3\left[\sqrt{5}\operatorname{cis}(-\theta)\right]^n$

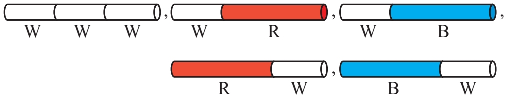
$$= 3 \times 5^{\frac{n}{2}}\operatorname{cis}(n\theta) + 3 \times 5^{\frac{n}{2}}\operatorname{cis}(-n\theta)$$
$$= 3 \times 5^{\frac{n}{2}}\left[\operatorname{cis}(n\theta) + \operatorname{cis}(-n\theta)\right]$$
$$= 3 \times 5^{\frac{n}{2}} \times 2\cos(n\theta)$$
$$\therefore \quad a_n = 6 \times 5^{\frac{n}{2}}\cos(n\theta), \ \ \theta = \arctan(\tfrac{1}{2}), \ n \in \mathbb{N}.$$

6 Let a_n = the number of pipe constructions of length n metres, $n \in \mathbb{N}$.

$a_0 = 1$ {the empty set is unique}

$a_1 = 1$ {one white pipe}

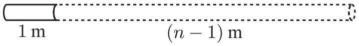
$a_2 = 3$ 

$a_3 = 5$ 

$\vdots$

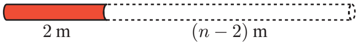
Now consider a pipe construction of length n metres, $n \geqslant 2$.

<u>If the first section is white</u>

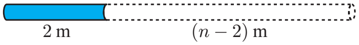


the remaining $(n-1)$ metres can be constructed in a_{n-1} ways.

<u>If the first section is not white</u>, then it must start with red or blue



or



Thus $a_n = a_{n-1} + 2a_{n-2}$ for $n \geqslant 2$ which has characteristic equation $\lambda^2 - \lambda - 2 = 0$

$\therefore \; (\lambda - 2)(\lambda + 1) = 0$

$\therefore \; \lambda = 2$ or -1, distinct real roots.

$\therefore$ the general solution is $a_n = c_1(2^n) + c_2(-1)^n$, $n \in \mathbb{N}$.

Using the initial conditions:

$a_0 = 1 \quad \therefore \; c_1 + c_2 = 1$ .... (1)

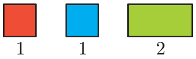
and $a_1 = 1 \quad \therefore \; 2c_1 - c_2 = 1$ .... (2)

Solving (1) and (2) simultaneously, $c_1 = \frac{2}{3}$ and $c_2 = \frac{1}{3}$.

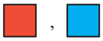
Hence, $a_n = \frac{2}{3}(2^n) + \frac{1}{3}(-1)^n$

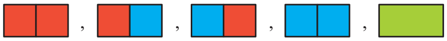
$\therefore \; a_n = \frac{1}{3}\left[2^{n+1} + (-1)^n\right], \; n \in \mathbb{N}$

7



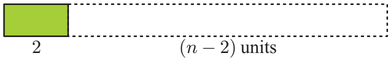
$a_0 = 1$ {the empty set is unique}

$a_1 = 2$ 

$a_2 = 5$ 

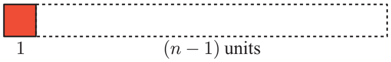
Consider a line of length n units where $n \geqslant 2$.

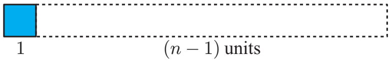
<u>If the first block is green</u>



the remainder of the line can be constructed in a_{n-2} ways.

<u>If the first block is not green</u>, then it must be either red or blue





the remainder of the line, in each case, can be constructed in a_{n-1} ways.

Thus $a_n = 2a_{n-1} + a_{n-2}$ where $n \geqslant 2$.

This recurrence relationship has characteristic equation

$\lambda^2 - 2\lambda - 1 = 0$

$$\therefore \; \lambda = \frac{2 \pm \sqrt{4 - 4(1)(-1)}}{2}$$

$$\therefore \; \lambda = 1 \pm \sqrt{2}$$

Hence $a_n = c_1(1+\sqrt{2})^n + c_2(1-\sqrt{2})^n$, $n \in \mathbb{N}$.

Using the initial conditions:

$a_0 = 1 \quad \therefore \; c_1 + c_2 = 1$ .... (1)

and $a_1 = 2 \quad \therefore \; c_1(1+\sqrt{2}) + c_2(1-\sqrt{2}) = 2$

$\therefore \; (c_1 + c_2) + (c_1 - c_2)\sqrt{2} = 2$ .... (2)

Subtracting (1) from (2) gives

$\sqrt{2}(c_1 - c_2) = 1$

$\therefore \; \sqrt{2}(c_1 - 1 + c_1) = 1$ {$c_2 = 1 - c_1$, using (1)}

$\therefore \; 2\sqrt{2}c_1 - \sqrt{2} = 1$

$\therefore \; 2\sqrt{2}c_1 = 1 + \sqrt{2}$

$$\therefore \; c_1 = \frac{1+\sqrt{2}}{2\sqrt{2}}$$

Hence $c_2 = \dfrac{1-\sqrt{2}}{2\sqrt{2}}$

$$\therefore \; a_n = \frac{1+\sqrt{2}}{2\sqrt{2}}(1+\sqrt{2})^n + \frac{1-\sqrt{2}}{1\sqrt{2}}(1-\sqrt{2})^n$$

$$\therefore \; a_n = \frac{1}{2\sqrt{2}}(1+\sqrt{2})^{n+1} - \frac{1}{2\sqrt{2}}(1-\sqrt{2})^{n+1}$$

$$\therefore \; a_n = \frac{1}{2\sqrt{2}}\left[(1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}\right], \; n \in \mathbb{N}$$

8 Let a_n = the number of ternary strings of length n with no consecutive 0s, $n \in \mathbb{N}$.

$a_0 = 1$ {the unique empty string has no consecutive 0s}

$a_1 = 3$ {0, 1, 2}

$a_2 = 8$ {01, 02, 10, 11, 12, 20, 21, 22}

Consider a string of length n where $n \geqslant 2$.

Either the first digit is 0 or is not 0.

<u>If the first digit is 0,</u>

the second is 1 or 2 (two possibilities) and the remainder of digits on the string can be constructed in a_{n-2} ways

$$\begin{array}{lll} & \text{1st} \quad \text{2nd} & \underbrace{\text{3rd} \quad \text{4th} \quad \ldots.}_{} \\ \text{ways:} & 1 \qquad 2 & (n-2) \text{ bits} \end{array}$$

<u>If the first digit is not 0,</u>

then it must be 1 or 2 (two possibilities) and the remainder of the string can be constructed in a_{n-1} ways

$$\begin{array}{lll} & \text{1st} & \underbrace{\text{2nd} \quad \text{3rd} \quad \text{4th} \quad \ldots.}_{} \\ \text{ways:} & 2 & (n-1) \text{ bits} \end{array}$$

$\therefore \; a_n = 2a_{n-1} + 2a_{n-1}$ for $n \geqslant 2$.

The characteristic equation is

$\lambda^2 - 2\lambda - 2 = 0$

$$\therefore \quad \lambda = \frac{2 \pm \sqrt{4 - 4(1)(-2)}}{2}$$

$$\therefore \quad \lambda = 1 \pm \sqrt{3}$$

$\therefore \quad a_n = c_1(1+\sqrt{3})^n + c_2(1-\sqrt{3})^n, \quad n \in \mathbb{N}.$

Using the initial conditions:

$a_0 = 1 \qquad \therefore \quad c_1 + c_2 = 1 \quad .... (1)$

and $\quad a_1 = 3 \quad \therefore \quad c_1(1+\sqrt{3}) + c_2(1-\sqrt{3}) = 3$

$\therefore \quad (c_1 + c_2) + (c_1 - c_2)\sqrt{3} = 3 \quad .... (2)$

Subtracting (1) from (2) gives

$\sqrt{3}(c_1 - c_2) = 2$

$\therefore \quad \sqrt{3}(c_1 - 1 + c_1) = 2 \qquad \{c_2 = 1 - c_1, \text{ using (1)}\}$

$\therefore \quad 2\sqrt{3}c_1 - \sqrt{3} = 2$

$$\therefore \quad c_1 = \frac{2+\sqrt{3}}{2\sqrt{3}}\,\frac{\sqrt{3}}{\sqrt{3}}$$

$$\therefore \quad c_1 = \frac{3+2\sqrt{3}}{6}$$

Hence, $\quad c_2 = \dfrac{3-2\sqrt{3}}{6}$

$$\therefore \quad a_n = \frac{3+2\sqrt{3}}{6}(1+\sqrt{3})^n + \frac{3-2\sqrt{3}}{6}(1-\sqrt{3})^n, \quad n \in \mathbb{N}.$$

9 Let a_n = the number of sequences of \$1 and \$2 coins which sum to \$$n$, $n \in \mathbb{N}$.

$a_0 = 1 \qquad$ {the empty set is unique}

$a_1 = 1 \qquad$ {a \$1 coin}

$a_2 = 2 \qquad$ {**either** two \$1 **or** one \$2}

$a_3 = 3 \qquad$ {1-1-1, 1-2, 2-1}

Suppose a travel card worth \$$n$ is purchased, $n \geqslant 2$.

The first coin deposited is **either** \$1 **or** it is not \$1.

If it is a \$1 coin,

then the remaining \$$(n-1)$ can be purchased in a_{n-1} ways.

If it is not a \$1,

it is a \$2 coin and the remaining \$$(n-2)$ can be purchased in a_{n-2} ways.

$\therefore \quad a_n = a_{n-1} + a_{n-2}$ for $n \geqslant 2$.

The characteristic equation is

$\lambda^2 - \lambda - 1 = 0$

$$\therefore \quad \lambda = \frac{1 \pm \sqrt{1 - 4(1)(-1)}}{2}$$

$$\therefore \quad \lambda = \frac{1 \pm \sqrt{5}}{2}$$

$$\therefore \quad a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n, \quad n \in \mathbb{N}.$$

Using the initial conditions:

$a_0 = 1 \quad \therefore \quad c_1 + c_2 = 1 \quad .... (1)$

and $\quad a_1 = 1$

$$\therefore \quad c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

$\therefore \quad (c_1 + c_2) + (c_1 - c_2)\sqrt{5} = 2 \quad .... (2)$

Subtracting (1) from (2) gives

$\sqrt{5}(c_1 - c_2) = 1$

$\therefore \quad \sqrt{5}(c_1 - 1 + c_1) = 1 \qquad \{c_2 = 1 - c_1, \text{ using (1)}\}$

$\therefore \quad 2\sqrt{5}c_1 - \sqrt{5} = 1$

$$\therefore \quad c_1 = \frac{1+\sqrt{5}}{2\sqrt{5}}$$

and $\quad c_2 = -\dfrac{1-\sqrt{5}}{2\sqrt{5}}$

Hence, $\quad a_n = \dfrac{1+\sqrt{5}}{2\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \dfrac{1-\sqrt{5}}{2\sqrt{5}}\left(\dfrac{1-\sqrt{5}}{2}\right)^n$

$$\therefore \quad a_n = \frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}, \quad n \in \mathbb{N}$$

EXERCISE 1C.1

1 $d \mid n \;\Rightarrow\;$ there exists $k \in \mathbb{Z}$ such that $n = kd$

$\Rightarrow \; an = kad, \quad k \in \mathbb{Z}$

$\Rightarrow \; an = k(ad), \quad k \in \mathbb{Z}$

$\Rightarrow \; ad \mid an$

2 $d \mid n$ and $d \mid m$

$\Rightarrow$ there exist $k_1, k_2 \in \mathbb{Z}$ such that $n = k_1 d$ and $m = k_2 d$

$\Rightarrow \; an = k_1 ad$ and $bm = k_2 bd$

$\Rightarrow \; an + bm = k_1 ad + k_2 bd$

$\Rightarrow \; an + bm = d(k_1 a + k_2 b)$ where $k_1 a + k_2 b \in \mathbb{Z}$

$\Rightarrow \; d \mid an + bm$

3 $d \mid n \;\Rightarrow\;$ there exists $k \in \mathbb{Z}^+$ such that $n = kd$

$\Rightarrow \; n \geqslant d \qquad \{\text{as } k \geqslant 1\}$

$\Rightarrow \; d \leqslant n$

4 Let d be a common positive divisor of a and $a+1$

$\Rightarrow \; d \mid a$ and $d \mid a+1$

$\Rightarrow \; d \mid (a+1) - a \qquad$ {linearity}

$\Rightarrow \; d \mid 1$

$\Rightarrow \; d = 1 \qquad \{\text{as } d \neq 0\}$

5 **a** As $14m + 20n = 2(7m + 20n)$ where $7m + 20n \in \mathbb{Z}$,

then $\; 2 \mid 14m + 20n$

$\Rightarrow \; 2 \mid 101, \;$ which is false.

Hence, no such integers m, n exist.

b As $14m + 21n = 7(2m + 3n)$ where $2m + 3n \in \mathbb{Z}$,

then $\; 7 \mid 14m + 21n$

$\Rightarrow \; 7 \mid 100, \;$ which is false

Hence, no such integers m, n exist.

6 $a, b, c \in \mathbb{Z}$ and $a \neq 0$.

$a \mid b$ and $a \mid c$

$\Rightarrow$ there exist $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $c = k_2 a$

$\Rightarrow \; b \pm c = k_1 a \pm k_2 a$

$\Rightarrow \; b \pm c = (k_1 \pm k_2)a, \quad k_1 \pm k_2 \in \mathbb{Z}$

$\Rightarrow \; a \mid (b \pm c)$

7 $a, b, c, d \in \mathbb{Z}, \quad a \neq 0, \quad c \neq 0.$

$a \mid b$ and $c \mid d$

$\Rightarrow$ there exist $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $d = k_2 c$

$\Rightarrow \; bd = (k_1 k_2)ac, \;$ where $k_1, k_2 \in \mathbb{Z}$

$\Rightarrow \; ac \mid bd$

8 $p, q \in \mathbb{Z}$

$p \mid q$

$\Rightarrow$ there exists $k \in \mathbb{Z}$ such that $q = kp$

$\Rightarrow \; q^n = k^n p^n \;$ where $k^n \in \mathbb{Z}$

$\Rightarrow \; p^n \mid q^n$

EXERCISE 1C.2

1 **a** As $66 = 22 \times 3$ then $3 \mid 66$

b As $385 = 55 \times 7$ then $7 \mid 385$

c As $0 = 0 \times 654$ then $654 \mid 0$

2 **a** $a = 100,\ b = 17$

$\frac{a}{b} = 5.882....$

$\therefore\ q = 5$

Now $r = a - bq = 100 - 17 \times 5$

$\therefore\ r = 15$

b $a = 289,\ b = 17$

$\frac{a}{b} = 17$

$\therefore\ q = 17$ and $r = 0$

c $a = -44,\ b = 17$

$\frac{a}{b} = -2.588....$

$\therefore\ q = -3$

Now $r = a - bq = -44 - 17(-3)$

$\therefore\ r = 7$

d $a = -100,\ b = 17$

$\frac{a}{b} = -5.882....$

$\therefore\ q = -6$

Now $r = a - bq = -100 - 17(-6)$

$\therefore\ r = 2$

3 a and b are not multiples of each other.

4 **a** No, as the only positive divisors of q are 1 and q and of r are 1 and r

$\therefore$ if $p \mid qr$ then $p = 1, q$, or r

$\therefore$ either $p \mid q$ or $p \mid r$ or both.

b Notice, for example, that $6 \mid 4 \times 3$ but $6 \nmid 4$ and $6 \nmid 3$.
p must be composite and $p = mn$ where $n \mid q,\ m \mid r$.

5 If at least one of the k integers is even then the product is even.

Using the contrapositive:

If the product is **not** even

$\Rightarrow$ all integers are odd

$\therefore$ the product is odd $\Rightarrow$ all integers are odd.

6 **a** On dividing any integer by 3 the remainder is 0, 1, or 2.

$\therefore$ the integer has form $3a,\ 3a+1$, or $3a+2$

$\therefore$ an integer squared has form

$(3a)^2,\ (3a+1)^2$, or $(3a+2)^2$

$= 9a^2,\ 9a^2+6a+1$, or $9a^2+12a+4$

$= 3[3a^2],\ 3[3a^2+2a]+1$, or $3[3a^2+4a+1]+1$

where the only remainders are 0 and 1

$= 3k_1,\ 3k_2+1$, or $3k_3+1$

$\therefore$ of form $3k$ or $3k+1,\ k \in \mathbb{Z}$.

b On division of an integer by 4, the remainder is 0, 1, 2, or 3

$\therefore$ the integer squared is

$(4a)^2,\ (4a+1)^2,\ (4a+2)^2$, or $(4a+3)^2$

$= 16a^2,\ 16a^2+8a+1,\ 16a^2+16a+4$,

or $16a^2+24a+9$

$= 4(4a^2),\ 4(4a^2+2a)+1,\ 4(4a^2+4a+1)$,

or $4(4a^2+6a+2)+1$

$= 4q_1,\ 4q_2+1,\ 4q_3$, or $4q_4+1$

$\therefore$ of form $4q$ or $4q+1,\ q \in \mathbb{Z}$.

c $1\,234\,567 = 4(308\,641) + 3$

which is of the form $4q+3,\ q \in \mathbb{Z}$

$\therefore$ $1\,234\,567$ is not a perfect square {from **b**}

7 **a** **To prove** $5 \mid a \Leftrightarrow 5 \mid a^2$

$(\Rightarrow)$ If $5 \mid a$ then $a = 5q$ for some $q \in \mathbb{Z}$

$\Rightarrow a^2 = 25q^2$

$\Rightarrow a^2 = 5(5q^2)$ where $5q^2 \in \mathbb{Z}$

$\Rightarrow 5 \mid a^2$

$(\Leftarrow)$ Instead of showing $5 \mid a^2 \Rightarrow 5 \mid a$, we will prove the contrapositive $5 \nmid a \Rightarrow 5 \nmid a^2$.

If $5 \nmid a$ then

$a = 5k+1,\ 5k+2,\ 5k+3$, or $5k+4$.

Hence

$a^2 = 25k^2+10k+1,\ 25k^2+20k+4,$

$25k^2+30k+9$, or $25k^2+40k+16$

$\Rightarrow a^2 = 5(5k^2+2k)+1,\ 5(5k^2+4k)+4,$

$5(5k^2+6k+1)+4,$

or $5(5k^2+8k+3)+1$

$\Rightarrow a^2 = 5b+1$ or $5b+4$ for $b \in \mathbb{Z}$

$\Rightarrow 5 \nmid a^2$

Hence $5 \nmid a \Rightarrow 5 \nmid a^2$, and therefore $5 \mid a^2 \Rightarrow 5 \mid a$ {contrapositive}

b $3 \mid a^2 \Leftrightarrow 9 \mid a^2$

$(\Rightarrow)$ $3 \mid a^2 \Rightarrow 3 \mid a$ {**Example 19**}

$\Rightarrow a = 3k$ for some $k \in \mathbb{Z}$

$\Rightarrow a^2 = 9k^2$

$\Rightarrow 9 \mid a^2$ as $k^2 \in \mathbb{Z}$

$(\Leftarrow)$ $9 \mid a^2 \Rightarrow a^2 = 9k,\ k \in \mathbb{Z}$

$\Rightarrow a^2 = 3(3k)$ where $3k \in \mathbb{Z}$

$\Rightarrow 3 \mid a^2$

8 **a** $n = 2 \Rightarrow (n-2) = 0$

$\Rightarrow (n+3)(n-2) = 0$

b $n = -3 \Rightarrow n+3 = 0$

$\Rightarrow (n+3)(n-2) = 0$

$\not\Rightarrow n = 2$

That is the converse is **not** true.

c **i** The statement is "$n^2+n-6=0 \Rightarrow n=2$".

$n^2+n-6=0$

$\Rightarrow (n+3)(n-2)=0$

$\Rightarrow n=-3$ or 2

$\therefore$ the statement is false.

ii The statement is "$n=2 \Rightarrow n^2+n-6=0$".

$n=2 \Rightarrow (n-2)=0$

$\Rightarrow (n-2)(n+3)=0$

$\Rightarrow n^2+n-6=0$

$\therefore$ the statement is true.

iii The statement is "$n^2+n-6=0 \Rightarrow n=2$".

$\therefore$ the statement is false. {See **c i**}

iv The statement is "$a<b \Rightarrow 4ab<(a+b)^2$".

Notice that $(a+b)^2-4ab$

$= a^2+2ab+b^2-4ab$

$= a^2-2ab+b^2$

$= (a-b)^2$

$a < b \;\Rightarrow\; a - b < 0$ and $(a-b)^2 > 0$

$\Rightarrow\; (a+b)^2 - 4ab > 0$

$\Rightarrow\; 4ab < (a+b)^2$

$\therefore$ the statement is true.

v, **vi**, **vii**

These statements all read

"$a < b \;\Leftrightarrow\; 4ab < (a+b)^2$"

and so are either all true or all false.

They are *all false*.

For example, if $a = 2$, $b = 1$ then $b < a$

but $4ab = 8$ and

$(a+b)^2 = 9$

and so $4ab < (a+b)^2$.

9 **a** $8p + 7 = 8p + 4 + 3, \;\; p \in \mathbb{Z}$

$= 4(2p+1) + 3$ where $2p + 1 \in \mathbb{Z}$

$= 4q + 3$ where $q \in \mathbb{Z}$

b $11 = 4(2) + 3$ has form $4q + 3, \;\; q \in \mathbb{Z}$

but $11 = 8(1) + 3$ is not in the form $8p + 7$.

or suppose $11 = 8p + 7$ where $p \in \mathbb{Z}$

$\therefore\; 8p = 4$

$\therefore\; p = \frac{1}{2}$, a contradiction

$\therefore$ 11 cannot be put in the form $8p + 7, \;\; p \in \mathbb{Z}$.

10 **a** Every integer n has form $3a$, $3a + 1$, or $3a - 1$ where $a \in \mathbb{Z}$

$\Rightarrow\; n^3 = 27a^3$ or $27a^3 \pm 27a^2 + 9a \pm 1$

$\Rightarrow\; n^3 = 9(3a^3)$ or $9(3a^3 \pm 3a^2 + a) \pm 1$

$\Rightarrow\; n^3$ has form $9k$ or $9k \pm 1$

b Every integer n has form $5a$, $5a \pm 1$, or $5a \pm 2$ where $a \in \mathbb{Z}$.

$\Rightarrow\; n^4 = (5a)^4 = 625a^4$, or

$(5a \pm 1)^4 = 625a^4 \pm 500a^3 + 150a^2 \pm 20a + 1$, or

$(5a \pm 2)^4 = 625a^4 \pm 1000a^3 + 600a^2 \pm 160a + 16$

$\Rightarrow\; n^4 = 5(125a^4)$, or

$5(125a^4 \pm 100a^3 + 30a^2 \pm 4a) + 1$, or

$5(125a^4 \pm 200a^3 + 120a^2 \pm 32a + 3) + 1$

$\Rightarrow\; n^4$ has form $5k$ or $5k + 1, \;\; k \in \mathbb{Z}$.

11 Suppose $3k^2 - 1 = n^2$ for some $n \in \mathbb{Z}$

$\Rightarrow\; 3k^2 - 1 = (3a)^2$ or $(3a \pm 1)^2$

{as n must have one of the forms $3a$, $3a + 1$, $3a - 1$}

$\Rightarrow\; 3k^2 = 9a^2 + 1$ or $9a^2 \pm 6a + 2$

All 3 of these forms are impossible as

LHS is divisible by 3 and

RHS is not divisible by 3

$\therefore$ the supposition is false

$\therefore$ integers of the form $3k^2 - 1, \;\; k \in \mathbb{Z}$ cannot be perfect squares.

12 $n \in \mathbb{Z}^+ \Rightarrow n$ must have one of the forms $6a$, $6a \pm 1$, $6a \pm 2$, $6a + 3$ where $a \in \mathbb{N}$.

If $n = 6a$, $\quad f(n) = \dfrac{\cancel{6}a(6a+1)(12a+1)}{\cancel{6}_1} \in \mathbb{Z}$

If $n = 6a + 1$, $\quad f(n) = \dfrac{(6a+1)(6a+2)(12a+3)}{6}$

$= \dfrac{\cancel{2 \times 3} \times (6a+1)(3a+1)(4a+1)}{\cancel{6}_1}$

which is in $\mathbb{Z}$

If $n = 6a - 1$, $\quad f(n) = \dfrac{(6a-1)(\cancel{6}a)(12a-1)}{\cancel{6}_1}$

which is in $\mathbb{Z}$

If $n = 6a + 2$, $\quad f(n) = \dfrac{(6a+2)(6a+3)(12a+5)}{6}$

$= \dfrac{\cancel{2 \times 3} \times (3a+1)(2a+1)(12a+5)}{\cancel{6}_1}$

which is in $\mathbb{Z}$

If $n = 6a - 2$, $\quad f(n) = \dfrac{(6a-2)(6a-1)(12a-3)}{6}$

$= \dfrac{\cancel{2 \times 3} \times (3a-1)(6a-1)(4a-1)}{\cancel{6}_1}$

which is in $\mathbb{Z}$

If $n = 6a + 3$, $\quad f(n) = \dfrac{(6a+3)(6a+4)(12a+7)}{6}$

$= \dfrac{\cancel{3 \times 2} \times (2a+1)(3a+2)(12a+7)}{\cancel{6}_1}$

which is in $\mathbb{Z}$

Alternatively:

$$\frac{n(n+1)(2n+1)}{6} = 1^2 + 2^2 + 3^2 + ... + n^2$$

is a well known formula for the sum of the first n perfect squares and the RHS is always an integer.

$\therefore$ the LHS is always an integer.

13 The first repunit is 1, which is a perfect square.

The other repunits are 11, 111, 1111, 11 111, ... and the nth repunit is

$1 + 10^1 + 10^2 + 10^3 + ... + 10^{n-1}$

$= 1 + 10 +$ other terms which are **all** divisible by 4

$\therefore$ the nth repunit has form $4k_1 + 11$

$= 4k_1 + 8 + 3$

$= 4(k_1 + 2) + 3$

$= 4k + 3, \;\; k \in \mathbb{Z}$

However, we proved in **6 b** of this Exercise that all perfect squares have form $4k$ or $4k + 1$.

Hence, the nth repunit cannot be a perfect square.

14 A non-negative integer a has form $7n$, $7n \pm 1$, $7n \pm 2$, or $7n \pm 3$.

$\Rightarrow\; a^2 = 49n^2$, $49n^2 \pm 14n + 1$, $49n^2 \pm 28n + 4$,

or $49n^2 \pm 42n + 9$

$\Rightarrow\; a^2 = 7(7n^2)$, $7(7n^2 \pm 2n) + 1$, $7(7n^2 \pm 4n) + 4$,

or $7(7n^2 \pm 6n + 1) + 2$

$\Rightarrow\; a^2$ has form $7k$, $7k + 1$, $7k + 4$, or $7k + 2$ .... (1)

Also $a^3 = 343n^3$, $343n^3 \pm 147n^2 + 21n \pm 1$,

$343n^3 \pm 294n^2 + 84n \pm 8$,

or $343n^3 \pm 441n^2 + 189n \pm 27$

$\Rightarrow\; a^3 = 7(49n^3)$, $7(49n^3 \pm 21n^2 + 3n) \pm 1$,

$7(49n^3 \pm 42n^2 + 12n) \pm 8$,

or $7(49n^3 \pm 63n^2 + 27n) \pm 27$

$\Rightarrow\; a^3$ has form $7k$, $7k \pm 1$, $7k \pm 8$, or $7k \pm 27, \;\; k \in \mathbb{Z}$

$\Rightarrow\; a^3$ has form $7k$ or $7k \pm 1, \;\; k \in \mathbb{Z}$ .... (2)

From both (1) and (2) the only cases common are a^2 and a^3 have form $7k$ and $7k + 1$.

15 **a** n is either even or odd

$\Rightarrow\; n = 2a$ or $2a + 1, \;\; a \in \mathbb{Z}^+$

$\therefore \quad 7n^3 + 5n$

$= n(7n^2 + 5)$

$= 2a(7(2a)^2 + 5)$ or $(2a+1)(7(2a+1)^2 + 5)$

$= 2a(28a^2 + 5)$ or $(2a+1)(28a^2 + 28a + 12)$

$= 2a(28a^2 + 5)$ or $4(2a+1)(7a^2 + 7a + 3)$

both of which are even.

b $n \in \mathbb{Z}^+$

$\Rightarrow$ n has form $3a$ or $3a \pm 1$

$\Rightarrow$ $n(7n^2 + 5)$

$= 3a(63a^2 + 5)$ or $(3a \pm 1)(7[3a \pm 1]^2 + 5)$

$= (3a \pm 1)(63a^2 \pm 42a + 12)$

$= 3(3a \pm 1)(21a^2 \pm 14a + 4)$

$\Rightarrow$ $n(7n^2 + 5) = 3k, \ k \in \mathbb{Z}$

c From **a** and **b**, $n(7n^2 + 5)$ is divisible by 2 and 3

$\therefore$ $n(7n^2 + 5)$ is divisible by 6.

d Any integer n has form $6n$, $6n \pm 1$, $6n \pm 2$, $6n + 3$, $n \in \mathbb{Z}$

$\therefore$ $n(7n^2 + 5)$ has form

$= 6n(7(6n)^2 + 5)$ which is divisible by 6.

or $(6n \pm 1)(7(6n \pm 1)^2 + 5)$

$= (6n \pm 1)(252n^2 \pm 84n + 12)$

$= 6(6n \pm 1)(42n^2 \pm 14n + 2)$

which is divisible by 6.

or $(6n \pm 2)(7(6n \pm 2)^2 + 5)$

$= 2(3n \pm 1)(252n^2 \pm 168n + 33)$

$= 6(3n \pm 1)(84n^2 \pm 56n + 11)$

which is divisible by 6.

or $(6n + 3)(7(6n + 3)^2 + 5)$

$= 3(2n + 1)(252n^2 + 252n + 68)$

$= 6(2n + 1)(126n^2 + 126n + 34)$

which is divisible by 6.

In all cases, $n(7n^2 + 5)$ is divisible by 6.

16 $a^3 - a = a(a^2 - 1) = a(a+1)(a-1)$ which is the product of 3 consecutive integers one of which must be a multiple of 3

$\therefore$ $3 \mid (a^3 - a)$.

17 **a** Consider $4a + 1$ and $4b + 1$; $a, b \in \mathbb{Z}$

$\therefore$ their product

$= (4a + 1)(4b + 1)$

$= 16ab + 4a + 4b + 1$

$= 4(4ab + a + b) + 1$ where $4ab + a + b \in \mathbb{Z}$

which has form $4k + 1$, $k \in \mathbb{Z}$.

b Consider $4a + 3$ and $4b + 3$

$\therefore$ the product

$= (4a + 3)(4b + 3)$

$= 16ab + 12a + 12b + 9$

$= 4(4ab + 3a + 3b + 2) + 1$

where $4ab + 3a + 3b + 2 \in \mathbb{Z}$

which has form $4p + 1$, $p \in \mathbb{Z}$.

c Any integer has form

$4k$, $4k + 1$, $4k + 2$, or $4k + 3$ for $k \in \mathbb{Z}$

$\therefore$ any odd integer has form $4k + 1$ or $4k + 3$

$\therefore$ the square of an integer is $(4k + 1)^2$ or $(4k + 3)^2$.

From **a** and **b** such squares have form $4p + 1$, $p \in \mathbb{Z}$.

d From **c**, for any odd integer a,

$a^2 = 4p + 1$ for $p \in \mathbb{Z}$

$\Rightarrow$ $a^4 = 16p^2 + 8p + 1$

$\Rightarrow$ $a^4 = 8(2p^2 + p) + 1$

which has form $8k + 1$, $k \in \mathbb{Z}$.

18 **a** **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$n(n+1)(n+2)$ is divisible by 6", $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $1 \times 2 \times 3 = 6$ is divisible by 6.

$\therefore$ P_1 is true.

(2) If P_k is true, then $k(k+1)(k+2) = 6A$, $A \in \mathbb{Z}$.

$\therefore \quad (k+1)(k+2)(k+3)$

$= k(k+1)(k+2) + 3(k+1)(k+2)$

$= 6A + 3(2B)$

{as $(k+1)$, $(k+2)$ are consecutive, one of them must be even}

$= 6(A + B)$ where $A + B \in \mathbb{Z}$

$\therefore$ $(k+1)(k+2)(k+3)$ is divisible by 6.

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true, $n \in \mathbb{Z}^+$.

b Every integer n has form $6a$, $6a + 1$, $6a + 2$, $6a + 3$, $6a + 4$, or $6a + 5$, $a \in \mathbb{Z}$.

$\therefore$ $n(n+1)(n+2)$

$= 6a(6a + 1)(6a + 2)$, or $(6a + 1)(6a + 2)(6a + 3)$,

or $(6a + 2)(6a + 3)(6a + 4)$,

or $(6a + 3)(6a + 4)(6a + 5)$,

or $(6a + 4)(6a + 5)(6a + 6)$,

or $(6a + 5)(6a + 6)(6a + 7)$

$= 6a(6a + 1)(6a + 2)$, or $6(6a + 1)(3a + 1)(2a + 1)$,

or $6(3a + 1)(2a + 1)(6a + 4)$,

or $6(2a + 1)(3a + 2)(6a + 5)$,

or $6(6a + 4)(6a + 5)(a + 1)$,

or $6(6a + 5)(a + 1)(6a + 7)$

In each case divisibility by 6 occurs.

19 **a** **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$5 \mid (n^5 - n)$", $n \in \mathbb{Z}^+$.

(1) If $n = 1$, $1^5 - 1 = 0$ and $0 = 5(0)$

$\therefore$ $5 \mid 0$

$\therefore$ P_1 is true.

(2) If P_k is true, then $k^5 - k = 5A$, $A \in \mathbb{Z}$.

$\therefore \quad (k+1)^5 - (k+1)$

$= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + \cancel{1} - k - \cancel{1}$

$= k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k)$

$= 5A + 5B$ where $A, B \in \mathbb{Z}$

$= 5(A + B)$

Thus P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true, $n \in \mathbb{Z}^+$.

b $n^5 - n = n(n^4 - 1)$

$= n(n^2 - 1)(n^2 + 1)$

$= n(n + 1)(n - 1)(n^2 + 1)$

where n has form $5a$, $5a + 1$, $5a + 2$, $5a + 3$, $5a + 4$

$\therefore$ $n^5 - n = 5a(5a + 1)(5a - 1)(25a^2 + 1)$

which is divisible by 5

or $= (5a + 1)(5a + 2)(5a)((5a + 1)^2 + 1)$

which is divisible by 5

or $= (5a+2)(5a+3)(5a+1)(25a^2+20a+5)$

$= 5(5a+2)(5a+3)(5a+1)(5a^2+4a+1)$

which is divisible by 5

or $= (5a+3)(5a+4)(5a+2)(25a^2+30a+10)$

$= 5(5a+3)(5a+4)(5a+2)(5a^2+6a+2)$

which is divisible by 5

or $= (5a+4)(5a+5)(5a+3)(25a^2+40a+17)$

$= 5(5a+4)(a+1)(5a+3)(25a^2+40a+17)$

which is divisible by 5

So, in all cases $n^5 - n$ is divisible by 5.

20 Let the integers be $n-1$, n, and $n+1$, $n \in \mathbb{Z}$.

$\therefore$ the sum of cubes

$= (n-1)^3 + n^3 + (n+1)^3$

$= n^3 - \cancel{3n^2} + 3n - \cancel{1} + n^3 + n^3 + \cancel{3n^2} + 3n + \cancel{1}$

$= 3n^3 + 6n$

$= 3n(n^2+2)$ which is divisible by 3.

We now need to prove that $n(n^2+2)$ is divisible by 3 for all $n \in \mathbb{Z}$.

Proof: If n is divisible by 3 there is nothing to prove.

If n is not divisible by 3 then $n = 3k \pm 1$.

$\therefore$ $n(n^2+2) = (3k \pm 1)(9k^2 \pm 6k + 3)$

$= 3(3k \pm 1)(3k^2 \pm 2k + 1)$

which is divisible by 3.

EXERCISE 1C.3

1 $110\,101\,011_2$

$= 2^8 + 2^7 + 2^5 + 2^3 + 2^1 + 1$ (in base 10)

$= 427$ (in base 10)

2 $21\,012\,201_3$

$= 2(3^7) + 1(3^6) + 1(3^4) + 2(3^3) + 2(3^2) + 1$ (in base 10)

$= 5257$ (in base 10)

3 **a**

3	347	r
3	115	2
3	38	1
3	12	2
3	4	0
	1	1

$\therefore$ $347_{10} = 110\,212_3$

b

8	1234	r
8	154	2
8	19	2
	2	3

$\therefore$ $1234_{10} = 2322_8$

c

7	5728	r
7	818	2
7	116	6
7	16	4
	2	2

$\therefore$ $5728_{10} = 22\,462_7$

4

5	87 532	r
5	17 506	2
5	3501	1
5	700	1
5	140	0
5	28	0
5	5	3
	1	0

$\therefore$ $87\,532_{10} = 10\,300\,112_5$

5 **a** $1\,001\,111\,101_2$

$= 2^9 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 1$ (in base 10)

$= 637_{10}$

b

4	637	r
4	159	1
4	39	3
4	9	3
	2	1

$\therefore$ $637_{10} = 21\,331_4$

c

8	637	r
8	79	5
8	9	7
	1	1

$\therefore$ $637_{10} = 1175_8$

6 **a** $201\,021\,102_3$

$= 2(3^8) + 3^6 + 2(3^4) + 3^3 + 3^2 + 2$ (base 10)

$= 14\,051_{10}$

b

9	14 051	r
9	1561	2
9	173	4
9	19	2
	2	1

$\therefore$ $14\,051_{10} = 21\,242_9$

7 $2\,122\,122\,102_3$

$= 2(3^9) + 3^8 + 2(3^7) + 2(3^6) + 3^5 + 2(3^4) + 2(3^3)$

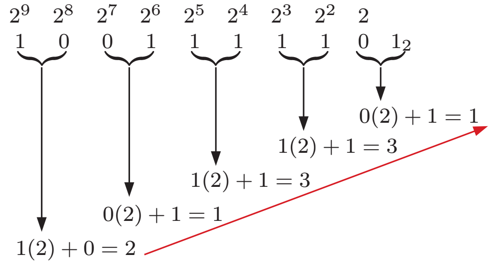
$+ 3^2 + 2$ (in base 10)

$= 52\,229_{10}$

9	52 229	r
9	5803	2
9	644	7
9	71	5
	7	8

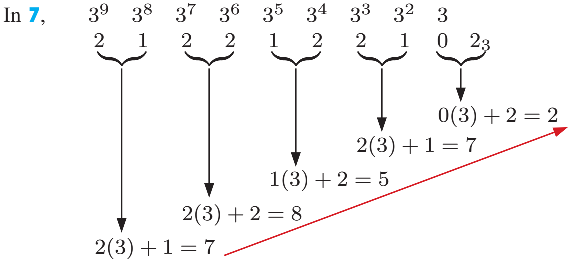
$\therefore$ $2\,122\,122\,102_3 = 78\,572_9$

8 In **5**,



$\therefore$ $1\,001\,111\,101_2 = 21\,331_4$

In **7**,



$\therefore \quad 2\,122\,122\,102_3 = 78\,572_9$

Suppose we have columns

$$\begin{array}{ccccccccc} k^8 & k^7 & k^6 & k^5 & k^4 & k^3 & k^2 & k^1 & k^0 \\ a_8 & \underbrace{a_7 \quad a_6} & & \underbrace{a_5 \quad a_4} & & a_3 & a_2 & \underbrace{a_1 \quad a_0}_{} & {}_k \longleftarrow \text{base } k \end{array}$$

We pair the digits from right to left.

For base k^2, $a_1k + a_0$ gives the number of k^0s

$a_3k + a_2$ gives the number of k^2s

$a_5k + a_4$ gives the number of k^4s

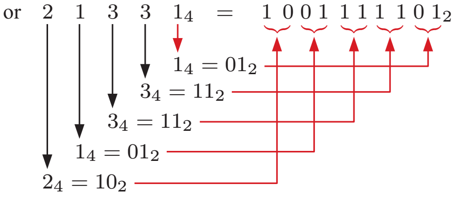
$a_7k + a_6$ gives the number of k^6s

etc.

9 We use the reverse process to that in **8**.

For example, in **5** we showed that

$1\,001\,111\,101_2 = 21\,331_4$



$$\begin{array}{ccccc} & k^6 & k^4 & k^2 & k^0 \\ \ldots & a_3 & a_2 & a_1 & a_{0\,k^2} \end{array}$$

$a_{0_{k^2}}$ becomes $b_1k + b_0$

$a_{1_{k^2}}$ becomes $b_3k + b_2$

$\vdots$

etc.

10 In base 2, $0_4 = 00_2$, $1_4 = 01_2$, $2_4 = 10_2$, $3_4 = 11_2$.

$\therefore \quad 3 \quad 1 \quad 3 \quad 1 \quad 2 \quad 3 \quad 0 \quad 1 \quad 2_4$

$= 11\;01\;11\;01\;10\;11\;00\;01\;10_2$

11 In base 3, $0_9 = 00_3$, $1_9 = 01_3$, $2_9 = 02_3$,

$3_9 = 10_3$, $4_9 = 11_3$, $5_9 = 12_3$,

$6_9 = 20_3$, $7_9 = 21_3$, $8_9 = 22_3$.

$\therefore \quad 6 \quad 3 \quad 2 \quad 6 \quad 4 \quad 5 \quad 2 \quad 3 \quad 7 \quad 8_9$

$= 20\;10\;02\;20\;11\;12\;02\;10\;21\;22_3$

12 $56\,352\,743_8$

$= 5(8^7) + 6(8^6) + 3(8^5) + 5(8^4) + 2(8^3) + 7(8^2)$

$+ 4(8) + 3$ (in base 10)

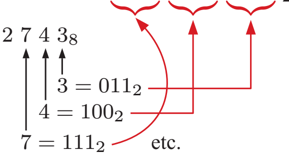
$= 12\,178\,915_{10}$

2	12 178 915	r
2	6 089 457	1
2	3 044 728	1
2	1 522 364	0
2	761 182	0
2	380 591	0
2	190 295	1
2	95 147	1
2	47 573	1
2	23 786	1
2	11 893	0
2	5946	1
2	2973	0
2	1486	1
2	743	0
2	371	1
2	185	1
2	92	1
2	46	0
2	23	0
2	11	1
2	5	1
2	2	1
	1	0

$\therefore \quad 56\,352\,743_8$

$= 101\;110\;011\;101\;010\;111\;100\;011_2$

Note: In $5\;6\;3\;5\;2\;7\;4\;3_8$



gives a quicker method for converting base 8 to base 2 numbers.

13 Suppose $\frac{5}{7} = a_1 \times 10^{-1} + a_2 \times 10^{-2} + \ldots.$

$\therefore \quad \frac{50}{7} = a_1 + \dfrac{a_2}{10} + \dfrac{a_3}{10^2} + \ldots.$

$\therefore \quad 7 + \frac{1}{7} = a_1 + \dfrac{a_2}{10} + \dfrac{a_3}{10^2} + \ldots.$

$\therefore \quad a_1 = 7$

Also $\frac{500}{7} = 10a_1 + a_2 + \dfrac{a_3}{10} + \dfrac{a_4}{10^2} + \ldots.$

$\therefore \quad 71\frac{3}{7} = 70 + a_2 + \dfrac{a_3}{10} + \dfrac{a_4}{10^2} + \ldots.$

$\therefore \quad 71 = 70 + a_2$

$\therefore \quad a_2 = 1$

And $\frac{5000}{7} = 100a_1 + 10a_2 + a_3 + \dfrac{a_4}{10} + \ldots.$

$\therefore \quad 714\frac{2}{7} = 710 + a_3 + \dfrac{a_4}{10} + \ldots.$

$\therefore \quad 714 = 710 + a_3$

$\therefore \quad a_3 = 4$

Continuing this process gives

$a_4 = 2$, $a_5 = 8$, $a_6 = 5$, $a_7 = 7$, $a_8 = 1$, etc.

$\therefore \quad \frac{5}{7} = 0.714\,285\,714\,285\ldots.$

That is, $\frac{5}{7} = 0.\overline{714\,285}.$

EXERCISE 1C.4

1 (1) First we prove that

'if p^2 is even then p is even; $p \in \mathbb{Z}^+$'.

Proof: $p = 2t$ or $2t+1$ for every $p \in \mathbb{Z}^+$

$\therefore$ $p^2 = 4t^2$ or $4t^2 + 4t + 1$

$\therefore$ $p^2 = \underbrace{2(2t^2)}_{\text{even}}$ or $\underbrace{2(2t^2+2t)+1}_{\text{odd}}$

Thus p^2 being even can only result in p being even.

(2) Now we prove that $\sqrt{2}$ is irrational.

Proof: (by contradiction)

Suppose $\sqrt{2}$ is rational.

$\therefore$ $\sqrt{2} = \dfrac{p}{q}$, $p, q \in \mathbb{Z}^+$, $q \neq 0$ and p, q have no common factors besides 1.

$\therefore$ $p = q\sqrt{2}$

$\therefore$ $p^2 = 2q^2$ .... $(*)$

$\therefore$ p^2 is even $\{q^2 \in \mathbb{Z}^+\}$

$\therefore$ p is even $\{$from (1)$\}$

$\therefore$ $p = 2t$, for some $t \in \mathbb{Z}^+$

$\therefore$ $4t^2 = 2q^2$ $\{$in $*\}$

$\therefore$ $q^2 = 2t^2$

$\therefore$ q^2 is even

$\therefore$ q is even $\{$from (1)$\}$

On the supposition we have shown that both p and q are even and $\therefore$ share a common factor of 2, a contradiction.

$\therefore$ $\sqrt{2}$ is irrational.

2 (1) First we prove that

'if p^2 has a factor of 5, then p has a factor of 5 for all $p \in \mathbb{Z}^+$'.

Proof:

For every $p \in \mathbb{Z}^+$,

$p = 5t,\ 5t \pm 1,$ or $5t \pm 2,$ $t \in \mathbb{Z}^+$

$\therefore$ $p^2 = 25t^2,\ 25t^2 \pm 10t + 1,$ or $25t^2 \pm 20t + 4$

$\therefore$ $p^2 = 5(5t^2),\ 5(5t^2 \pm 2t) + 1,$ or $5(5t^2 \pm 4t) + 4$

where only $p^2 = 5(5t^2)$ has 5 as a factor

$\therefore$ if p^2 has a factor 5, then p has a factor of 5.

(2) Now we prove that $\sqrt{5}$ is irrational.

Proof: (by contradiction)

Suppose $\sqrt{5}$ is rational.

$\therefore$ $\sqrt{5} = \dfrac{p}{q}$; $p, q \in \mathbb{Z}^+$, $q \neq 0$ and p and q have no common factors besides 1.

$\therefore$ $p = q\sqrt{5}$

$\therefore$ $p^2 = 5q^2$ .... $(*)$

$\therefore$ p^2 has a factor of 5

$\therefore$ p has a factor of 5 $\{$from (1)$\}$

$\therefore$ $p = 5t$ for some $t \in \mathbb{Z}^+$

$\therefore$ $25t^2 = 5q^2$ $\{$in $*\}$

$\therefore$ $q^2 = 5t^2$

$\therefore$ q^2 has a factor of 5

$\therefore$ q has a factor of 5 $\{$from (1)$\}$

$\therefore$ both p and q have a common factor of 5, which is a contradiction.

$\therefore$ $\sqrt{5}$ is irrational.

3 If p^2 has a factor of 4 then it **does not** follow that p has a factor of 4.

For example, $6^2 = 36$ has a factor of 4 but 6 does not.

4 $2^{\frac{1}{4}}$ is irrational.

Proof: (by contradiction)

Let $2^{\frac{1}{4}} = \dfrac{p}{q}$ where $p, q \in \mathbb{Z}^+$, $q \neq 0$ and p, q have no common factors besides 1.

$\therefore$ $\dfrac{p^4}{q^4} = 2$

$\therefore$ $p^4 = 2q^4$ .... $(*)$

$\therefore$ p^4 is even

$\therefore$ p^2 is even $\{a^2$ even $\Rightarrow a$ even, from **1**$\}$

$\therefore$ p is even

$\therefore$ $p = 2t$ for some $t \in \mathbb{Z}^+$

$\therefore$ $16t^4 = 2q^4$ $\{$in $*\}$

$\therefore$ $q^4 = 8t^4$

$\therefore$ q^4 is even

$\therefore$ q^2 even

$\therefore$ q is even

$\therefore$ both p, q are even and $\therefore$ have a common factor of 2, which is a contradiction.

$\therefore$ $2^{\frac{1}{4}}$ is irrational.

EXERCISE 1D.1

1 **a** **i** $a \mid b \Rightarrow b = ka$ for some $k \in \mathbb{Z}$

$\Rightarrow bc = kac$

$\Rightarrow a \mid bc$ $\{$as $kc \in \mathbb{Z}\}$

ii $a \mid b$ and $a \mid c$

$\Rightarrow b = k_1 a$ and $c = k_2 a$ for $k_1, k_2 \in \mathbb{Z}$

$\Rightarrow bc = k_1 k_2 a^2$

$\Rightarrow a^2 \mid bc$ $\{$as $k_1 k_2 \in \mathbb{Z}\}$

iii $a \mid b$ and $c \mid d$

$\Rightarrow b = k_1 a$ and $d = k_2 c$ for $k_1, k_2 \in \mathbb{Z}$

$\Rightarrow bd = k_1 k_2 ac$

$\Rightarrow ac \mid bd$ $\{$as $k_1 k_2 \in \mathbb{Z}\}$

iv $a \mid b$

$\Rightarrow b = ka$ for some $k \in \mathbb{Z}$

$\Rightarrow b^n = k^n a^n$

$\Rightarrow a^n \mid b^n$ $\{$as $k^n \in \mathbb{Z}\}$

b The converse is true.

Proof: $a^n \mid b^n$

$\Rightarrow b^n = ka^n$ for $k \in \mathbb{Z}$

$\Rightarrow k = \left(\dfrac{b}{a}\right)^n$, which is only an integer if $\dfrac{b}{a}$ is an integer

$\Rightarrow a \mid b$

2 For $k \in \mathbb{Z}$, k must have one of the forms $3a$, $3a+1$, $3a+2$, $a \in \mathbb{Z}$.

k	$k+2$	$k+4$
$3a$	$3a+2$	$3a+4$
$3a+1$	$3a+3$	$3a+5$
$3a+2$	$3a+4$	$3a+6$

So, for each value of k, one of k, $k+2$, $k+4$ is divisible by 3.

3 The statement is false. A counter example is:

$8 \mid (13+3)$, but $8 \nmid 13$ and $8 \nmid 3$.

4 **a** No integer solutions exist for $24x + 18y = 9$ as $\gcd(24, 18) = 6$ and 9 is not a multiple of 6.

or LHS is even and RHS is odd.

b Integer solutions exist for $2x+3y=67$ as $\gcd(2,\,3)=1$ and 67 is a multiple of 1.
$x_0=32,\ \ y_0=1$ is one solution.
Since $\frac{3}{1}=3$ and $\frac{2}{1}=2,$ the solutions are
$x=32+3t,\ \ y=1-2t$ for $t\in\mathbb{Z}$.

Check:
$$\begin{aligned}2x+3y&=2(32+3t)+3(1-2t)\\&=64+6t+3-6t\\&=67\ \ \checkmark\end{aligned}$$

c Integer solutions exist for $57x+95y=19$ as $\gcd(57,\,95)=19$ and 19 is a multiple of 19.
$x_0=-3,\ \ y_0=2$ is one solution.
Since $\frac{95}{19}=5$ and $\frac{57}{19}=3,$ the solutions are
$x=-3+5t,\ \ y=2-3t$ for $t\in\mathbb{Z}$.

d
$$\begin{array}{r|r} 5 & 1035 \\ \hline 3 & 207 \\ \hline 3 & 69 \\ \hline 23 & 23 \\ \hline & 1 \end{array}\qquad\qquad \begin{array}{r|r} 5 & 585 \\ \hline 3 & 117 \\ \hline 3 & 39 \\ \hline 13 & 13 \\ \hline & 1 \end{array}$$

$\therefore\ \ \gcd(1035,\,585)=5\times3^2=45$
So, no integer solutions exist for $1035x+585y=901$ as 901 is not a multiple of 45.

e Integer solutions exist for $45x-81y=108$ as $\gcd(45,\,81)=9$ and 108 is a multiple of 9.
$x_0=6,\ \ y_0=2$ is one solution.
Since $-\frac{81}{9}=-9$ and $\frac{45}{9}=5,$ the solutions are
$x=6-9t,\ \ y=2-5t$ for $t\in\mathbb{Z}$ $\{b=-81\}$

5 **a** **i** Any integer n must be of the form $3a,\ \ 3a+1,$ or $3a+2$.

n	$n+1$	$n+2$
$3a$	$3a+1$	$3a+2$
$3a+1$	$3a+2$	$3a+3$
$3a+2$	$3a+3$	$3a+4$

Each time one of the factors is divisible by 3
$\therefore\ \ n(n+1)(n+2)$ is divisible by 3.

ii In any set of 3 consecutive integers at least one of them is even (divisible by 2), and from **i** the product is divisible by 3. Since $\gcd(2,\,3)=1,$ the product is divisible by $2\times3=6$.

iii In any set of 4 consecutive integers one of them must be divisible by 2 and another by 4
$\therefore$ their product is divisible by 8.

iv In any set of 4 consecutive integers at least one of them is divisible by 3, so the product is divisible by 3.
From **iii**, the product is also divisible by 8.
Since $\gcd(3,\,8)=1,$ the product of the four consecutive integers is divisible by $3\times8=24$.

b Let $x+1,\ \ x+2,\ \ x+3,\ \ ....,\ \ x+n$ be the n consecutive integers, $x\in\mathbb{N}$.
Now their product is
$$\begin{aligned}&(x+1)(x+2)(x+3)....(x+n)\\&=\frac{(x+n)!}{x!}\\&=n!\frac{(x+n)!}{x!\,n!}\\&=n!\times\binom{x+n}{x}\end{aligned}$$
where $\binom{x+n}{x}\in\mathbb{Z}$ {binomial coefficient}
$\therefore$ the product is divisible by $n!$

6 For $k\in\mathbb{Z},\ \ k$ must have form $3a,\ \ 3a+1,$ or $3a+2$.
$$\begin{aligned}\therefore\ \ k(k^2+8)&=3a(9a^2+8)\\ \textit{or}\quad &(3a+1)[(3a+1)^2+8]\\&=(3a+1)[9a^2+6a+9]\\&=3(3a+1)(3a^2+2a+3)\\ \textit{or}\quad &(3a+2)[(3a+2)^2+8]\\&=(3a+2)[9a^2+12a+12]\\&=3(3a+2)(3a^2+4a+4)\end{aligned}$$
In each case $3\mid k(k^2+8)$.

7 **a** $1\times2\times3\times4=24\ \ =5^2-1\ \ \checkmark$
$2\times3\times4\times5=120=11^2-1\ \ \checkmark$
$3\times4\times5\times6=360=19^2-1\ \ \checkmark$

b Let the integers be $n-1,\ \ n,\ \ n+1,\ \ n+2$.
$\therefore$ their product
$$\begin{aligned}&=(n-1)n(n+1)(n+2)\\&=(n^2+n)(n^2+n-2)\\&=(n^2+n-1+1)(n^2+n-1-1)\\&=(n^2+n-1)^2-1\end{aligned}$$
where $(n^2+n-1)^2$ is a perfect square
$\therefore$ Heta's claim is valid.

8 **a** Let $\gcd(a,\,a+n)=d$
$\therefore\ \ d\mid a$ and $d\mid a+n$
$\therefore\ \ d\mid(a+n)-a$ {linearity property}
$\therefore\ \ d\mid n$
$\therefore\ \ \gcd(a,\,a+n)\mid n$.

b If $n=1,\ \ \gcd(a,\,a+1)\mid1$ {from **a**}
$\therefore\ \ \gcd(a,\,a+1)=1$
{since $\gcd(a,\,a+1)\geqslant1$}

9 *Theorem to use*: $\gcd(a,\,b)=\gcd(a+cb,\,b),\ \ a,\,b,\,c\in\mathbb{Z}$.

a
$$\begin{aligned}&\gcd(3k+1,\,13k+4)\\&=\gcd(13k+4,\,3k+1)\\&=\gcd(13k+4-4(3k+1),\,3k+1)\\&=\gcd(k,\,3k+1)\\&=\gcd(3k+1,\,k)\\&=\gcd(3k+1-3k,\,k)\\&=\gcd(1,\,k)\\&=1\end{aligned}$$

b
$$\begin{aligned}&\gcd(5k+2,\,7k+3)\\&=\gcd(7k+3,\,5k+2)\\&=\gcd(7k+3-(5k+2),\,5k+2)\\&=\gcd(2k+1,\,5k+2)\\&=\gcd(5k+2,\,2k+1)\\&=\gcd(5k+2-2(2k+1),\,2k+1)\\&=\gcd(k,\,2k+1)\\&=\gcd(2k+1,\,k)\\&=\gcd(2k+1-2k,\,k)\\&=\gcd(1,\,k)\\&=1\end{aligned}$$

10 **a** Let $d = \gcd(4a-3b,\ 8a-5b)$

$$\begin{aligned} &= \gcd(8a-5b,\ 4a-3b) \\ &= \gcd(8a-5b-2(4a-3b),\ 4a-3b) \\ &= \gcd(b,\ 4a-3b) \\ &= \gcd(4a-3b,\ b) \\ &= \gcd(4a-3b+3b,\ b) \\ &= \gcd(4a,\ b) \end{aligned}$$

$\therefore\ d \mid b$ and $d \mid 4a$

$\therefore\ d$ divides b, but $d \mid a$ is not necessarily true.

b In **a**, if $b=-1$, $d = \gcd(4a+3,\ 8a+5)$

$\therefore\ d \mid -1$

$\therefore\ d = 1$ {as $d > 0$}

$\therefore\ \gcd(4a+3,\ 8a+5) = 1.$

11 $\gcd(a, b) = 1$

$\therefore\ x, y \in \mathbb{Z}$ exist such that $ax+by=1.$

But $c \mid a$

$\therefore\ a = kc$ where $k \in \mathbb{Z}.$

Thus $kcx + by = 1$

$\therefore\ c(kx) + by = 1$ for integers $kx, y \in \mathbb{Z}$

$\therefore\ \gcd(c, b) = 1$

{$\gcd(c, b)$ is the least positive integer which can be expressed as an integer linear combination of c and b.}

12 If $\gcd(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that

$ax + by = 1$ .... (1)

$\therefore\ (ax+by)^2 = 1$

$\therefore\ a^2x^2 + 2abxy + b^2y^2 = 1$

$\therefore\ a^2x^2 + (2axy + by^2)b = 1$

and $(ax^2 + 2bxy)a + b^2y^2 = 1$

$\therefore\ \gcd(a^2, b) = 1$ and $\gcd(a, b^2) = 1$

To prove $\gcd(a^2, b^2) = 1$

Proof:

$\gcd(a^2, b) = 1 \ \Rightarrow\ a^2p_1 + bp_2 = 1$ .... (2)

$\gcd(a, b^2) = 1 \ \Rightarrow\ aq_1 + b^2q_2 = 1$ .... (3)

where $p_1, p_2, q_1, q_2 \in \mathbb{Z}.$

But as $ax + by = 1$, {from (1)}

then $a^2bx + ab^2y = ab$ .... (4)

From (2), $a^3p_1 + abp_2 = a$

Hence $a^3p_1 + (a^2bx + ab^2y)p_2 = a$ {using (4)}

and in (3), $(a^3p_1 + a^2bp_2x + ab^2p_2y)q_1 + b^2q_2 = 1$

$\therefore\ a^2[ap_1q_1 + bp_2q_1x] + b^2[ap_2q_1y + q_2] = 1$

where $ap_1q_1 + bp_2q_1x,\ ap_2q_1y + q_2 \in \mathbb{Z}$

$\therefore\ \gcd(a^2, b^2) = 1$

13 **Proof:** (by contradiction)

Suppose $\sqrt{3}$ is rational

$\therefore\ \sqrt{3} = \dfrac{p}{q}$ where $p, q \in \mathbb{Z}^+$, $\gcd(p, q) = 1$

$\therefore\ rp + sq = 1$ for some $r, s \in \mathbb{Z}^+$

Hence $\sqrt{3} = \sqrt{3}(rp + sq)$

$\therefore\ \sqrt{3} = (\sqrt{3}p)r + (\sqrt{3}q)s$

$\therefore\ \sqrt{3} = (\sqrt{3}\sqrt{3}q)r + \sqrt{3}\left(\dfrac{p}{\sqrt{3}}\right)s$

$\therefore\ \sqrt{3} = 3qr + ps$

$\therefore\ \sqrt{3}$ is an integer {as $p, q, r, s \in \mathbb{Z}$}

which is a contradiction. Hence $\sqrt{3}$ is irrational.

14 **a** Using the given identity with $x = 2$, we have:

$$\begin{aligned} 2^k - 1 &= 2^{k-1} + 2^{k-2} + 2^{k-3} + \dots + 2^2 + 2 + 1 \\ &= \underbrace{1111\dots11}_{k \text{ of them}}{}_2 \\ &= k\text{th repunit in base } 2 \end{aligned}$$

So, $d \mid n \ \Rightarrow\ d$th repunit $\mid n$th repunit {in base 2}

$\Rightarrow\ (2^d - 1) \mid (2^n - 1)$

b $5 \mid 35 \ \Rightarrow\ (2^5 - 1) \mid (2^{35} - 1)$

$\Rightarrow\ 31 \mid (2^{35} - 1)$

and $7 \mid 35 \ \Rightarrow\ (2^7 - 1) \mid (2^{35} - 1)$

$\Rightarrow\ 127 \mid (2^{35} - 1)$

So, $2^{35} - 1$ is divisible by 31 and 127.

15 $\gcd(3k+2,\ 5k+3)$

$$\begin{aligned} &= \gcd(5k+3,\ 3k+2) \\ &= \gcd(5k+3-(3k+2),\ 3k+2) \\ &= \gcd(2k+1,\ 3k+2) \\ &= \gcd(3k+2,\ 2k+1) \\ &= \gcd(3k+2-(2k+1),\ 2k+1) \\ &= \gcd(k+1,\ 2k+1) \\ &= \gcd(2k+1,\ k+1) \\ &= \gcd(2k+1-(k+1),\ k+1) \\ &= \gcd(k,\ k+1) \\ &= 1 \qquad \{\text{from } \mathbf{8\ b}\} \end{aligned}$$

$\therefore\ 3k+2$ and $5k+3$ are relatively prime.

16 $\gcd(11k+7,\ 5k+3)$

$$\begin{aligned} &= \gcd(11k+7-2(5k+3),\ 5k+3) \\ &= \gcd(k+1,\ 5k+3) \\ &= \gcd(5k+3,\ k+1) \\ &= \gcd(5k+3-4(k+1),\ k+1) \\ &= \gcd(k-1,\ k+1) \\ &= \gcd(k+1,\ k-1) \\ &= \gcd(k+1-(k-1),\ k-1) \\ &= \gcd(2,\ k-1) \\ &= \begin{cases} 1 & \text{if } k \text{ is even} \\ 2 & \text{if } k \text{ is odd} \end{cases} \end{aligned}$$

$\therefore\ 5k+3$ and $11k+7$ are relatively prime if $k \in \mathbb{Z}^+$ is even.

17 Let $d = \gcd(a+b,\ a-b)$

$\therefore\ d = \gcd(a+b-(a-b),\ a-b)$

$\therefore\ d = \gcd(2b,\ a-b)$

$\therefore\ d \mid (2b)$ .... (1)

Also $d = \gcd(a+b+(a-b),\ a-b)$

$\therefore\ d = \gcd(2a,\ a-b)$

$\therefore\ d \mid (2a)$ .... (2)

But $\gcd(a, b) = 1$ and so $\gcd(2a, 2b) = 2$

$\therefore$ from (1) and (2), $d \mid 2$

$\therefore\ d = 1$ or 2

$\therefore\ \gcd(a+b,\ a-b) = 1$ or 2.

EXERCISE 1D.2

1 **a** $803 = 154(5) + 33$

$154 = 33(4) + 22$

$33 = 22(1) + 11$

$22 = 11(2) + 0$

$$\begin{aligned}
\therefore\quad &\gcd(803,\ 154) = 11\\
\text{and}\quad 11 &= 33 - 22\\
&= 33 - (154 - 33(4))\\
&= 33 \times 5 - 154\\
&= (803 - 154(5)) \times 5 - 154\\
&= 5 \times 803 - 26 \times 154
\end{aligned}$$

$\therefore\quad 11 = r(803) + s(154)$ where $r = 5,\ s = -26.$

b

$$\begin{aligned}
12\,378 &= 3054(4) + 162\\
3054 &= 162(18) + 138\\
162 &= 138(1) + 24\\
138 &= 24(5) + 18\\
24 &= 18(1) + 6\\
18 &= 6(3) + 0
\end{aligned}$$

$$\begin{aligned}
\therefore\quad &\gcd(12\,378,\ 3054) = 6\\
\text{and}\quad 6 &= 24 - 18\\
&= 24 - (138 - 24(5))\\
&= 24 \times 6 - 138\\
&= (162 - 138) \times 6 - 138\\
&= 6 \times 162 - 7 \times 138\\
&= 6 \times 162 - 7(3054 - 162(18))\\
&= 132 \times 162 - 7 \times 3054\\
&= 132(12\,378 - 3054(4)) - 7 \times 3054\\
&= \underset{\substack{\uparrow\\ r}}{132} \times 12\,378\ \underbrace{-\ 535}_{\substack{\uparrow\\ s}} \times 3054
\end{aligned}$$

c $3172 = 793(4) + 0$

$\therefore\quad \gcd(3174,\ 793) = 793$

and $\quad 793 = \underset{\substack{\uparrow\\ r}}{0} \times 3174 + \underset{\substack{\uparrow\\ s}}{1} \times 793$

d

$$\begin{aligned}
1265 &= 805(1) + 460\\
805 &= 460(1) + 345\\
460 &= 345(1) + 115\\
345 &= 115(3) + 0
\end{aligned}$$

$$\begin{aligned}
\therefore\quad &\gcd(1265,\ 805) = 115\\
\text{and}\quad 115 &= 460 - 345\\
&= 460 - (805 - 460)\\
&= 460 \times 2 - 805\\
&= (1265 - 805) \times 2 - 805\\
&= \underset{\substack{\uparrow\\ r}}{2} \times 1265\ \underbrace{-\ 3}_{\substack{\uparrow\\ s}} \times 805
\end{aligned}$$

e

$$\begin{aligned}
55 &= 34(1) + 21\\
34 &= 21(1) + 13\\
21 &= 13(1) + 8\\
13 &= 8(1) + 5\\
8 &= 5(1) + 3\\
5 &= 3(1) + 2\\
3 &= 2(1) + 1\\
2 &= 1(2) + 0
\end{aligned}$$

$$\begin{aligned}
\therefore\quad &\gcd(55,\ 34) = 1\\
\text{and}\quad 1 &= 3 - 2\\
&= 3 - (5 - 3)\\
&= 3 \times 2 - 5\\
&= (8 - 5) \times 2 - 5\\
&= 2 \times 8 - 3 \times 5\\
&= 2 \times 8 - 3(13 - 8)\\
&= 5 \times 8 - 3 \times 13\\
&= 5(21 - 13) - 3 \times 13\\
&= 5 \times 21 - 8 \times 13\\
&= 5 \times 21 - 8(34 - 21)\\
&= 13 \times 21 - 8 \times 34\\
&= 13(55 - 34) - 8 \times 34\\
&= \underset{\substack{\uparrow\\ r}}{13} \times 55\ \underbrace{-\ 21}_{\substack{\uparrow\\ s}} \times 34
\end{aligned}$$

2 **a**

$$\begin{aligned}
&\gcd(f_{n+1},\ f_n)\\
&= \gcd(f_{n+1} - f_n,\ f_n) \qquad \{\text{theorem}\}\\
&= \gcd(f_{n-1},\ f_n)\\
&= \gcd(f_n,\ f_{n-1})\\
&\ \ \vdots\\
&= \gcd(f_{n-1},\ f_{n-2})\\
&\ \ \vdots\\
&= \gcd(f_2,\ f_1)\\
&= \gcd(1,\ 1)\\
&= 1
\end{aligned}$$

b **i**

$$\begin{aligned}
\gcd(f_8,\ f_4) &= \gcd(21,\ 3) &&= 3\\
\gcd(f_{12},\ f_8) &= \gcd(144,\ 21) &&= 3\\
\gcd(f_{16},\ f_{12}) &= \gcd(987,\ 144) &&= 3\\
\gcd(f_{20},\ f_{16}) &= \gcd(6765,\ 987) &&= 3
\end{aligned}$$

ii The results of **i** suggest that $\gcd(f_{4(n+1)},\ f_{4n}) = 3$ for all $n \in \mathbb{Z}^+$.

Proof:

$$\begin{aligned}
&f_{4(n+1)}\\
&= f_{4n+4}\\
&= f_{4n+3} + f_{4n+2}\\
&= f_{4n+2} + f_{4n+1} + f_{4n+2}\\
&= 2f_{4n+2} + f_{4n+1}\\
&= 2(f_{4n+1} + f_{4n}) + f_{4n+1}\\
&= 3f_{4n+1} + 2f_{4n} \quad \ldots.\ (1)
\end{aligned}$$

So, if $3 \mid f_{4n}$ then $3 \mid f_{4(n+1)}$.

But $3 \mid f_4 \qquad \{f_4 = 3\}$

$$\begin{aligned}
&\therefore\ 3 \mid f_8\\
&\therefore\ 3 \mid f_{12}\\
&\qquad\vdots\ \text{etc.}\\
&\therefore\ 3 \mid f_{4n} \quad \ldots.\ (2)
\end{aligned}$$

$$\begin{aligned}
\text{Now}\quad &\gcd(f_{4(n+1)},\ f_{4n})\\
&= \gcd(3f_{4n+1} + 2f_{4n},\ f_{4n}) \qquad \{\text{using (1)}\}\\
&= \gcd(3f_{4n+1} + \cancel{2f_{4n}} - \cancel{2f_{4n}},\ f_{4n})\\
&= \gcd(3f_{4n+1},\ f_{4n})\\
&= 3 \qquad \{\text{from (2), and } \gcd(f_{4n+1},\ f_{4n}) = 1\}
\end{aligned}$$

c

$$\begin{aligned}
\gcd(f_{10},\ f_5) &= \gcd(55,\ 5) &&= 5\\
\gcd(f_{15},\ f_{10}) &= \gcd(610,\ 55) &&= 5\\
\gcd(f_{20},\ f_{15}) &= \gcd(6765,\ 610) &&= 5
\end{aligned}$$

suggesting that $\gcd(f_{5(n+1)},\ f_{5n}) = 5$ for all $n \in \mathbb{Z}^+$.

Proof:

$$\begin{aligned}
&f_{5(n+1)}\\
&= f_{5n+5}\\
&= f_{5n+4} + f_{5n+3}\\
&= 2f_{5n+3} + f_{5n+2}\\
&= 2(f_{5n+2} + f_{5n+1}) + f_{5n+2}\\
&= 3f_{5n+2} + 2f_{5n+1}\\
&= 3(f_{5n+1} + f_{5n}) + 2f_{5n+1}\\
&= 5f_{5n+1} + 3f_{5n} \quad .... \ (1)
\end{aligned}$$

So, if $5 \mid f_{5n}$ then $5 \mid f_{5(n+1)}$.

But $5 \mid f_5$ $\{f_5 = 5\}$

$\therefore\ 5 \mid f_{10}$

$\therefore\ 5 \mid f_{15}$

$\vdots$

$\therefore\ 5 \mid f_{5n}$ .... (2)

$$\begin{aligned}
\text{Now}\quad &\gcd(f_{5(n+1)}, f_{5n})\\
&= \gcd(5f_{5n+1} + 3f_{5n}, f_{5n}) \qquad \{\text{using (1)}\}\\
&= \gcd(5f_{5n+1} + \cancel{3f_{5n}} - \cancel{3f_{5n}}, f_{5n})\\
&= \gcd(5f_{5n+1}, f_{5n})\\
&= 5 \qquad \{\text{from (2), and } \gcd(f_{5n+1}, f_{5n}) = 1\}
\end{aligned}$$

3 **a** $227 = 143(1) + 84$

$143 = 84(1) + 59$

$84 = 59(1) + 25$

$59 = 25(2) + 9$

$25 = 9(2) + 7$

$9 = 7(1) + 2$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

$\therefore\ \gcd(227, 143) = 1$

Now $\text{lcm} \times \gcd = 227 \times 143$

$\therefore\ \text{lcm} = 32\,461$

b $1749 = 272(6) + 117$

$272 = 117(2) + 38$

$117 = 38(3) + 3$

$38 = 3(12) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$\therefore\ \gcd(1749, 272) = 1$

Now $\text{lcm} \times \gcd = 1749 \times 272$

$\therefore\ \text{lcm} = 475\,728$

c From **1 b**, $\gcd(3054, 12\,378) = 6$

Now $\text{lcm} \times \gcd = 3054 \times 12\,378$

$\therefore\ \text{lcm} = \dfrac{3054 \times 12\,378}{6}$

$\therefore\ \text{lcm} = 6\,300\,402$

d $1121 = 267(4) + 53$

$267 = 53(5) + 2$

$53 = 2(26) + 1$

$2 = 1(2) + 0 \qquad \therefore\ \gcd(1121, 267) = 1$

Now $\text{lcm} \times \gcd = 1121 \times 267$

$\therefore\ \text{lcm} = 299\,307$

4 **To prove:** $\text{lcm}(a, b) = ab \Leftrightarrow \gcd(a, b) = 1$

Proof:

$(\Rightarrow)$ $\gcd(a, b) \times \text{lcm}(a, b) = ab$ $\{\text{theorem}\}$

$\therefore\ \gcd(a, b) \times ab = ab$ $\{\text{lcm}(a, b) = ab\}$

$\therefore\ \gcd(a, b) = 1$ $\{a, b \neq 0\}$

$(\Leftarrow)$ $\gcd(a, b) \times \text{lcm}(a, b) = ab$

$\therefore\ 1 \times \text{lcm}(a, b) = ab$ $\{\gcd(a, b) = 1\}$

$\therefore\ \text{lcm}(a, b) = ab$

EXERCISE 1D.3

1 **a** $\gcd(6, 51) = 3$ and $3 \nmid 22$

$\therefore$ no integer solutions exist.

b $\gcd(33, 14) = 1$ and $1 \mid 115$

$\therefore$ integer solutions exist.

Now $33 = 14(2) + 5$

$14 = 5(2) + 4$

$5 = 4(1) + 1$

$4 = 1(4) + 0$

$$\begin{aligned}
\text{thus}\quad 1 &= 5 - 4\\
&= 5 - (14 - 5(2))\\
&= 3 \times 5 - 14\\
&= 3(33 - 14(2)) - 14\\
&= 3 \times 33 - 7 \times 14
\end{aligned}$$

$\therefore\ 115 = 345 \times 33 - 805 \times 14$

$\therefore\ x_0 = 345,\ y_0 = -805$ is one solution

$\therefore$ solutions are $x = x_0 + t(\frac{14}{1}),\ y = y_0 - t(\frac{33}{1})$

$\therefore\ x = 345 + 14t,\ y = -805 - 33t,\ t \in \mathbb{Z}.$

Check: $33(345 + 14t) + 14(-805 - 33t)$

$= 11\,385 + \cancel{462t} - 11\,270 - \cancel{462t}$

$= 115$ ✓

c $\gcd(14, 35) = 7$ and $7 \nmid 93$

$\therefore$ no integer solutions exist.

d $\gcd(72, 56) = 8$ and $8 \mid 40$

$\therefore$ integer solutions exist.

Now $72 = 56(1) + 16$

$56 = 16(3) + 8$

$16 = 8(2) + 0$

$$\begin{aligned}
\text{thus}\quad 8 &= 56 - 16(3)\\
&= 56 - (72 - 56) \times 3\\
&= -3 \times 72 + 4 \times 56
\end{aligned}$$

$\therefore\ 40 = -15 \times 72 + 20 \times 56$

$\therefore\ x_0 = -15,\ y_0 = 20$ is one solution

$\therefore$ solutions are $x = -15 + t(\frac{56}{8}),\quad y = 20 - t(\frac{72}{8})$

$\therefore\ x = -15 + 7t,\quad y = 20 - 9t,\ t \in \mathbb{Z}.$

Check: $72x + 56y$

$= 72(-15 + 7t) + 56(20 - 9t)$

$= -1080 + \cancel{504t} + 1120 - \cancel{504t}$

$= 40$ ✓

e $\gcd(138, 24) = 6$ and $6 \mid 18$

$\therefore$ integer solutions exist.

Now $138 = 24(5) + 18$

$24 = 18(1) + 6$

$18 = 6(3) + 0$

$$\begin{aligned}
\text{thus}\quad 6 &= 24 - 18\\
&= 24 - (138 - 24(5))\\
&= -1 \times 138 + 6 \times 24
\end{aligned}$$

$\therefore\ \ 18 = -3 \times 138 + 18 \times 24$

$\therefore\ \ x_0 = -3,\ y_0 = 18$ is one solution

$\therefore$ solutions are $x = -3 + t(\frac{24}{6}),\quad y = 18 - t(\frac{138}{6})$

$\therefore\ \ x = -3 + 4t, \qquad y = 18 - 23t,\ \ t \in \mathbb{Z}.$

f $\gcd(221, 35) = 1$ and $1 \mid 11$

$\therefore$ integer solutions exist.

Now $\quad 221 = 35(6) + 11$

$35 = 11(3) + 2$

$11 = 2(5) + 1$

$2 = 1(2) + 0$

$$\begin{aligned}\text{Thus}\quad 1 &= 11 - 2(5)\\ &= 11 - (35 - 11(3)) \times 5\\ &= -5 \times 35 + 16 \times 11\\ &= -5 \times 35 + 16(221 - 35(6))\\ &= 16 \times 221 - 101 \times 35\end{aligned}$$

$\therefore\ \ 11 = 176 \times 221 - 1111 \times 35$

$\therefore\ \ x_0 = 176,\ y_0 = -1111$ is one solution.

$\therefore$ solutions are

$x = 176 + t(\frac{35}{1}),\quad y = -1111 - t(\frac{221}{1})$

$\therefore\ \ x = 176 + 35t, \qquad y = -1111 - 221t,\ \ t \in \mathbb{Z}.$

2 **a** $18x + 5y = 48$

$\gcd(18, 5) = 1$ and $1 \mid 48$

$\therefore$ integer solutions exist.

Now $\quad 18 = 5(3) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$$\begin{aligned}\text{Thus}\quad 1 &= 3 - 2\\ &= 3 - (5 - 3)\\ &= -5 + 2 \times 3\\ &= -5 + 2(18 - 5(3))\\ &= 2 \times 18 - 7 \times 5\end{aligned}$$

$\therefore\ \ 48 = 96 \times 18 - 336 \times 5$

$\therefore\ \ x_0 = 96,\ y_0 = -336$ is one solution.

$\therefore$ solutions are $x = 96 + 5t,\ \ y = -336 - 18t,\ \ t \in \mathbb{Z}.$

For positive solutions we require

$96 + 5t > 0 \qquad$ *and* $\qquad -336 - 18t > 0$

$\therefore\ \ 5t > -96 \qquad$ *and* $\qquad 18t < -336$

$\therefore\ \ t > -19.2 \qquad$ *and* $\qquad t < -18.\overline{6}$

$\therefore\ \ t = -19$

where $\quad x = 96 + 5(-19) = 1$

and $\quad y = -336 - 18(-19) = 6$

$\therefore\ \ x = 1,\ \ y = 6$ is the only positive integer solution pair.

b $54x + 21y = 906$

$\gcd(54, 21) = 3$ and $3 \mid 906$

$\therefore$ integer solutions exist.

Now $\quad 54 = 21(2) + 12$

$21 = 12(1) + 9$

$12 = 9(1) + 3$

$9 = 3(3) + 0$

$$\begin{aligned}\text{Thus}\quad 3 &= 12 - 9\\ &= 12 - (21 - 12)\\ &= -21 + 2 \times 12\\ &= -21 + 2(54 - 21(2))\\ &= 2 \times 54 - 5 \times 21\end{aligned}$$

$\therefore\ \ 906 = 604 \times 54 - 1510 \times 21$

$\therefore\ \ x_0 = 604,\ \ y_0 = -1510$ is one solution.

$\therefore$ solutions are

$x = 604 + t(\frac{21}{3}),\quad y = -1510 - t(\frac{54}{3})$

$\therefore\ \ x = 604 + 7t, \qquad y = -1510 - 18t,\ \ t \in \mathbb{Z}.$

For positive solutions we require

$604 + 7t > 0 \qquad$ *and* $\qquad -1510 - 18t > 0$

$\therefore\ \ 7t > -604 \qquad$ *and* $\qquad 18t < -1510$

$\therefore\ \ t > -86.3 \qquad$ *and* $\qquad t < -83.9$

$\therefore\ \ t = -84,\ -85$, or -86

$\therefore$ positive integer solutions are:

x	2	9	16
y	38	20	2

c $123x + 360y = 99$

$\gcd(123, 360) = 3$ and $3 \mid 99$

$\therefore$ integer solutions exist.

Now $\quad 360 = 123(2) + 114$

$123 = 114(1) + 9$

$114 = 9(12) + 6$

$9 = 6(1) + 3$

$6 = 3(2) + 0$

$$\begin{aligned}\text{Thus}\quad 3 &= 9 - 6\\ &= 9 - (114 - 9(12))\\ &= -114 + 13 \times 9\\ &= -114 + 13(123 - 114)\\ &= 13 \times 123 - 14 \times 114\\ &= 13 \times 123 - 14(360 - 123(2))\\ &= 41 \times 123 - 14 \times 360\end{aligned}$$

$\therefore\ \ 99 = 1353 \times 123 - 462 \times 360$

$\therefore\ \ x_0 = 1353,\ \ y_0 = -462$ is one solution.

$\therefore$ solutions are

$x = 1353 + (\frac{360}{3})t,\quad y = -462 - (\frac{123}{3})t$

$\therefore\ \ x = 1353 + 120t, \qquad y = -462 - 41t,\ \ t \in \mathbb{Z}.$

For positive solutions we require

$1353 + 120t > 0 \qquad$ *and* $\qquad -462 - 41t > 0$

$\therefore\ \ 120t > -1353 \qquad$ *and* $\qquad 41t < -462$

$\therefore\ \ t > -11.275 \qquad$ *and* $\qquad t < -11.268$

$\therefore$ no integer t exists.

$\therefore\ \ 123x + 360y = 99$ has no positive integer solutions.

d $158x - 57y = 11$ or $158x + 57(-y) = 11$

$\gcd(158, 57) = 1$ and $1 \mid 11$

$\therefore$ integer solutions exist.

Now $\quad 158 = 57(2) + 44$

$57 = 44(1) + 13$

$44 = 13(3) + 5$

$13 = 5(2) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$$\begin{aligned}\text{Thus}\quad 1 &= 3 - 2\\ &= 3 - (5 - 3)\\ &= -5 + 2 \times 3\\ &= -5 + 2(13 - 5(2))\\ &= 2 \times 13 - 5 \times 5\\ &= 2 \times 13 - 5(44 - 13(3))\\ &= -5 \times 44 + 17 \times 13\\ &= -5 \times 44 + 17(57 - 44)\end{aligned}$$

$$\begin{aligned}&= 17 \times 57 - 22 \times 44\\&= 17 \times 57 - 22(158 - 57(2))\\&= -22 \times 158 + 61 \times 57\end{aligned}$$

$\therefore\ 11 = -242 \times 158 + 671 \times 57$

$\therefore\ x_0 = -242,\ -y_0 = 671$ is one solution.

$\therefore$ solutions are $x = -242 + (\frac{57}{1})t,\ \ -y = 671 - (\frac{158}{1})t$

$\therefore\ x = -242 + 57t, \qquad y = -671 + 158t$

For positive solutions we require

$-242 + 57t > 0$ *and* $-671 + 158t > 0$

$\therefore\ t > 4.245....$ *and* $t > 4.246....$

$\therefore\ t \geqslant 5$

Thus, there are infinitely many positive integer solutions. These are:

$x = -242 + 57t,\ \ y = -671 + 158t,\ \ t \geqslant 5,\ \ t \in \mathbb{Z}.$

3 $7 \mid a$ and $11 \mid b$

$\Rightarrow\ a = 7x$ and $b = 11y$ for $x, y \in \mathbb{Z}^+$

$\Rightarrow\ 7x + 11y = 100$ for $x, y \in \mathbb{Z}^+$

$\gcd(7, 11) = 1$ and $1 \mid 100$

$\therefore$ integer solutions exist.

Now
$$\begin{aligned}11 &= 7(1) + 4\\7 &= 4(1) + 3\\4 &= 3(1) + 1\\3 &= 1(3) + 0\end{aligned}$$

Thus
$$\begin{aligned}1 &= 4 - 3\\&= 4 - (7 - 4)\\&= -7 + 2 \times 4\\&= -7 + 2(11 - 7)\\&= 2 \times 11 - 3 \times 7\end{aligned}$$

$$\begin{aligned}\therefore\ 100 &= 200 \times 11 - 300 \times 7\\&= -300 \times 7 + 200 \times 11\end{aligned}$$

$\therefore\ x_0 = -300,\ y_0 = 200$ is one solution.

$\therefore$ solutions are $x = -300 + 11t,\ y = 200 - 7t,\ t \in \mathbb{Z}.$

For positive solutions we require

$-300 + 11t > 0$ *and* $200 - 7t > 0$

$\therefore\ 11t > 300$ *and* $7t < 200$

$\therefore\ t > 27.27$ *and* $t < 28.57$

$\therefore\ t = 28$

Hence, $x = 8,\ y = 4$

$\therefore$ the numbers are 56 and 44.

4 Let m = number of men

w = number of women

c = number of children

$\therefore\ m + w + c = 20$ {total number present}

and $5m + 4w + 2c = 62$

Thus $5m + 4w + 2(20 - m - w) = 62$

$\therefore\ 5m + 4w + 40 - 2m - 2w = 62$

$\therefore\ 3m + 2w = 22$

By inspection, one solution is $m_0 = 0,\ w_0 = 11.$

$\therefore\ m = 2t$ and $w = 11 - 3t,\ t \in \mathbb{Z}$ is the general solution.

$$\begin{aligned}\therefore\ c &= 20 - m - w\\&= 20 - 2t - 11 + 3t\\&= 9 + t,\ \ t \in \mathbb{Z}\end{aligned}$$

But $m > 0, \qquad w > 0, \qquad c > 0$

$\therefore\ 2t > 0, \qquad 11 - 3t > 0, \qquad 9 + t > 0$

$\therefore\ t > 0, \qquad t < 3\frac{2}{3}, \qquad t > -9$

$\therefore\ t = 1, 2,$ or 3

So, the possible solutions are:

m	2	4	6
w	8	5	2
c	10	11	12

Check: $5m + 4w + 2c$

$= 5(2) + 4(8) + 2(10) = 62$ ✓

or $5(4) + 4(5) + 2(11) = 62$ ✓

or $5(6) + 4(2) + 2(12) = 62$ ✓

5 Let c = number of cats bought

r = number of rabbits bought

f = number of fish bought

$\therefore\ c + r + f = 100$

and $50c + 10r + 0.5f = 1000$

$\therefore\ 50c + 10r + 0.5(100 - c - r) = 1000$

$\therefore\ 50c + 10r + 50 - \frac{1}{2}c - \frac{1}{2}r = 1000$

$\therefore\ 49\frac{1}{2}c + 9\frac{1}{2}r = 950$

$\therefore\ 99c + 19r = 1900$

By inspection, one solution is $c_0 = 0,\ r_0 = 100.$

$\therefore\ c = 19t,\ r = 100 - 99t,\ t \in \mathbb{Z}$ is the general solution.

$$\begin{aligned}\therefore\ f &= 100 - 19t - (100 - 99t)\\&= 80t,\ \ t \in \mathbb{Z}\end{aligned}$$

But $c \geqslant 1, \qquad r \geqslant 1, \qquad f \geqslant 1$

$\therefore\ 19t \geqslant 1, \qquad 100 - 99t \geqslant 1, \qquad 80t \geqslant 1$

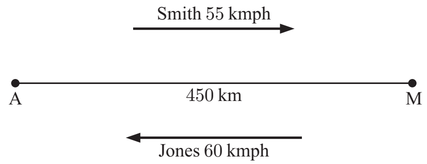
$\therefore\ t \geqslant \frac{1}{19}, \qquad t \leqslant 1, \qquad t \geqslant \frac{1}{80}$

$\therefore\ t = 1$

Thus $c = 19,\ r = 1,\ f = 80$

$\therefore$ I buy 19 cats, 1 rabbit, and 80 fish.

6



Let Smith travel for x hours and Jones for y hours; $x, y \in \mathbb{Z}^+$

$\therefore$ Smith travels $55x$ km, and Jones $60y$ km.

Thus $55x + 60y = 450$

$\therefore\ 11x + 12y = 90$

where $\gcd(11, 12) = 1$ and $1 \mid 90.$

$\therefore$ integer solutions exist.

Now $12 = 11(1) + 1$

$\therefore\ 1 = 12 - 11$

$\therefore\ 90 = 90 \times 12 - 90 \times 11$

$\therefore$ one solution is $x_0 = -90,\ y_0 = 90$

$\therefore$ solutions are $x = -90 + 12t,\ y = 90 - 11t,\ t \in \mathbb{Z}.$

For positive solutions,

$-90 + 12t > 0$ *and* $90 - 11t > 0$

$\therefore\ 12t > 90$ *and* $11t < 90$

$\therefore\ t > 7.5$ *and* $t < 8.18....$

$\therefore\ t = 8$

Thus $x = 6,\ y = 2$

$\therefore$ Smith travels for 6 hours, Jones for 2 hours

$\therefore$ they meet 330 km from A (or 120 km from B).

7 $x =$ number bought at \$3.50
$y =$ number bought at $\$4 \div 3$
$z =$ number bought at \$0.50

$\therefore\ x + y + z = 100$ and
$3\frac{1}{2}x + \frac{4}{3}y + \frac{1}{2}z = 100$

$\therefore\ x + y + z = 100$ and
$21x + 8y + 3z = 600$

$$\begin{array}{rl} \therefore & -3x - 3y - 3z = -300 \quad \text{and} \\ & \underline{21x + 8y + 3z = 600} \\ & 18x + 5y \qquad = 300 \end{array}$$

By inspection, one solution is $x_0 = 0,\ y_0 = 60$.
$\therefore\ x = 5t,\ \ y = 60 - 18t,\ \ t \in \mathbb{Z}$ is the general solution.
$\therefore\ z = 100 - 5t - (60 - 18t)$
$\qquad = 40 + 13t$

For positive solutions

$$\begin{array}{lllll} & 5t > 0 & \textit{and} \quad 60 - 18t > 0 & \textit{and} & 40 + 13t > 0 \\ \therefore & t > 0 & \textit{and} \qquad 18t < 60 & \textit{and} & 13t > -40 \\ \therefore & t > 0 & \textit{and} \qquad\ \ t < 3\frac{1}{3} & \textit{and} & t > -3.08 \\ \therefore & t = 1,\ 2, \text{ or } 3 & & & \end{array}$$

So the possible solutions are:

x	5	10	15
y	42	24	6
z	53	66	79

EXERCISE 1E

1 **a** $143 = 13 \times 11$ and so 143 is not a prime.
b $221 = 13 \times 17$ and so 221 is not a prime.
c 199 is a prime as 2, 3, 5, 7, 11, and 13 are not factors of 199.
$\{\sqrt{199} \approx 14.1,$ so we need only check for divisibility by primes less than $14.1\}$
d 223 is a prime as $\sqrt{223} \approx 14.9$ and 2, 3, 5, 7, 11, and 13 are not factors of 223.

2 Any even number greater than 2 is composite, as it has a factor other than itself and 1 (namely, 2).
So, 2 is the only even prime.

3 **a** 11 is prime.
b $111 = 3 \times 37$ is not prime.
c $1111 = 11 \times 101$ is not prime.
d $11\,111 = 41 \times 271$ is not prime.

4 If $p \mid q$ then $q = kp$ for some $k \in \mathbb{Z}$.
If $k \neq 1$, q is composite, a contradiction to q being a prime.
Thus $k = 1$
$\therefore\ p = q$

5 **a** **i** Suppose the powers in the factorisation of n are even
$\Leftrightarrow\ n = {p_1}^{2a_1}{p_2}^{2a_2}{p_3}^{2a_3}\ldots.{p_k}^{2a_k}$
$\Leftrightarrow\ n = \left({p_1}^{a_1}{p_2}^{a_2}{p_3}^{a_3}\ldots.{p_k}^{a_k}\right)^2$
$\Leftrightarrow\ n$ is a square number.

ii The power of a prime, p^n has $n+1$ factors.
These are $1,\ p,\ p^2,\ p^3,\ \ldots.,\ p^n$
$\therefore$ by the product principle of counting
$n = {p_1}^{n_1}{p_2}^{n_2}{p_3}^{n_3}\ldots.{p_k}^{n_k}$ has
$(n_1+1)(n_2+1)(n_3+1)\ldots.(n_k+1)$ factors.
The number of factors of n is odd
$\Leftrightarrow$ all of the $(n_i + 1)$s are odd
$\Leftrightarrow$ all of the n_is are even
$\Leftrightarrow$ n is a square. $\{$by **i**$\}$

b Suppose $\sqrt{2}$ is rational
$\therefore\ \sqrt{2} = \dfrac{p}{q}$ where $\gcd(p,\ q) = 1,\ q \neq 0$
$\therefore\ p^2 = 2q^2$
a contradiction as the number of factors of p^2 is odd and the number of factors of $2q^2$ is even. $\{$from **a ii**$\}$

6 **a** $1 + a + a^2 + a^3 + \ldots. + a^{n-1} = \dfrac{1(a^n - 1)}{a - 1},\ \ a \neq 1$
$\{$sum of a GS$\}$
$\therefore\ a^n - 1 = (a-1)(1 + a + a^2 + a^3 + \ldots. + a^{n-1})$
Thus if $a^n - 1$ is prime, $a - 1 = 1$
$\{$otherwise it has two factors other than itself and 1$\}$
$\therefore\ a = 2$

b No, as for example, $2^4 - 1$
$= 15$
$= 3 \times 5$

c No, as for example, $2^3 - 1$
$= 7$ which is not composite.

d No, as for example, $2^{11} - 1$
$= 2047$
$= 23 \times 89$

7 **a**
$$\begin{array}{r|r} 5 & 9555 \\ \hline 3 & 1911 \\ \hline 7 & 637 \\ \hline 7 & 91 \\ \hline & 13 \end{array}$$
$\therefore\ 9555 = 3 \times 5 \times 7^2 \times 13$

b
$$\begin{array}{r|r} 23 & 989 \\ \hline & 43 \end{array}$$
$\therefore\ 989 = 23 \times 43$

c
$$\begin{array}{r|r} 3 & 9999 \\ \hline 3 & 3333 \\ \hline 11 & 1111 \\ \hline & 101 \end{array}$$
$\therefore\ 9999 = 3^2 \times 11 \times 101$

d
$$\begin{array}{r|r} 3 & 111\,111 \\ \hline 37 & 37\,037 \\ \hline 11 & 1001 \\ \hline 7 & 91 \\ \hline & 13 \end{array}$$
$\therefore\ 111\,111 = 3 \times 7 \times 11 \times 13 \times 37$

8 **a** The product of two equal primes, p^2 has exactly 3 divisors, $1,\ p$, and p^2.
b The product of two distinct primes, pq has exactly 4 divisors, $1,\ p,\ q$, and pq.

9 **a** The primes which divide 50! are the primes in the list $1, 2, 3, 4, \ldots., 49, 50$.
These are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47.

b An end zero results when we have a product 2×5. There is an abundance of factors of 2, so we need only count the factors of 5 in 50!

$$\underbrace{5,\ 10,\ 15,\ 20,}_{\text{1 each}}\ \ \underbrace{25,}_{2}\ \ \underbrace{30,\ 35,\ 40,\ 45,}_{\text{1 each}}\ \ \underbrace{50}_{2}$$

$\therefore\ 4 + 2 + 4 + 2 = 12$
$\therefore$ 50! ends in 12 zeros.

c In 1 to 25 there are 6 factors of 5
In 26 to 50 there are 6
In 51 to 75 there are 6
In 76 to 100 there are 6
In 101 to 125 there are 7 {125 has 3 factors of 5}
31
In 126 to 250 there are 31
62
In 251 to 300 there are 12
74

∴ we have 74 ending zeros for 300!, 301!, 302!, 303!, 304!

10 **a** By the Fundamental Theorem of Arithmetic,

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots . p_k^{a_k}$$

$$\therefore \; a^n = p_1^{na_1} p_2^{na_2} p_3^{na_3} \ldots . p_k^{na_k}$$

So, if $p \mid a^n$, then p is one of the p_i $(i = 1, 2, 3, \ldots., k)$

$\Rightarrow$ $p^n \mid a^n$

b $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots . p_k^{a_k}$

{Fundamental Theorem of Arithmetic}

$$\therefore \; a^2 = p_1^{2a_1} p_2^{2a_2} p_3^{2a_3} \ldots . p_k^{2a_k}$$

So, if $p \mid a^2$, then p is one of the p_i

$\Rightarrow$ $p \mid a$

c $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots . p_k^{a_k}$

$$\therefore \; a^n = p_1^{na_1} p_2^{na_2} p_3^{na_3} \ldots . p_k^{na_k}$$

So, if $p \mid a^n$, then p is one of the p_i

$\Rightarrow$ $p \mid a$

11 **a** All integers have form $4n$, $4n+1$, $4n+2$, or $4n+3$ where $4n$ and $4n+2$ are composites (they are even).

∴ all odd primes must have form $4n+1$ or $4n+3$.

b Suppose there are a finite number of primes of the form $4n+3$ and these are p_1, p_2, p_3, p_4, ..., p_k where $p_1 < p_2 < p_3 < p_4 < \ldots. < p_k$.

Now consider $N = 4(p_1 p_2 p_3 \ldots . p_k) + 3$ which is of the form $4n+3$.

If N is a prime number, then p_k is not the largest prime of the form $4n+3$.

If N is composite, then it must contain prime factors of the form $4n+1$ or $4n+3$.

But N cannot contain only prime factors of the form $4n+1$ since the product of such numbers is not of the form $4n+3$.

This is shown by:

$$\begin{aligned} &(4n_1+1)(4n_2+1) \\ &= 16n_1n_2 + 4n_1 + 4n_2 + 1 \\ &= 4(4n_1n_2 + n_1n_2) + 1. \end{aligned}$$

Hence, N must contain a prime factor of the form $4n+3$.

Since p_1, p_2, p_3, ..., p_k are not factors of N, there exists another prime factor of the form $4n+3$.

This is a contradiction.

So, there are infinitely many primes of the form $4n+3$.

12 **a** If $n = 1$, $2^{2^1} + 1 = 5$, a prime.

If $n = 2$, $2^{2^2} + 1 = 2^4 + 1 = 17$, a prime.

If $n = 3$, $2^{2^3} + 1 = 2^8 + 1 = 257$, a prime.

If $n = 4$, $2^{2^4} + 1 = 2^{16} + 1 = 65\,537$, a prime.

b If $n = 5$,
$$\begin{aligned} 2^{2^5} + 1 &= 4\,294\,967\,297 \\ &= 641 \times 6\,700\,417 \end{aligned}$$

{using a prime factors calculator via the internet}

∴ Fermat's conjecture was incorrect.

EXERCISE 1F.1

1 a, b are congruent (mod 7) $\Leftrightarrow$ $a \equiv b \pmod 7$
$\Leftrightarrow$ $7 \mid a - b$

a $15 - 1 = 14$ and $7 \mid 14$

∴ 1, 15 are congruent (mod 7)

b $8 - {-1} = 9$ and $7 \nmid 9$

∴ -1, 8 are *not* congruent (mod 7)

c $99 - 2 = 97$ and $7 \nmid 97$

∴ 2, 99 are *not* congruent (mod 7)

d $699 - {-1} = 700$ and $7 \mid 700$

∴ -1, 699 are congruent (mod 7)

2 **a** $29 - 7 = 22$ and 22 has factors 1, 2, 11, 22.

∴ $m = 1, 2, 11, 22$.

b $100 - 1 = 99$ and 99 has factors 1, 3, 9, 11, 33, 99.

∴ $m = 1, 3, 9, 11, 33, 99$.

c $53 - 0 = 53$ which is a prime with factors 1, 53.

∴ $m = 1, 53$.

d $61 - 1 = 60$ which has factors 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

∴ $m = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

3 **a**
$$\begin{aligned} 2^{28} &= (2^3)^9 \times 2 \\ &\equiv 1 \times 2 \pmod 7 \qquad \{2^3 = 8 \equiv 1\} \\ &\equiv 2 \pmod 7 \end{aligned}$$

b
$$\begin{aligned} 10 &\equiv 3 \pmod 7 \qquad \{10 - 3 = 7 = 1 \times 7\} \\ \therefore\; 10^{33} &\equiv 3^{33} \pmod 7 \\ &\equiv (3^3)^{11} \pmod 7 \\ &\equiv (-1)^{11} \pmod 7 \qquad \{3^3 = 27 \equiv -1\} \\ &\equiv -1 \pmod 7 \\ &\equiv 6 \pmod 7 \end{aligned}$$

c
$$\begin{aligned} 3^{50} &= (3^3)^{16} 3^2 \\ &\equiv (-1)^{16} \times 2 \pmod 7 \qquad \{3^3 = 27 \equiv -1\} \\ &\equiv 2 \pmod 7 \end{aligned}$$

d
$$\begin{aligned} 41 &\equiv -1 \pmod 7 \qquad \{41 - {-1} = 42 = 6 \times 7\} \\ \therefore\; 41^{23} &\equiv (-1)^{23} \pmod 7 \\ &\equiv -1 \pmod 7 \\ &\equiv 6 \pmod 7 \end{aligned}$$

4 **a**
$$\begin{aligned} 2^{28} &= (2^5)^5 \times 2^3 \\ &\equiv (-5)^5 \times 8 \pmod{37} \qquad \{2^5 = 32 \equiv -5\} \\ &\equiv (-5)^2 \times (-5)^2 \times (-5) \times 8 \pmod{37} \\ &\equiv -12 \times -12 \times -40 \pmod{37} \\ &\qquad \{(-5)^2 = 25 \equiv -12\} \\ &\equiv -12 \times -12 \times -3 \pmod{37} \\ &\equiv -12 \times 36 \pmod{37} \\ &\equiv -12 \times -1 \pmod{37} \\ &\equiv 12 \pmod{37} \end{aligned}$$

b
$$\begin{aligned} 3^{65} &= (3^3)^{21} \times 3^2 \\ &\equiv 1^{21} \times 9 \pmod{13} \qquad \{3^3 = 27 \equiv 1\} \\ &\equiv 9 \pmod{13} \end{aligned}$$

c
$$\begin{aligned} 7^{44} &= (7^2)^{22} \\ &\equiv 5^{22} \pmod{11} \qquad \{7^2 = 49 \equiv 5\} \\ &\equiv (5^2)^{11} \pmod{11} \\ &\equiv 3^{11} \pmod{11} \qquad \{5^2 = 25 \equiv 3\} \\ &\equiv (3^2)^5 \times 3 \pmod{11} \end{aligned}$$

$$\begin{aligned}
&\equiv (-2)^5 \times 3 \pmod{11} \quad \{3^2 = 9 \equiv -2\}\\
&\equiv -32 \times 3 \pmod{11}\\
&\equiv 1 \times 3 \pmod{11}\\
&\equiv 3 \pmod{11}
\end{aligned}$$

5 **a** $53 \equiv 14 \pmod{39}$ and $103 \equiv -14 \pmod{39}$

$$\begin{aligned}
\therefore \quad & 53^{103} + 103^{53} \pmod{39}\\
&\equiv 14^{103} + (-14)^{53} \pmod{39}\\
&\equiv 14^{103} - 14^{53} \pmod{39}\\
&\equiv 14^{53}(14^{50} - 1) \pmod{39}\\
&\equiv 14^{53}[(14^2)^{25} - 1] \pmod{39}\\
&\equiv 14^{53}[1^{25} - 1] \pmod{39} \qquad \{14^2 = 196 \equiv 1\}\\
&\equiv 0 \pmod{39}
\end{aligned}$$

Thus $53^{103} + 103^{53}$ is divisible by 39.

b $333 \equiv 4 \pmod 7$ and $111 \equiv -1 \pmod 7$

$$\begin{aligned}
\therefore \quad & 333^{111} + 111^{333} \pmod 7\\
&\equiv 4^{111} + (-1)^{333} \pmod 7\\
&\equiv [(4^2)^{55} \times 4 - 1] \pmod 7\\
&\equiv [2^{55} \times 2^2 - 1] \pmod 7 \qquad \{4^2 = 16 \equiv 2\}\\
&\equiv [2^{57} - 1] \pmod 7\\
&\equiv [(2^3)^{19} - 1] \pmod 7\\
&\equiv [1^{19} - 1] \pmod 7 \qquad \{2^3 = 8 \equiv 1\}\\
&\equiv 0 \pmod 7
\end{aligned}$$

$\therefore$ $333^{111} - 111^{333}$ is divisible by 7.

6

$$\begin{aligned}
& 2^{100} + 3^{100}\\
&= (2^2)^{50} + (3^4)^{25}\\
&\equiv (-1)^{50} + 1^{25} \pmod 5 \qquad \{2^2 = 4 \equiv -1;\ 3^4 = 81 \equiv 1\}\\
&\equiv 1 + 1 \pmod 5\\
&\equiv 2 \pmod 5
\end{aligned}$$

$\therefore$ the remainder when $2^{100} + 3^{100}$ is divided by 5 is 2.

7 $203 \equiv 3 \pmod{100}$

$$\begin{aligned}
\therefore \quad 203^{20} &\equiv 3^{20} \pmod{100}\\
&\equiv (3^4)^5 \pmod{100}\\
&\equiv (-19)^5 \pmod{100} \qquad \{3^4 = 81 \equiv -19\}\\
&\equiv 361 \times 361 \times -19 \pmod{100}\\
&\equiv -39 \times -39 \times -19 \pmod{100}\\
&\equiv 1521 \times -19 \pmod{100}\\
&\equiv 21 \times -19 \pmod{100}\\
&\equiv -399 \pmod{100}\\
&\equiv 1 \pmod{100}
\end{aligned}$$

$\therefore$ last two digits are 01.

8 **a** $5! = 120 \equiv 0 \pmod{20}$

$\therefore$ $k! \equiv 0 \pmod{20}$ for all $k \geqslant 5$

$$\begin{aligned}
\therefore \quad \sum_{k=1}^{50} k! \pmod{20} &\equiv (1! + 2! + 3! + 4!) \pmod{20}\\
&\equiv 1 + 2 + 6 + 24 \pmod{20}\\
&\equiv 33 \pmod{20}\\
&\equiv 13 \pmod{20}
\end{aligned}$$

b $7! = 5040 \equiv 0 \pmod{42}$

$\therefore$ $k! \equiv 0 \pmod{42}$ for all $k \geqslant 7$

$$\begin{aligned}
\therefore \quad & \sum_{k=1}^{50} k! \pmod{42}\\
&\equiv (1! + 2! + 3! + 4! + 5! + 6!) \pmod{42}\\
&\equiv 873 \pmod{42}\\
&\equiv 33 \pmod{42}
\end{aligned}$$

c 4×3 is contained in 10!

$\therefore$ $10! \equiv 0 \pmod{12}$

$\therefore$ $k! \equiv 0 \pmod{12}$ for all $k \geqslant 10$

$\therefore$ $\displaystyle\sum_{k=10}^{100} k! \pmod{12} \equiv 0 \pmod{12}$

d 2×5 is contained in 5!

$\therefore$ $5! \equiv 0 \pmod{10}$

$\therefore$ $k! \equiv 0 \pmod{10}$ for all $k \geqslant 5$.

$$\begin{aligned}
\text{Now} \quad \sum_{k=4}^{30} k! &= 4! + \sum_{k=5}^{30} k!\\
&\equiv 24 + 0 \pmod{10}\\
&\equiv 4 \pmod{10}
\end{aligned}$$

9 **a** **i**

$$\begin{aligned}
& 5^{10} \pmod{11}\\
&\equiv 25^5 \pmod{11}\\
&\equiv 3^5 \pmod{11}\\
&\equiv 1 \pmod{11}
\end{aligned}$$

ii

$$\begin{aligned}
& 3^{12} \pmod{13}\\
&\equiv (3^3)^4 \pmod{13}\\
&\equiv 27^4 \pmod{13}\\
&\equiv 1^4 \pmod{13}\\
&\equiv 1 \pmod{13}
\end{aligned}$$

iii

$$\begin{aligned}
& 2^{18} \pmod{19}\\
&\equiv (2^4)^4 2^2 \pmod{19}\\
&\equiv 16^4 \times 4 \pmod{19}\\
&\equiv (-3)^4 \times 4 \pmod{19}\\
&\equiv 81 \times 4 \pmod{19}\\
&\equiv 5 \times 4 \pmod{19}\\
&\equiv 1 \pmod{19}
\end{aligned}$$

iv

$$\begin{aligned}
& 7^{16} \pmod{17}\\
&\equiv (7^2)^8 \pmod{17}\\
&\equiv 49^8 \pmod{17}\\
&\equiv (-2)^8 \pmod{17}\\
&\equiv 2^8 \pmod{17}\\
&\equiv (2^4)^2 \pmod{17}\\
&\equiv 16^2 \pmod{17}\\
&\equiv (-1)^2 \pmod{17}\\
&\equiv 1 \pmod{17}
\end{aligned}$$

b *Conjecture*: (from **a**)

For $a \in \mathbb{Z}$, $a^{n-1} \equiv 1 \pmod n$. n may have to be prime.

c **i**

$$\begin{aligned}
& 4^{11} \pmod{12}\\
&\equiv (4^3)^3 \times 4^2 \pmod{12}\\
&\equiv 64^3 \times 16 \pmod{12}\\
&\equiv 4^3 \times 4 \pmod{12}\\
&\equiv 4 \times 4 \pmod{12}\\
&\equiv 16 \pmod{12}\\
&\equiv 4 \pmod{12}
\end{aligned}$$

ii

$$\begin{aligned}
& 5^8 \pmod 9\\
&\equiv (5^2)^4 \pmod 9\\
&\equiv (-2)^4 \pmod 9\\
&\equiv 16 \pmod 9\\
&\equiv 7 \pmod 9
\end{aligned}$$

iii

$$\begin{aligned}
& 33^{10} \pmod{11}\\
&\equiv 0^{10} \pmod{11}\\
&\equiv 0 \pmod{11}
\end{aligned}$$

iv

$$\begin{aligned}
& 34^{16} \pmod{17}\\
&\equiv 0^{16} \pmod{17}\\
&\equiv 0 \pmod{17}
\end{aligned}$$

d *New conjecture*: based on **c** examples.

For $a \in \mathbb{Z}$, and p a prime, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$.

10 **a** **i**

$$\begin{aligned}
& 2! \pmod 3\\
&\equiv 2 \pmod 3
\end{aligned}$$

ii

$$\begin{aligned}
& 4! \pmod 5\\
&\equiv 24 \pmod 5\\
&\equiv 4 \pmod 5
\end{aligned}$$

iii
$$\begin{aligned}
&10!\ (\text{mod}\ 11)\\
&\equiv 10\times 9\times 8\times 7\times 6\times 5\times 4\times 3\times 2\times 1\ (\text{mod}\ 11)\\
&\equiv 90\times 56\times 30\times 24\ (\text{mod}\ 11)\\
&\equiv 2\times 1\times 8\times 2\ (\text{mod}\ 11)\\
&\equiv 32\ (\text{mod}\ 11)\\
&\equiv 10\ (\text{mod}\ 11)
\end{aligned}$$

iv
$$\begin{aligned}
&6!\ (\text{mod}\ 7)\\
&\equiv 6\times 5\times 4\times 3\times 2\times 1\ (\text{mod}\ 7)\\
&\equiv 30\times 24\ (\text{mod}\ 7)\\
&\equiv 2\times 3\ (\text{mod}\ 7)\\
&\equiv 6\ (\text{mod}\ 7)
\end{aligned}$$

b *Conjecture*:
$$(n-1)!\equiv n-1\ (\text{mod}\ n),\quad n\in\mathbb{Z}^+,\quad n\geqslant 2.$$

c **i**
$$\begin{aligned}
&3!\ (\text{mod}\ 4)\\
&\equiv 6\ (\text{mod}\ 4)\\
&\equiv 2\ (\text{mod}\ 4)\\
&\not\equiv 3\ (\text{mod}\ 4)
\end{aligned}$$

ii
$$\begin{aligned}
&5!\ (\text{mod}\ 6)\\
&\equiv 120\ (\text{mod}\ 6)\\
&\equiv 0\ (\text{mod}\ 6)\\
&\not\equiv 5\ (\text{mod}\ 6)
\end{aligned}$$

d From **c** we make a *new conjecture*:
$$(p-1)!\equiv p-1\ (\text{mod}\ p)\quad\text{for any prime } p.$$

11 **a**
$$\begin{aligned}
&5^{2n}+3\times 2^{5n-2}\ (\text{mod}\ 7)\\
&\equiv 25^n+3\times 32^n\times 2^{-2}\ (\text{mod}\ 7)\\
&\equiv 4^n+\tfrac{3}{4}(4^n)\ (\text{mod}\ 7)\qquad \{25\equiv 4;\ \ 32\equiv 4\}\\
&\equiv 4^n+3(4^{n-1})\ (\text{mod}\ 7)\\
&\equiv 4^{n-1}(4+3)\ (\text{mod}\ 7)\\
&\equiv 4^{n-1}(0)\ (\text{mod}\ 7)\\
&\equiv 0\ (\text{mod}\ 7)
\end{aligned}$$
$\therefore\ \ 5^{2n}+3\times 2^{5n-2}$ is divisible by 7 for all $n\in\mathbb{Z}^+$.

b
$$\begin{aligned}
&3^{n+2}+4^{2n+1}\ (\text{mod}\ 13)\\
&\equiv 3^{n+2}+16^n\times 4\ (\text{mod}\ 13)\\
&\equiv 3^{n+2}+3^n\times 4\ (\text{mod}\ 13)\\
&\equiv 3^n(3^2+4)\ (\text{mod}\ 13)\\
&\equiv 3^n(13)\ (\text{mod}\ 13)\\
&\equiv 3^n(0)\ (\text{mod}\ 13)\\
&\equiv 0\ (\text{mod}\ 13)
\end{aligned}$$
$\therefore\ \ 3^{n+2}+4^{2n+1}$ is divisible by 13 for all $n\in\mathbb{Z}^+$.

c
$$\begin{aligned}
&5^{n+2}+2^{5n+1}\ (\text{mod}\ 27)\\
&\equiv 5^{n+2}+32^n\times 2\ (\text{mod}\ 27)\\
&\equiv 5^{n+2}+5^n\times 2\ (\text{mod}\ 27)\\
&\equiv 5^n(5^2+2)\ (\text{mod}\ 27)\\
&\equiv 5^n\times 27\ (\text{mod}\ 27)\\
&\equiv 5^n(0)\ (\text{mod}\ 27)\\
&\equiv 0\ (\text{mod}\ 27)
\end{aligned}$$
$\therefore\ \ 5^{n+2}+2^{5n+1}$ is divisible by 27 for all $n\in\mathbb{Z}^+$.

12 Consider
$$N=a_n10^n+a_{n-1}10^{n-1}+....+a_2 10^2+a_1 10+a_0$$
Now $10\equiv 1\ (\text{mod}\ 3)$

$\therefore\ \ 10^n\equiv 1\ (\text{mod}\ 3)$ for all $n\in\mathbb{Z}^+$

$\therefore\ \ N\equiv a_n+a_{n-1}+....+a_2+a_1+a_0\ (\text{mod}\ 3)$

$\therefore\ \ N$ is divisible by 3

$\Leftrightarrow a_n+a_{n-1}+....+a_2+a_1+a_0$ is divisible by 3.

13 **a** Any even integer n leaves a remainder of 0 or 2 when divided by 4

$\therefore\ \ n\equiv 0\ (\text{mod}\ 4)$ or $2\ (\text{mod}\ 4)$

$\therefore\ \ n^2\equiv 0\ (\text{mod}\ 4)$ or $4\ (\text{mod}\ 4)=0\ (\text{mod}\ 4)$

Thus $n^2\equiv 0\ (\text{mod}\ 4)$.

b Any odd integer leaves a remainder of 1 or 3 when divided by 4

$\therefore\ \ n\equiv 1\ (\text{mod}\ 4)$ or $3\ (\text{mod}\ 4)$

$\therefore\ \ n^2\equiv 1\ (\text{mod}\ 4)$ or $9\ (\text{mod}\ 4)=1\ (\text{mod}\ 4)$

$\therefore\ \ n^2\equiv 1\ (\text{mod}\ 4)$

c Any integer leaves a remainder of 0, 1, or 2 when divided by 3

$\therefore\ \ n\equiv 0,\ 1,\ \text{or}\ 2\ (\text{mod}\ 3)$

$\therefore\ \ n^2\equiv 0,\ 1,\ \text{or}\ 4\ (\text{mod}\ 3)$

$\therefore\ \ n^2\equiv 0\ \text{or}\ 1\ (\text{mod}\ 3)$

d Any integer leaves a remainder of 0, 1, 2, 3, 4, 5, 6, 7, or 8 when divided by 9

$\therefore\ \ n\equiv 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ \text{or}\ 8\ (\text{mod}\ 9)$

$\therefore\ \ n^3\equiv 0,\ 1,\ 8,\ 0,\ 1,\ 8,\ 0,\ 1,\ \text{or}\ 8\ (\text{mod}\ 9)$

$\therefore\ \ n^3\equiv 0,\ 1,\ \text{or}\ 8\ (\text{mod}\ 9)$

14 **a** Any odd integer has form $n=2k+1$ where $k\in\mathbb{Z}$.

$\Rightarrow\ \ n^2=4k^2+4k+1$

$\Rightarrow\ \ n^2=4k(k+1)+1$

$\Rightarrow\ \ n^2=4(2A)+1,\ \ A\in\mathbb{Z}$ as $k(k+1)$ is even

$\{k,\ \ k+1$ are consecutive integers, one of which is even$\}$

$\Rightarrow\ \ n^2=8A+1$

$\Rightarrow\ \ n^2\equiv 1\ (\text{mod}\ 8)$

b If n is an even integer then $n=2k$ where $k\in\mathbb{Z}$.

$\Rightarrow\ \ n^2=4k^2$ where k could be even or odd

$\Rightarrow\ \ n^2=4(2a)^2$ or $4(2a+1)^2$

$\Rightarrow\ \ n^2=4(4a^2)$ or $4(4a^2+4a+1)$

$\Rightarrow\ \ n^2=8(2a^2)$ or $16a^2+16a+4$

$\Rightarrow\ \ n^2\equiv 0\ \text{or}\ 4\ (\text{mod}\ 8)$

Thus, the square of any even integer is congruent to either 0 or 4 (mod 8).

15 $a,\ b,\ c\in\mathbb{Z}^+$ such that $a\equiv b\ (\text{mod}\ c)$

$\therefore\ \ a-b=kc$ for some integer k

$\Rightarrow\ \ a=b+kc$

$$\begin{aligned}
\text{Now}\quad &\gcd(a,\ c)\\
&=\gcd(b+kc,\ c)\\
&=\gcd(b,\ c)\qquad\{\text{linearity property of }\gcd\}
\end{aligned}$$

16 **a** **i** $x^2\equiv 1\ (\text{mod}\ 3)$

Now $x\equiv 0,\ 1,\ 2\ (\text{mod}\ 3)$

$\Rightarrow\ \ x^2\equiv 0,\ 1,\ 1\ (\text{mod}\ 3)$

$\therefore\ \ $ if $x^2\equiv 1\ (\text{mod}\ 3)$ then $x\equiv 1\ \text{or}\ 2\ (\text{mod}\ 3)$

or
$$\begin{aligned}
&x^2\equiv 1\ (\text{mod}\ 3)\\
\Leftrightarrow\ \ &x^2-1\equiv 0\ (\text{mod}\ 3)\\
\Leftrightarrow\ \ &(x+1)(x-1)\equiv 0\ (\text{mod}\ 3)\\
\Leftrightarrow\ \ &x\equiv -1\ \text{or}\ 1\ (\text{mod}\ 3)\\
\Leftrightarrow\ \ &x\equiv 2\ \text{or}\ 1\ (\text{mod}\ 3)
\end{aligned}$$

ii
$$\begin{aligned}
&x^2\equiv 4\ (\text{mod}\ 7)\\
\Leftrightarrow\ \ &x^2-4\equiv 0\ (\text{mod}\ 7)\\
\Leftrightarrow\ \ &(x+2)(x-2)\equiv 0\ (\text{mod}\ 7)\\
\Leftrightarrow\ \ &x\equiv -2\ \text{or}\ 2\ (\text{mod}\ 7)\\
\Leftrightarrow\ \ &x\equiv 5\ \text{or}\ 2\ (\text{mod}\ 7)
\end{aligned}$$

b
$$\begin{aligned}
& x^2 \equiv a^2 \pmod p \\
\Leftrightarrow\ & x^2 - a^2 \equiv 0 \pmod p \\
\Leftrightarrow\ & (x+a)(x-a) \equiv 0 \pmod p \\
\Leftrightarrow\ & x \equiv -a \text{ or } a \pmod p \\
\Leftrightarrow\ & x \equiv \pm a \pmod p
\end{aligned}$$

17 **a**
$$\begin{aligned}
\sum_{k=1}^{n} k &= 1+2+3+4+ \dots + n \\
&= \frac{n(n+1)}{2} \quad \text{where } \frac{n+1}{2} \in \mathbb{Z} \text{ as } n \text{ is odd}
\end{aligned}$$
$$\therefore \sum_{k=1}^{n} k \equiv 0 \pmod n$$

b If n is even,

for $n = 2$, $\sum_{k=1}^{2} k = 1+2 = 3 \equiv 1 \pmod 2$

for $n = 4$, $\sum_{k=1}^{4} k = 1+2+3+4 = 10 \equiv 2 \pmod 4$

for $n = 6$, $\sum_{k=1}^{6} k = 1+2+3+4+5+6 = 21 \equiv 3 \pmod 6$

These results suggest that

$$\text{for } n \text{ even, } \sum_{k=1}^{n} k = \frac{n}{2} \pmod n$$

Proof:

As $1+2+3+4+ \dots + n = \frac{n}{2}(n+1)$ then in $\bmod n$, $n+1 \equiv 1$

$$\therefore \sum_{k=1}^{n} k \equiv \frac{n}{2} \pmod n.$$

18
$$\begin{aligned}
\sum_{k=1}^{n-1} k^3 &= \left[\frac{(n-1)n}{2}\right]^2 \qquad \{\text{using the hint}\} \\
&= \frac{(n-1)^2 n^2}{4}
\end{aligned}$$

Now consider $n = 4m + r$ where $r = 0, 1, 2, 3$.

If $r = 0$, $n = 4m$ and $\frac{(n-1)^2 n^2}{4} = 4m^2(4m-1)^2$ which is divisible by $n = 4m$.

If $r = 1$, $n = 4m+1$ and $\frac{(n-1)^2 n^2}{4} = 4m^2(4m+1)^2$ which is divisible by $n = 4m+1$.

If $r = 2$, $n = 4m+2$ and
$$\begin{aligned}
\frac{(n-1)^2 n^2}{4} &= \frac{(4m+1)^2(4m+2)^2}{4} \\
&= (4m+1)^2(2m+1)^2
\end{aligned}$$
which is *not divisible* by $n = 4m+2$.

If $r = 3$, $n = 4m+3$ and
$$\begin{aligned}
\frac{(n-1)^2 n^2}{4} &= \frac{(4m+2)^2(4m+3)^2}{4} \\
&= (2m+1)^2(4m+3)^2
\end{aligned}$$
which is divisible by $n = 4m+3$.

$$\therefore \sum_{k=1}^{n-1} k^3 \equiv 0 \pmod n \quad \text{for } n \equiv 0, 1, \text{ or } 3 \pmod 4.$$

19
$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad \{\text{well known formula}\}$$

$$\begin{aligned}
\therefore \sum_{k=1}^{n} k^2 = 0 \pmod n \ &\Leftrightarrow\ \frac{(n+1)(2n+1)}{6} \in \mathbb{Z} \\
&\Leftrightarrow\ 6 \mid (n+1)(2n+1) \\
&\Leftrightarrow\ (n+1)(2n+1) \equiv 0 \pmod 6
\end{aligned}$$

Now $n \equiv 0, 1, 2, 3, 4, \text{ or } 5 \pmod 6$.

If $n = 0$, $(n+1)(2n+1) \equiv 1 \pmod 6$

If $n = 1$, $(n+1)(2n+1) = 6 \equiv 0 \pmod 6$ ✓

If $n = 2$, $(n+1)(2n+1) = 15 \equiv 3 \pmod 6$

If $n = 3$, $(n+1)(2n+1) = 28 \equiv 4 \pmod 6$

If $n = 4$, $(n+1)(2n+1) = 45 \equiv 3 \pmod 6$

If $n = 5$, $(n+1)(2n+1) = 66 \equiv 0 \pmod 6$ ✓

$$\therefore \sum_{k=1}^{n} k^2 \equiv 0 \pmod n \ \Leftrightarrow\ n \equiv 1 \text{ or } 5 \pmod 6.$$

20 **a** **i** **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$3^n \equiv 1 + 2n \pmod 4$"

(1) If $n = 1$, $3^1 \equiv 1 + 2 \pmod 4$ is true.

$\therefore$ P_1 is true.

(2) If P_k is true, then $3^k \equiv 1 + 2k \pmod 4$

$$\begin{aligned}
\therefore\ 3^{k+1} &= 3 \times 3^k \\
&\equiv 3(1+2k) \pmod 4 \\
&\equiv 3 + 6k \pmod 4 \\
&\equiv 3 + 2k \pmod 4 \\
&\equiv 1 + 2[k+1] \pmod 4
\end{aligned}$$

$\therefore$ P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true, $n \in \mathbb{Z}^+$.

ii **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$4^n \equiv 1 + 3n \pmod 9$"

(1) If $n = 1$, $4^1 \equiv 1 + 3 \pmod 9$ is true.

$\therefore$ P_1 is true.

(2) If P_k is true, then $4^k \equiv 1 + 3k \pmod 9$

$$\begin{aligned}
\therefore\ 4^{k+1} &= 4 \times 4^k \\
&\equiv 4(1+3k) \pmod 9 \\
&\equiv 4 + 12k \pmod 9 \\
&\equiv 4 + 3k \pmod 9 \\
&\equiv 1 + 3[k+1] \pmod 9
\end{aligned}$$

$\therefore$ P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true, $n \in \mathbb{Z}^+$.

iii **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$5^n \equiv 1 + 4n \pmod{16}$"

(1) If $n = 1$, $5 \equiv 1 + 4 \pmod{16}$ is true.

$\therefore$ P_1 is true.

(2) If P_k is true, then $5^k \equiv 1 + 4k \pmod{16}$

$$\begin{aligned}
\therefore\ 5^{k+1} &= 5 \times 5^k \\
&\equiv 5(1+4k) \pmod{16} \\
&\equiv 5 + 20k \pmod{16} \\
&\equiv 5 + 4k \pmod{16} \\
&\equiv 1 + 4[k+1] \pmod{16}
\end{aligned}$$

$\therefore$ P_1 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true, $n \in \mathbb{Z}^+$.

b We conjecture that:

$(m+1)^n \equiv 1 + mn \pmod{m^2}$ for $m \in \mathbb{Z}^+$, $n \in \mathbb{Z}^+$.

Proof: (by induction)

(1) If $n = 1$, $m + 1 \equiv 1 + m \pmod{m^2}$

$\therefore$ P_1 is true.

(2) If P_k is true then $(m+1)^k \equiv 1 + mk \pmod{m^2}$

$$\begin{aligned} \therefore\quad (m+1)^{k+1} &= (m+1)^k(m+1) \\ &\equiv (1+mk)(m+1) \pmod{m^2} \\ &\equiv m+m^2k+1+mk \pmod{m^2} \\ &\equiv m+0+1+mk \pmod{m^2} \\ &\equiv 1+m(k+1) \pmod{m^2} \end{aligned}$$

Thus P_1 is true and P_{k+1} is true whenever P_k is true.

$\Rightarrow$ P_n is true. {Principle of mathematical induction}

21 $$\begin{aligned} 2^{11}-1 &= (2^4)^2\times 2^3-1 \\ &= 16^2\times 8-1 \\ &\equiv (-7)^2\times 8-1 \pmod{23} \\ &\equiv 49\times 8-1 \pmod{23} \\ &\equiv 3\times 8-1 \pmod{23} \\ &\equiv 0 \pmod{23} \qquad \therefore\ 2^{11}-1 \text{ is divisible by } 23. \end{aligned}$$

EXERCISE 1F.2

1 **a** $2x \equiv 3 \pmod 7$ has $\gcd(2, 7) = 1$

$\therefore$ we have a unique solution.

By inspection, $x \equiv 5 \pmod 7$

{as $2\times 5 = 10 \equiv 3 \pmod 7$}

b $8x \equiv 5 \pmod{25}$ has $\gcd(8, 25) = 1$

$\therefore$ we have a unique solution.

By inspection, $x \equiv 10 \pmod{25}$

{as $8\times 10 = 80 \equiv 5 \pmod{25}$}

c $3x \equiv 6 \pmod{12}$ has $\gcd(3, 12) = 3$ where $3 \mid 6$

$\therefore$ there are exactly 3 incongruent solutions.

Cancelling by 3 gives $x \equiv 2 \pmod 4$

$\therefore$ the solutions are $x = 2+4t$ where $t = 0, 1, 2$

$\therefore$ $x \equiv 2, 6, \text{ or } 10 \pmod{12}$

d $9x \equiv 144 \pmod{99}$ has $\gcd(9, 99) = 9$

where $9 \mid 144$ {$144 = 9\times 16$}

$\therefore$ there are exactly 9 incongruent solutions.

Cancelling by 9 gives $x \equiv 16 \pmod{11}$

$\therefore$ $x \equiv 5 \pmod{11}$

$\therefore$ the solutions are $x = 5+11t$

where $t = 0, 1, 2, 3, 4, 5, 6, 7, 8$

$\therefore$ $x \equiv 5, 16, 27, 38, 49, 60, 71, 82, \text{ or } 93 \pmod{99}$

e $18x \equiv 30 \pmod{40}$ has $\gcd(18, 40) = 2$ where $2 \mid 30$

$\therefore$ there are exactly 2 incongruent solutions.

Cancelling by 2 gives $9x \equiv 15 \pmod{20}$.

By inspection, $x \equiv 15$ is a solution.

$\therefore$ the solutions are $x = 15+20t$ where $t = 0, 1$

$\therefore$ $x \equiv 15 \text{ or } 35 \pmod{40}$

f $3x \equiv 2 \pmod 7$ has $\gcd(3, 7) = 1$

$\therefore$ we have a unique solution.

By inspection, $x \equiv 3 \pmod 7$

{as $3\times 3 = 9 \equiv 2 \pmod 7$}

g $15x \equiv 9 \pmod{27}$ has $\gcd(15, 27) = 3$ where $3 \mid 9$

$\therefore$ there are exactly 3 incongruent solutions.

Cancelling by 3 gives $5x \equiv 3 \pmod 9$.

By inspection, $x \equiv 6$ is a solution.

$\therefore$ the solutions are $x = 6+9t$ where $t = 0, 1, 2$

$\therefore$ $x \equiv 6, 15, \text{ or } 24 \pmod{27}$

h $56x \equiv 14 \pmod{21}$ has $\gcd(56, 21) = 7$ where $7 \mid 14$

$\therefore$ there are exactly 7 incongruent solutions.

Cancelling by 7 gives $8x \equiv 2 \pmod 3$

By inspection, $x \equiv 1$ is a solution.

$\therefore$ the solutions are $x = 1+3t$ where

$t = 0, 1, 2, 3, 4, 5, 6$

$\therefore$ $x \equiv 1, 4, 7, 10, 13, 16, \text{ or } 19 \pmod{21}$

2 **a** $x \equiv 4 \pmod 7$ has $\gcd(1, 7) = 1$

$\therefore$ a unique solution exists

$\therefore$ $x = 4$

and $$\begin{aligned} &\gcd(x, 7) \\ &= \gcd(4, 7) \\ &= 1 \end{aligned}$$

$\therefore$ the statement is **true**.

b $12x \equiv 15 \pmod{35}$ has $\gcd(12, 35) = 1$

$\therefore$ a unique solution exists.

By inspection, $x = 10$

and $4(10) = 40 \equiv 5 \pmod 7$

$\therefore$ $4x \equiv 5 \pmod 7$

$\therefore$ the statement is **true**.

c $12x \equiv 15 \pmod{39}$ has $\gcd(12, 39) = 3$

$\therefore$ 3 solutions exist

and $4x \equiv 5 \pmod{\frac{39}{3}}$

$\therefore$ $4x \equiv 5 \pmod{13}$

$\therefore$ the statement is **true**.

d $x \equiv 7 \pmod{14}$

$\Rightarrow$ $x = 7+14k,\ k \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow\quad &\gcd(x, 14) \\ &= \gcd(7+14k, 14) \\ &= \gcd(7(1+2k), 2\times 7) \\ &= 7 \end{aligned}$$

$\therefore$ the statement is **true**.

e $5x \equiv 5y \pmod{19}$ has $\gcd(5, 19) = 1$

$\Rightarrow$ $x \equiv y \pmod{19}$

$\therefore$ the statement is **true**.

f $3x \equiv y \pmod 8$

$\Rightarrow$ $5(3x) \equiv 5(y) \pmod 8$ {congruence law}

$\Rightarrow$ $15x - 5y = 8t,\ t \in \mathbb{Z}$

$\Rightarrow$ $5(3x-y) = 8t$

$\Rightarrow$ $5 \mid t$ {as $5 \nmid 8$}

$\Rightarrow$ $40 \mid 8t$

$\Rightarrow$ $15x - 5y \equiv 0 \pmod{40}$

$\Rightarrow$ $15x \equiv 5y \pmod{40}$

$\therefore$ the statement is **true**.

g $10x \equiv 10y \pmod{14}$ has $\gcd(10, 14) = 2$

$\Rightarrow$ $x \equiv y \pmod{\frac{14}{2}}$

$\Rightarrow$ $x \equiv y \pmod 7$

$\therefore$ the statement is **true**.

h $x \equiv 41 \pmod{37}$

$\Rightarrow$ $x = 41+37k,\ k \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow\quad x \pmod{41} &\equiv 37k \pmod{41} \\ &\equiv 74 \pmod{41} \quad \text{when } k = 1 \\ &\equiv 33 \end{aligned}$$

$\therefore$ the statement is **false**.

i $x \equiv 37 \pmod{40}$ and $0 \leqslant x < 40$

$\Rightarrow$ $x = 37+40k,\ k \in \mathbb{Z}$ and $0 \leqslant x < 40$

$\Rightarrow$ $0 \leqslant 37+40k < 40$

$\Rightarrow$ $40k \geqslant -37$ and $40k < 3$

$\Rightarrow$ $k \geqslant -\frac{37}{40}$ and $k < \frac{3}{40}$

$\Rightarrow$ $k = 0$

$\Rightarrow$ $x = 37$

$\therefore$ the statement is **true**.

j $15x \equiv 11 \pmod{33}$ has $\gcd(15, 33) = 3$ and $3 \nmid 11$

$\therefore$ no solutions exist for $x \in \mathbb{Z}$

$\therefore$ the statement is **true**.

EXERCISE 1G

1 **a** $x \equiv 4 \pmod{11}, \ x \equiv 3 \pmod 7$

11 and 7 are relatively prime

and $M = 11 \times 7 = 77$

$\therefore \ M_1 = \frac{77}{11} = 7$ and $M_2 = \frac{77}{7} = 11$

Now $7x_1 \equiv 1 \pmod{11} \ \Rightarrow \ x_1 = 8$ {inspection}

and $11x_2 \equiv 1 \pmod 7 \ \Rightarrow \ x_2 = 2$ {inspection}

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 \pmod{77}$

$\therefore \ x \equiv (4)(7)(8) + (3)(11)(2) \pmod{77}$

$\therefore \ x \equiv 290 \pmod{77}$

$\therefore \ x \equiv 59 \pmod{77}$

b $x \equiv 1 \pmod 5, \ x \equiv 2 \pmod 6, \ x \equiv 3 \pmod 7$

where 5, 6, 7 are relatively prime and $M = 5 \times 6 \times 7 = 210$

$\therefore \ M_1 = \frac{210}{5} = 42, \ M_2 = \frac{210}{6} = 35, \ M_3 = \frac{210}{7} = 30$

Now $42x_1 \equiv 1 \pmod 5 \ \Rightarrow \ x_1 = 3$

$35x_2 \equiv 1 \pmod 6 \ \Rightarrow \ x_2 = 5$

$30x_3 \equiv 1 \pmod 7 \ \Rightarrow \ x_3 = 4$

Now

$x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{210}$

$\therefore \ x \equiv (1)(42)(3) + (2)(35)(5) + (3)(30)(4) \pmod{210}$

$\therefore \ x \equiv 836 \pmod{210}$

$\therefore \ x \equiv 206 \pmod{210}$

2 $x \equiv 2 \pmod 3, \ x \equiv 3 \pmod 5, \ x \equiv 2 \pmod 7$

3, 5, and 7 are relatively prime and $M = 3 \times 5 \times 7 = 105$

$\therefore \ M_1 = \frac{105}{3} = 35, \ M_2 = \frac{105}{5} = 21, \ M_3 = \frac{105}{7} = 15$

Now $35x_1 \equiv 1 \pmod 3 \ \Rightarrow \ x_1 = 2$

$21x_2 \equiv 1 \pmod 5 \ \Rightarrow \ x_2 = 1$

$15x_3 \equiv 1 \pmod 7 \ \Rightarrow \ x_3 = 1$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{105}$

$\therefore \ x \equiv (2)(35)(2) + (3)(21)(1) + (2)(15)(1) \pmod{105}$

$\therefore \ x \equiv 233 \pmod{105}$

$\therefore \ x \equiv 23 \pmod{105}$

$\therefore \ x = 23, 128, 233, 338$, and so on.

Thus 23 is the smallest solution, and all other solutions have the form $23 + 105k, \ k \in \mathbb{N}$.

3 **a** $x \equiv 1 \pmod 2, \ x \equiv 2 \pmod 3, \ x \equiv 3 \pmod 5$

2, 3, 5 are relatively prime and $M = 30$

$\therefore \ M_1 = 15, \ M_2 = 10, \ M_3 = 6$

Now $15x_1 \equiv 1 \pmod 2 \ \Rightarrow \ x_1 = 1$

$10x_2 \equiv 1 \pmod 3 \ \Rightarrow \ x_2 = 1$

$6x_3 \equiv 1 \pmod 5 \ \Rightarrow \ x_3 = 1$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{30}$

$\therefore \ x \equiv (1)(15)(1) + (2)(10)(1) + (3)(6)(1) \pmod{30}$

$\therefore \ x \equiv 53 \pmod{30}$

$\therefore \ x \equiv 23 \pmod{30}$

b $x \equiv 0 \pmod 2, \ x \equiv 0 \pmod 3, \ x \equiv 1 \pmod 5,$
$x \equiv 6 \pmod 7$

2, 3, 5, and 7 are relatively prime and
$M = 2 \times 3 \times 5 \times 7 = 210$

$\therefore \ M_1 = 105, \ M_2 = 70, \ M_3 = 42, \ M_4 = 30$

Now $105x_1 \equiv 1 \pmod 2 \ \Rightarrow \ x_1 = 1$

$70x_2 \equiv 1 \pmod 3 \ \Rightarrow \ x_2 = 1$

$42x_3 \equiv 1 \pmod 5 \ \Rightarrow \ x_3 = 3$

$30x_4 \equiv 1 \pmod 7 \ \Rightarrow \ x_4 = 4$

$\therefore \ x \equiv (0)(105)(1) + (0)(70)(1) + (1)(42)(3)$
$+ (6)(30)(4) \pmod{210}$

$\therefore \ x \equiv 846 \pmod{210}$

$\therefore \ x \equiv 6 \pmod{210}$

4 **a** $x \equiv 4 \pmod{11}$

$\therefore \ x = 4 + 11t, \ t \in \mathbb{Z}$

and as $x \equiv 3 \pmod 7$

then $4 + 11t \equiv 3 \pmod 7$

$\therefore \ 11t \equiv -1 \pmod 7$

$\therefore \ 11t \equiv 6 \pmod 7$

$\therefore \ t \equiv 5 \pmod 7$

$\therefore \ t = 5 + 7s, \ s \in \mathbb{Z}$

Thus $x = 4 + 11t$

$= 4 + 11(5 + 7s), \ s \in \mathbb{Z}$

$= 59 + 77s, \ s \in \mathbb{Z}$

$\therefore \ x \equiv 59 \pmod{77}$

(This agrees with **1 a**.)

b $x \equiv 1 \pmod 5$

$\therefore \ x = 1 + 5r, \ r \in \mathbb{Z}$

Substituting into the 2nd congruence $x \equiv 2 \pmod 6$,

$1 + 5r \equiv 2 \pmod 6$

$\therefore \ 5r \equiv 1 \pmod 6$

$\therefore \ r \equiv 5 \pmod 6$

$\therefore \ r = 5 + 6s, \ s \in \mathbb{Z}$

Substituting into the 3rd congruence $x \equiv 3 \pmod 7$,

$1 + 5(5 + 6s) \equiv 3 \pmod 7$

$\therefore \ 26 + 30s \equiv 3 \pmod 7$

$\therefore \ 30s \equiv -23 \pmod 7$

$\therefore \ 2s \equiv 5 \pmod 7$

$\therefore \ s \equiv 6 \pmod 7$

$\therefore \ s = 6 + 7t, \ t \in \mathbb{Z}$

$\therefore \ x = 26 + 30s$

$x = 26 + 30(6 + 7t)$

$x = 206 + 210t$

$\therefore \ x \equiv 206 \pmod{210}$

(This agrees with **1 b**.)

c $x \equiv 0 \pmod 2$

$\therefore \ x = 0 + 2q, \ q \in \mathbb{Z}$

Substituting into the 2nd congruence $x \equiv 0 \pmod 3$,

$2q \equiv 0 \pmod 3$

$\therefore \ q \equiv 0 \pmod 3$

$\therefore \ q = 3r, \ r \in \mathbb{Z}$

Substituting into the 3rd congruence $x \equiv 1 \pmod 5$,

$2(3r) \equiv 1 \pmod 5$

$\therefore \ 6r \equiv 1 \pmod 5$

$\therefore \ r \equiv 1 \pmod 5$

$\therefore \ r = 1 + 5s, \ s \in \mathbb{Z}$

Substituting into the 4th congruence $x \equiv 6 \pmod 7$,

$6(1 + 5s) \equiv 6 \pmod 7$

$6 + 30s \equiv 6 \pmod 7$

$\therefore \ 30s \equiv 0 \pmod 7$

$\therefore \ s \equiv 0 \pmod 7$

$\therefore \ s = 7t$

$\therefore \ x = 6 + 210t$

$\therefore \ x \equiv 6 \pmod{210}$

(This agrees with **3 b**.)

5 $17x \equiv 3 \pmod{210}$

As $210 = 2 \times 3 \times 5 \times 7$ where these factors are relatively prime, an equivalent problem is to solve simultaneously

$17x \equiv 3 \pmod{2}$, $17x \equiv 3 \pmod{3}$, $17x \equiv 3 \pmod{5}$, and $17x \equiv 3 \pmod{7}$.

$\therefore\ x \equiv 1 \pmod{2}$, $2x \equiv 0 \pmod{3}$, $2x \equiv 3 \pmod{5}$, and $3x \equiv 3 \pmod{7}$

$\therefore\ x \equiv 1 \pmod{2}$, $x \equiv 0 \pmod{3}$, $x \equiv 4 \pmod{5}$, and $x \equiv 1 \pmod{7}$.

As 2, 3, 5, and 7 are relatively prime, and $M = 210$, then $M_1 = 105$, $M_2 = 70$, $M_3 = 42$, $M_4 = 30$.

Now
$$\begin{aligned} 105x_1 &\equiv 1 \pmod{2} \Rightarrow x_1 = 1 \\ 70x_2 &\equiv 1 \pmod{3} \Rightarrow x_2 = 1 \\ 42x_3 &\equiv 1 \pmod{5} \Rightarrow x_3 = 3 \\ 30x_4 &\equiv 1 \pmod{7} \Rightarrow x_4 = 4 \end{aligned}$$

Thus
$$x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 + a_4M_4x_4 \pmod{210}$$
$$\therefore\ x \equiv (1)(105)(1) + 0 + (4)(42)(3) + (1)(30)(4) \pmod{210}$$
$$\therefore\ x \equiv 729 \pmod{210}$$
$$\therefore\ x \equiv 99 \pmod{210}$$

6 We need to find x for $x \equiv 2 \pmod{3}$, $x \equiv 2 \pmod{4}$

3, 4 are relatively prime and $M = 12$

$\therefore\ M_1 = 4$, $M_2 = 3$.

Now
$$\begin{aligned} 4x_1 &\equiv 1 \pmod{3} \Rightarrow x_1 = 1 \\ 3x_2 &\equiv 1 \pmod{4} \Rightarrow x_2 = 3 \end{aligned}$$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 \pmod{12}$
$$\therefore\ x \equiv (2)(4)(1) + (2)(3)(3) \pmod{12}$$
$$\therefore\ x \equiv 26 \pmod{12}$$
$$\therefore\ x \equiv 2 \pmod{12}$$
$$\therefore\ x = 2 + 12k,\ k \in \mathbb{Z}.$$

Thus, all integers with this property have form $2 + 12k$, $k \in \mathbb{Z}$.

7 We need to find x for

$x \equiv 2 \pmod{5}$, $x \equiv 2 \pmod{7}$, $x \equiv 0 \pmod{3}$

5, 7, and 3 are relatively prime and $M = 105$

$\therefore\ M_1 = 21$, $M_2 = 15$, $M_3 = 35$.

Now
$$\begin{aligned} 21x_1 &\equiv 1 \pmod{5} \Rightarrow x_1 = 1 \\ 15x_2 &\equiv 1 \pmod{7} \Rightarrow x_2 = 1 \\ 35x_3 &\equiv 1 \pmod{3} \Rightarrow x_3 = 2 \end{aligned}$$

$$\therefore\ x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{105}$$
$$\therefore\ x \equiv (2)(21)(1) + (2)(15)(1) + 0 \pmod{105}$$
$$\therefore\ x \equiv 72 \pmod{105}$$
$$\therefore\ x = 72 + 105k,\ k \in \mathbb{Z}.$$

Thus, all integers with this property have form $72+105k$, $k \in \mathbb{Z}$.

8 We need to find x for

$x \equiv 1 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 0 \pmod{4}$

where 3, 5, and 4 are relatively prime and $M = 3 \times 5 \times 4 = 60$

$\therefore\ M_1 = 20$, $M_2 = 12$, $M_3 = 15$.

Now
$$\begin{aligned} 20x_1 &\equiv 1 \pmod{3} \Rightarrow x_1 = 2 \\ 12x_2 &\equiv 1 \pmod{5} \Rightarrow x_2 = 3 \\ 15x_3 &\equiv 1 \pmod{4} \Rightarrow x_3 = 3 \end{aligned}$$

$$\therefore\ x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{60}$$
$$\therefore\ x \equiv (1)(20)(2) + (3)(12)(3) + 0 \pmod{60}$$
$$\therefore\ x \equiv 148 \pmod{60}$$
$$\therefore\ x \equiv 28 \pmod{60}$$
$$\therefore\ x = 28 + 60k,\ k \in \mathbb{Z}.$$

Thus, all integers with this property are of the form $28 + 60k$, $k \in \mathbb{Z}$.

9 Let the total number of sweets be x.

$\therefore\ x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{4}$,
$x \equiv 4 \pmod{5}$, $x \equiv 5 \pmod{6}$, $x \equiv 0 \pmod{7}$.

We cannot use the Chinese Remainder Theorem here as 2, 3, 4, 5, 6, and 7 are not relatively prime. For example, $\gcd(4, 6) = 2$.

We notice that $x + 1$ is divisible by 2, 3, 4, 5, and 6

$\therefore\ x + 1$ is divisible by 60 $\{60 = \operatorname{lcm}(2, 3, 4, 5, 6)\}$

$\therefore\ x = -1 + 60s,\ s \in \mathbb{Z}$

$\therefore\ x = 59, 119, 179, 239, ...$

We test these in order for divisibility by 7

$\therefore$ 119 is the smallest possible number of sweets.

10 Let x be the number of gold coins.

Then, $x \equiv 3 \pmod{17}$, $x \equiv 10 \pmod{16}$, $x \equiv 0 \pmod{15}$

where 17, 16, and 15 are relatively prime

and $M = 17 \times 16 \times 15 = 4080$

with $M_1 = 240$, $M_2 = 255$, $M_3 = 272$.

Now
$$\begin{aligned} 240x_1 &\equiv 1 \pmod{17} \Rightarrow x_1 = 9 \\ 255x_2 &\equiv 1 \pmod{16} \Rightarrow x_2 = 15 \\ 272x_3 &\equiv 1 \pmod{15} \Rightarrow x_3 = 8 \end{aligned}$$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{4080}$
$$\therefore\ x \equiv (3)(240)(9) + (10)(255)(15) + 0 \pmod{4080}$$
$$\therefore\ x \equiv 44\,730 \pmod{4080}$$
$$\therefore\ x \equiv 3930 \pmod{4080}$$

$\therefore$ the smallest number of coins is 3930.

11 **a** $4x + 7y = 5$ .... (1)

$$\begin{aligned} &\therefore\ 4x = 5 - 7y && \text{and} && 7y = 5 - 4x \\ &\therefore\ 4x \equiv 5 \pmod{7} && && \therefore\ 7y \equiv 5 \pmod{4} \\ &\therefore\ x \equiv 3 \pmod{7} && && \therefore\ 3y \equiv 1 \pmod{4} \\ &\therefore\ x = 3 + 7t,\ t \in \mathbb{Z} && && \therefore\ y \equiv 3 \pmod{4} \\ & && && \therefore\ y = 3 + 4s,\ s \in \mathbb{Z} \end{aligned}$$

and so in (1), $4(3 + 7t) + 7(3 + 4s) = 5$
$$\therefore\ 12 + 28t + 21 + 28s = 5$$
$$\therefore\ 28(s + t) = 5 - 33$$
$$\therefore\ 28(s + t) = -28$$
$$\therefore\ s + t = -1$$

Thus $y = 3 + 4(-1 - t)$
$$\therefore\ y = -1 - 4t$$
$$\therefore\ x = 3 + 7t,\ y = -1 - 4t,\ t \in \mathbb{Z}.$$

b **i**
$$\begin{aligned} &11x + 8y = 31 && \text{and} && 8y = 31 - 11x \\ &\therefore\ 11x = 31 - 8y && && \therefore\ 8y \equiv 31 \pmod{11} \\ &\therefore\ 11x \equiv 31 \pmod{8} && && \therefore\ 8y \equiv 9 \pmod{11} \\ &\therefore\ 3x \equiv 7 \pmod{8} && && \therefore\ y \equiv 8 \pmod{11} \\ &\therefore\ x \equiv 5 \pmod{8} && && \therefore\ y = 8 + 11s,\ s \in \mathbb{Z} \\ &\therefore\ x = 5 + 8t,\ t \in \mathbb{Z} && && \end{aligned}$$

But $11x + 8y = 31$
$$\therefore\ 55 + 88t + 64 + 88s = 31$$
$$\therefore\ 88(s + t) = -88$$
$$\therefore\ s + t = -1$$
$$\therefore\ s = -1 - t$$
$$\therefore\ y = 8 + 11(-1 - t)$$
$$\therefore\ y = -3 - 11t$$
$$\therefore\ x = 5 + 8t,\ y = -3 - 11t,\ t \in \mathbb{Z}.$$

ii $7x + 5y = 13$

$\therefore\ 7x = 13 - 5y$ and $5y = 13 - 7x$

$\therefore\ 7x \equiv 13 \pmod 5$ $\quad\therefore\ 5y \equiv 13 \pmod 7$

$\therefore\ 2x \equiv 3 \pmod 5$ $\quad\therefore\ 5y \equiv 6 \pmod 7$

$\therefore\ x \equiv 4 \pmod 5$ $\quad\therefore\ y \equiv 4 \pmod 7$

$\therefore\ x = 4 + 5t,\ t \in \mathbb{Z}$ $\quad\therefore\ y = 4 + 7s,\ s \in \mathbb{Z}$

But $7x + 5y = 13$

$\therefore\ 28 + 35t + 20 + 35s = 13$

$\therefore\ 35(s + t) = -35$

$\therefore\ s + t = -1$

$\therefore\ s = -1 - t$

$\therefore\ y = 4 + 7(-1 - t)$

$\therefore\ y = -3 - 7t$

$\therefore\ x = 4 + 5t,\ y = -3 - 7t,\ t \in \mathbb{Z}.$

12 $2 \mid a,\ 3 \mid (a + 1),\ 4 \mid (a + 2),\ 5 \mid (a + 3),\ 6 \mid (a + 4)$

$\therefore\ a \equiv 0 \pmod 2,\ a + 1 \equiv 0 \pmod 3,\ a + 2 \equiv 0 \pmod 4,$
$a + 3 \equiv 0 \pmod 5,\ a + 4 \equiv 0 \pmod 6$

$\therefore$ a is even and $a \equiv 2$ (mod 3, 4, 5, or 6)

$\therefore$ a is even and $a = 2 + 60t,\ t \in \mathbb{Z}$ $\{60 = \text{lcm}(3, 4, 5, 6)\}$

$\therefore\ a = 62, 122, 182, \ldots.$

$\therefore$ the smallest a is 62.

Note: As the divisors 2, 3, 4, 5, and 6 are not relatively prime the Chinese Remainder Theorem may not be appropriate.

13 $2x \equiv 1 \pmod 5$, $3x \equiv 9 \pmod 6$, $4x \equiv 1 \pmod 7$, and $5x \equiv 9 \pmod{11}$

$\therefore\ x \equiv 3 \pmod 5,\ \underset{\substack{\uparrow \\ \text{on cancellation}}}{x \equiv 3 \pmod 2},\ x \equiv 2 \pmod 7,$

$x \equiv 4 \pmod{11}$ where 5, 2, 7, and 11 are relatively prime.

$M = 770$

$\therefore\ M_1 = 154,\ M_2 = 385,\ M_3 = 110,\ M_4 = 70$

Now $154x_1 \equiv 1 \pmod 5$

$\therefore\ 4x_1 \equiv 1 \pmod 5$

$\therefore\ x_1 = 4$

$385x_2 \equiv 1 \pmod 2$

$\therefore\ x_2 \equiv 1 \pmod 2$

$\therefore\ x_2 = 1$

$110x_3 \equiv 1 \pmod 7$

$\therefore\ 5x_3 \equiv 1 \pmod 7$

$\therefore\ x_3 = 3$

$70x_4 \equiv 1 \pmod{11}$

$\therefore\ 4x_4 \equiv 1 \pmod{11}$

$\therefore\ x_4 = 3$

Thus $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 + a_4M_4x_4 \pmod{770}$

$\therefore\ x \equiv (3)(154)(4) + (3)(385)(1) + (2)(110)(3) + (4)(70)(3) \pmod{770}$

$\therefore\ x \equiv 4503 \pmod{770}$

$\therefore\ x \equiv 653 \pmod{770}.$

EXERCISE 1H

1 $A \pmod 2 = 1 \longleftarrow$ remainder

$A \pmod 3 = 1 \longleftarrow$ remainder

{The digit sum is $52 \equiv 1 \pmod 3$}

$A \pmod 5 = 2 \nwarrow$ {it ends in 7}

$A \pmod 9 = 7 \longleftarrow$ remainders

{The digit sum is $52 \equiv 7 \pmod 9$}

$A \pmod{11} = 0$

$\therefore$ A is divisible by 11

{sum of digits in odd positions − sum of digits in even positions
$= 26 - 26$
$= 0$ which is a multiple of 11}

2 **a** **i** $a_i10^i \equiv 0 \pmod{10}$ for $i \geqslant 1$

$\therefore\ A \pmod{10} = 0 + 0 + \ldots. + 0 + a_0$
$= a_0$

ii $a_i10^i \equiv 0 \pmod{100}$ for $i \geqslant 2$

$\therefore\ A \pmod{100} = 0 + 0 + \ldots. + 0 + a_110 + a_0$
$= 10a_1 + a_0$

iii $a_i10^i \equiv 0 \pmod{1000}$ for $i \geqslant 3$

$\therefore\ A \pmod{1000}$
$= 0 + 0 + \ldots. + 0 + a_210^2 + a_110 + a_0$
$= 100a_2 + 10a_1 + a_0$

b A is divisible by 10 if it ends in 0
A is divisible by 100 if it ends in 00
A is divisible by 1000 if it ends in 000.

3 $A = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \ldots. + a_210^2 + a_110 + a_0$

a $4 \mid A \ \Leftrightarrow\ 4 \mid 10a_1 + a_0$
$\Leftrightarrow\ 4 \mid 2a_1 + a_0$
$\{10^k$ for $k \geqslant 2$ are all divisible by 4$\}$

$8 \mid A \ \Leftrightarrow\ 8 \mid 4a_2 + 2a_1 + a_0$

Proof:

$a_i10^i \equiv 0 \pmod 8$ for $i \geqslant 3$

$\therefore\ A \pmod 8 = 100a_2 + 10a_1 + a_0$
$= 4a_2 + 2a_1 + a_0$

$\therefore\ 8 \mid A \ \Leftrightarrow\ 8 \mid (4a_2 + 2a_1 + a_0)$

b A is divisible by 16 $\Leftrightarrow$ $16 \mid (8a_3 + 4a_2 + 2a_1 + a_0)$

c **i** 2^8 **ii** 2^3 **iii** 2^{10} **iv** 2^1 **v** 2^4 **vi** 2^4

4 **a** $n \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \pmod{10}$

$\therefore\ n^2 \equiv 0, 1, 4, 9, 6, 5, 6, 9, 4, 1 \pmod{10}$

$\Rightarrow\ n^2 \equiv 0, 1, 4, 5, 6, \text{ or } 9 \pmod{10}$

b From **a**, an integer can be a perfect square if it ends in 0, 1, 4, 5, 6, or 9.
Thus none of the given integers can be a perfect square.

5 $\displaystyle\sum_{r=1}^{4} r! = 1! + 2! + 3! + 4!$
$= 33$ which is not a square

$\displaystyle\sum_{r=1}^{5} r! = 33 + 5!$
$= 33 + 120$
$= 153$ which is not a square

Since $n!$ ends in 0 for all $n \geqslant 5$, $\displaystyle\sum_{r=1}^{n} n!$ ends in 3 for all $n \geqslant 5$.

From **4**, any such number cannot be square, so Claudia is correct.

6 $R_k = \underbrace{111\,111\,11\ldots.1}_{k\ 1\text{s}}$

a R_k is divisible by 3 if $k = 3n,\ n \in \mathbb{Z}^+$.
For example, $R_6 = 111\,111$ and the sum of its digits is 6 and $3 \mid 6$.

b R_k is divisible by 9 if $k = 9n, \; n \in \mathbb{Z}^+$.

c R_k is divisible by 11 if $k = 2n, \; n \in \mathbb{Z}^+$.
For example, $111\,111 = 11 \times 10\,101$.

7 **a**
$$\begin{aligned} 7 \mid 6994 &\Leftrightarrow 7 \mid 699 - 2(4) \\ &\Leftrightarrow 7 \mid 691 \\ &\Leftrightarrow 7 \mid 69 - 2(1) \\ &\Leftrightarrow 7 \mid 67 \end{aligned}$$
which is not true.
So, $7 \nmid 6994$.
$$\begin{aligned} 7 \mid 6993 &\Leftrightarrow 7 \mid 699 - 2(3) \\ &\Leftrightarrow 7 \mid 693 \\ &\Leftrightarrow 7 \mid 69 - 2(3) \\ &\Leftrightarrow 7 \mid 63 \end{aligned}$$
which is true.
So, $7 \mid 6993$.

b
$$\begin{aligned} 13 \mid 6994 &\Leftrightarrow 13 \mid 699 - 9(4) \\ &\Leftrightarrow 13 \mid 663 \\ &\Leftrightarrow 13 \mid 66 - 9(3) \\ &\Leftrightarrow 13 \mid 39 \end{aligned}$$
which is true.
So, $13 \mid 6994$.
$$\begin{aligned} 13 \mid 6993 &\Leftrightarrow 13 \mid 699 - 9(3) \\ &\Leftrightarrow 13 \mid 672 \\ &\Leftrightarrow 13 \mid 67 - 9(2) \\ &\Leftrightarrow 13 \mid 49 \end{aligned}$$
which is not true.
So, $13 \nmid 6993$.

8 Let $c = (a_{n-1}a_{n-2}....a_3a_2a_1)$
$$\begin{aligned} \therefore \quad A &= 10c + a_0 \\ \therefore \quad -9A &= -90c - 9a_0 \\ \therefore \quad -9A &\equiv c - 9a_0 \pmod{13} \end{aligned}$$
$$\begin{aligned} \text{Thus} \quad 13 \mid A &\Leftrightarrow 13 \mid -9A \\ &\Leftrightarrow 13 \mid c - 9a_0 \\ &\Leftrightarrow 13 \mid ((a_{n-1}a_{n-2}....a_2a_1) - 9a_0) \end{aligned}$$

9 **a** **i** An integer is divisible by 25 if (a_1a_0) is divisible by 25.

ii An integer is divisible by 125 if $(a_2a_1a_0)$ is divisible by 125.

b **i** 5^3 **ii** 5^1 **iii** 5^9

10 **a** An integer is divisible by 6 if it is divisible by both 2 and 3.

b An integer is divisible by 12 if it is divisible by both 4 and 3.

c An integer is divisible by 14 if it is divisible by both 2 and 7.

d An integer is divisible by 15 if it is divisible by both 3 and 5.

11 **a**
$$\begin{aligned} &(1+7+3+3) - (0+6+7+2) \\ &= 14 - 15 \\ &= -1 \quad \text{which is not divisible by 11} \end{aligned}$$
$\therefore$ the number is not divisible by 11.

b
$$\begin{aligned} &(8+2+3+0+6+5+8) - (9+4+1+0+4+3) \\ &= 32 - 21 \\ &= 11 \quad \text{which is divisible by 11} \end{aligned}$$
$\therefore$ the number is divisible by 11.

c
$$\begin{aligned} &(1+8+3+6+1) - (0+6+2+7+5) \\ &= 19 - 20 \\ &= -1 \quad \text{which is not a multiple of 11} \end{aligned}$$
$\therefore$ the number is not divisible by 11.

12 **a** $A = 201\,984$

- $\begin{aligned} \text{sum of digits} &= 2+0+1+9+8+4 \\ &= 24 \quad \text{where} \quad 3 \mid 24 \end{aligned}$
  $\therefore$ A is divisible by 3.
- sum of digits $= 24$ and $9 \nmid 24$
  $\therefore$ A is not divisible by 9.
- $\begin{aligned} &(2+1+8) - (0+9+4) \\ &= 11 - 13 \\ &= -2 \quad \text{which is not a multiple of 11} \end{aligned}$
  $\therefore$ A is not divisible by 11

b $A = 101\,582\,283$

- $\begin{aligned} \text{sum of digits} &= 1+0+1+5+8+2+2+8+3 \\ &= 30 \quad \text{and} \quad 3 \mid 30 \end{aligned}$
  $\therefore$ A is divisible by 3.
- sum of digits $= 30$ and $9 \nmid 30$
  $\therefore$ A is not divisible by 9.
- $\begin{aligned} &(1+1+8+2+3) - (0+5+2+8) \\ &= 15 - 15 \\ &= 0 \quad \text{which is a multiple of 11} \end{aligned}$
  $\therefore$ A is divisible by 11.

c $A = 41\,578\,912\,245$

- sum of digits $= 48$ and $3 \mid 48$ and $9 \nmid 48$
  $\therefore$ A is divisible by 3 but not by 9.
- $\begin{aligned} &(4+5+8+1+2+5) - (1+7+9+2+4) \\ &= 25 - 23 \\ &= 2 \quad \text{which is not a multiple of 11} \end{aligned}$
  $\therefore$ A is not divisible by 11.

d $A = 10\,415\,486\,358$

- sum of digits $= 45$ and $3 \mid 45$ and $9 \mid 45$
  $\therefore$ A is divisible by 3 and 9.
- $\begin{aligned} &(1+4+5+8+3+8) - (0+1+4+6+5) \\ &= 29 - 16 \\ &= 13 \quad \text{and} \quad 11 \nmid 13 \end{aligned}$
  $\therefore$ A is not divisible by 11.

13
$$\begin{aligned} n &\equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \pmod{10} \\ \therefore \quad n(n-1) &\equiv 0, 0, 2, 6, 2, 0, 0, 2, 6, 2 \pmod{10} \\ \therefore \quad n^2 - n &\equiv 0, 2, 6 \pmod{10} \\ \therefore \quad n^2 - n + 7 &\equiv 7, 9, 3 \pmod{10} \end{aligned}$$
$\therefore$ $n^2 - n + 7$ has a last digit of 3, 7, or 9.

14 **a** **i**
$$\begin{aligned} A &= 101\,110\,101\,001 \\ &= 2^{11} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3 + 1 \end{aligned}$$
which is odd $\therefore$ highest power of 2 is 2^0.

ii **Note:**
$$\begin{aligned} &2^{2n} && 2^{2n+1} \\ &= 4^n && = 4^n \times 2 \\ &\equiv 1^n \pmod 3 && \equiv 1 \times 2 \pmod 3 \\ &\equiv 1 \pmod 3 && \equiv 2 \pmod 3 \end{aligned}$$
$$\begin{aligned} \therefore \quad A &\equiv 2+2+1+2+2+2+1 \pmod 3 \\ \therefore \quad A &\equiv 12 \pmod 3 \\ \therefore \quad A &\equiv 0 \pmod 3 \end{aligned}$$
$\therefore$ A is divisible by 3.

b **i** $A = 1\,001\,110\,101\,000$

$= 2^{12} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3$

$= 2^3(\underbrace{2^9 + 2^6 + 2^5 + 2^4 + 2^2 + 1}_{\text{odd}})$

$\therefore$ highest power of 2 is 2^3.

ii $A \equiv 1 + 2 + 1 + 2 + 2 + 2 \pmod 3$

$\therefore$ $A \equiv 10 \pmod 3$

$\therefore$ $A \equiv 1 \pmod 3$

$\therefore$ A is not divisible by 3.

c **i** $A = 1\,010\,101\,110\,100\,100$

$= 2^{15} + 2^{13} + 2^{11} + 2^9 + 2^8 + 2^7 + 2^5 + 2^2$

$= 2^2(\underbrace{2^{13} + 2^{11} + 2^9 + 2^7 + 2^6 + 2^5 + 2^3 + 1}_{\text{odd}})$

$\therefore$ highest power of 2 is 2^2.

ii $A \equiv 2 + 2 + 2 + 2 + 1 + 2 + 2 + 1 \pmod 3$

$\therefore$ $A \equiv 14 \pmod 3$

$\therefore$ $A \equiv 2 \pmod 3$

$\therefore$ A is not divisible by 3.

Note: The highest power of 2 that divides a binary number is 2^n, where n is the number of 0s at the end of the number.

15 **a** **i** $A = 10\,200\,122\,221\,210$

$A = (3^{13}) + 2(3^{11}) + (3^8) + 2(3^7) + 2(3^6) + 2(3^5)$
$+ 2(3^4) + (3^3) + 2(3^2) + 3^1$

$\therefore$ highest power of 3 is 3^1.

ii **Note:** $3^n \equiv 1^n \pmod 2$

$\therefore$ $3^n \equiv 1 \pmod 2$ for all $n \in \mathbb{N}$

$\therefore$ $A \equiv 1 + 2 + 1 + 2 + 2 + 2 + 2 + 1 + 2$
$+ 1 \pmod 2$

$\equiv 16 \pmod 2$

$\equiv 0 \pmod 2$

$\therefore$ A is divisible by 2.

iii **Note:**

3^{2n}	3^{2n+1}
$= 9^n$	$= 9^n \times 3$
$\equiv 1^n \pmod 4$	$\equiv 1 \times 3 \pmod 4$
$\equiv 1 \pmod 4$	$\equiv 3 \pmod 4$

$\therefore$ $A \equiv 3 + 2(3) + 1 + 2(3) + 2(1) + 2(3) + 2(1)$
$+ 3 + 2(1) + 3 \pmod 4$

$\therefore$ $A \equiv 34 \pmod 4$

$\therefore$ $A \equiv 2 \pmod 4$

$\therefore$ A is not divisible by 4.

b **i** $A = 221\,021\,010\,020\,120$

$\therefore$ $A = 2(3^{14}) + 2(3^{13}) + 3^{12} + 2(3^{10}) + 3^9 + 3^7$
$+ 2(3^4) + 3^2 + 2(3)$

$\therefore$ highest power of 3 is 3^1.

ii $A \equiv 2 + 2 + 1 + 2 + 1 + 1 + 2 + 1 + 2 \pmod 2$

$\equiv 14 \pmod 2$

$\equiv 0 \pmod 2$

$\therefore$ A is divisible by 2.

iii $A \equiv 2(1) + 2(3) + 1 + 2(1) + 3 + 3 + 2(1) + 1$
$+ 2(3) \pmod 4$

$\equiv 26 \pmod 4$

$\equiv 2 \pmod 4$

$\therefore$ A is not divisible by 4.

c **i** $A = 1\,010\,101\,110\,100\,100$

$= 3^{15} + 3^{13} + 3^{11} + 3^9 + 3^8 + 3^7 + 3^5 + 3^2$

$\therefore$ highest power of 3 is 3^2.

ii $A \equiv 8 \pmod 2$

$\therefore$ $A \equiv 0 \pmod 2$

$\therefore$ A is divisible by 2.

iii $A \equiv 3 + 3 + 3 + 3 + 1 + 3 + 3 + 1 \pmod 4$

$\equiv 20 \pmod 4$

$\equiv 0 \pmod 4$

$\therefore$ A is divisible by 4.

16 Let
$A = a_{n-1}8^{n-1} + a_{n-2}8^{n-2} + ... + a_3 8^3 + a_2 8^2 + a_1 8 + a_0$

Now $8^k \equiv 1^k \pmod 7$

$\therefore$ $8^k \equiv 1 \pmod 7$ for all $k = 1, 2, ..., n-1$

$\therefore$ $A \equiv a_{n-1} + a_{n-2} + ... + a_3 + a_2 + a_1 + a_0 \pmod 7$

$\therefore$ A is divisible by 7 if the sum of its digits is divisible by 7.

Generalisation: If A is a base n number, A is divisible by $n-1$ if the sum of its digits is divisible by $n-1$.

17 Let
$A = a_{n-1}8^{n-1} + a_{n-2}8^{n-2} + ... + a_3 8^3 + a_2 8^2 + a_1 8 + a_0$

Now $8 \equiv (-1) \pmod 9$

$\therefore$ $8^{2k} \equiv (-1)^{2k} \pmod 9$

$\therefore$ $8^{2k} \equiv 1 \pmod 9$

and $8^{2k+1} \equiv -1 \pmod 9$

$\therefore$ $A \equiv a_0 - a_1 + a_2 - a_3 + a_4 - .... \pmod 9$

$\therefore$ $A \equiv [a_0 + a_2 + a_4 + ...] - [a_1 + a_3 + a_5 + ...] \pmod 9$

$\therefore$ A is divisible by 9 if the sum of the digits in the even positions minus the sum of the digits in the odd positions is divisible by 9.

Generalisation:
If A is a base n number, A is divisible by $n+1$ if the sum of the digits in the even positions minus the sum of the digits in the odd positions is divisible by $n+1$.

18 **a** $X = (x_n x_{n-1} x_{n-2} .... x_3 x_2 x_1 x_0)_{25}$

$= x_n 25^n + x_{n-1} 25^{n-1} + ... + x_2 25^2 + x_1 25 + x_0$

Now $25^k \equiv 0 \pmod 5$ for all $k = 1, 2, ..., n$

$\therefore$ $X \equiv x_0 \pmod 5$

$\therefore$ X is divisible by 5 if x_0 is divisible by 5.

b As $25 \equiv 1 \pmod 2$

then $25^k \equiv 1 \pmod 2$ for all $k = 1, 2, ..., n$

$\therefore$ $X \equiv x_n + x_{n-1} + ... + x_2 + x_1 + x_0 \pmod 2$

$\therefore$ X is divisible by 2 if the sum of its digits is divisible by 2.

c As $25 \equiv 1 \pmod 4$

then $25^k \equiv 1 \pmod 4$ for all $k = 1, 2, ..., n$

$\therefore$ $X \equiv x_n + x_{n-1} + ... + x_2 + x_1 + x_0 \pmod 4$

$\therefore$ X is divisible by 4 if the sum of its digits is divisible by 4.

Now if $X = (664\,089\,735)_{25}$

we see that $5 \mid X$ $\{$as $x_0 = 5\}$

Also the sum of the digits of X is

$6 + 6 + 4 + 0 + 8 + 9 + 7 + 3 + 5 = 48$ where $4 \mid 48$

$\therefore$ $4 \mid X$

As $\gcd(4, 5) = 1$ and $4 \mid X$, $5 \mid X$ then $4 \times 5 \mid X$

$\therefore$ $20 \mid X$

EXERCISE 1I

1 **a** $5^{152} \pmod{13}$

$\equiv (5^{12})^{12} \times 5^8 \pmod{13}$

$\equiv 1^{12} \times 25^4 \pmod{13}$ {FLT}

$\equiv 1 \times (-1)^4 \pmod{13}$

$\equiv 1 \pmod{13}$

b $4^{56} \pmod 7$

$\equiv (4^6)^9 \times 4^2 \pmod 7$

$\equiv 1^9 \times 16 \pmod 7$ {FLT}

$\equiv 1 \times 2 \pmod 7$

$\equiv 2 \pmod 7$

c $8^{205} \pmod{17}$

$\equiv (8^{16})^{12} \times 8^{13} \pmod{17}$

$\equiv 1^{12} \times 64^6 \times 8 \pmod{17}$ {FLT}

$\equiv 1 \times (-4)^6 \times 8 \pmod{17}$ $\{17 \times 4 = 68\}$

$\equiv 16^3 \times 8 \pmod{17}$

$\equiv (-1)^3 \times 8 \pmod{17}$

$\equiv -8 \pmod{17}$

$\equiv 9 \pmod{17}$

d $3^{95} \pmod{13}$

$\equiv (3^{12})^7 \times 3^{11} \pmod{13}$

$\equiv 1^7 \times (3^3)^3 \times 3^2 \pmod{13}$ {FLT}

$\equiv 1 \times 27^3 \times 9 \pmod{13}$

$\equiv 1^3 \times 9 \pmod{13}$

$\equiv 9 \pmod{13}$

2 **a** $3x \equiv 5 \pmod 7$ where $7 \nmid 3$

$\therefore\ x \equiv 3^5 \times 5 \pmod 7$

$\therefore\ x \equiv (3^2)^2 \times 15 \pmod 7$

$\therefore\ x \equiv 2^2 \times 1 \pmod 7$

$\therefore\ x \equiv 4 \pmod 7$

b $8x \equiv 3 \pmod{13}$ where $13 \nmid 8$

$\therefore\ x \equiv 8^{11} \times 3 \pmod{13}$

$\therefore\ x \equiv (8^2)^5 \times 24 \pmod{13}$

$\therefore\ x \equiv 64^5 \times (-2) \pmod{13}$

$\therefore\ x \equiv (-1)^5 \times (-2) \pmod{13}$ $\{65 = 13 \times 5\}$

$\therefore\ x \equiv 2 \pmod{13}$

c $7x \equiv 2 \pmod{11}$ where $11 \nmid 7$

$\therefore\ x \equiv 7^9 \times 2 \pmod{11}$

$\therefore\ x \equiv (7^2)^4 \times 14 \pmod{11}$

$\therefore\ x \equiv 49^4 \times 3 \pmod{11}$

$\therefore\ x \equiv 5^4 \times 3 \pmod{11}$

$\therefore\ x \equiv (25)^2 \times 3 \pmod{11}$

$\therefore\ x \equiv 3^2 \times 3 \pmod{11}$

$\therefore\ x \equiv 27 \pmod{11}$

$\therefore\ x \equiv 5 \pmod{11}$

d $4x \equiv 3 \pmod{17}$ where $17 \nmid 4$

$\therefore\ x \equiv 4^{15} \times 3 \pmod{17}$

$\therefore\ x \equiv (4^2)^7 \times 12 \pmod{17}$

$\therefore\ x \equiv 16^7 \times 12 \pmod{17}$

$\therefore\ x \equiv (-1)^7 \times 12 \pmod{17}$

$\therefore\ x \equiv -12 \pmod{17}$

$\therefore\ x \equiv 5 \pmod{17}$

3 **a** $2^{63} = (2^6)^{10} \times 2^3$

$= (64)^{10} \times 8$

$\equiv 1^{10} \times 8 \pmod{63}$

$\equiv 8 \pmod{63}$

$\not\equiv 2 \pmod{63}$ $\therefore$ 63 is not prime.

b $2^{117} = (2^7)^{16} \times 2^5$ $\{2^7 \equiv 128$ is close to $117\}$

$\equiv 11^{16} \times 2^5 \pmod{117}$

$\equiv 121^8 \times 2^5 \pmod{117}$

$\equiv 4^8 \times 2^5 \pmod{117}$

$\equiv 2^{21} \pmod{117}$

$\equiv (2^7)^3 \pmod{117}$

$\equiv 11^3 \pmod{17}$

$\equiv 121 \times 11 \pmod{117}$

$\equiv 4 \times 11 \pmod{117}$

$\equiv 44 \pmod{117}$

$\not\equiv 2 \pmod{117}$ $\therefore$ 117 is not prime.

c $2^{29} = (2^5)^5 \times 2^4$

$= 32^5 \times 16$

$\equiv 3^5 \times 16 \pmod{29}$

$\equiv 3^3 \times 3^2 \times 16 \pmod{29}$

$\equiv -2 \times 144 \pmod{29}$

$\equiv -2 \times -1 \pmod{29}$ $\{29 \times 5 = 145\}$

$\equiv 2 \pmod{29}$

This **does not** prove that 29 is a prime, as there exist Carmichael numbers which are composite and $a^n \equiv a \pmod n$.
{See note on page 84}

4 $3^{10} = (3^2)^5$

$= 9^5$

$\equiv (-2)^5 \pmod{11}$

$\equiv -32 \pmod{11}$

$\equiv 1 \pmod{11}$ $\{33 = 3 \times 11\}$

5 19 is prime and $19 \nmid 13$.

$\therefore$ $13^{18} \equiv 1 \pmod{19}$ {FLT} .... $(*)$

Thus $13^{133} + 5$

$= (13^{18})^7 \times 13^7 + 5$

$\equiv 1^7 \times 13^7 + 5 \pmod{19}$ {from $*$}

$\equiv (13^2)^3 \times 13 + 5 \pmod{19}$

$\equiv (-2)^3 \times 13 + 5 \pmod{19}$ $\{171 = 9 \times 19\}$

$\equiv -8 \times 13 + 5 \pmod{19}$

$\equiv -99 \pmod{19}$

$\equiv 15 \pmod{19}$

$\therefore$ the remainder is 15.

6 **a** 13 is a prime and $13 \nmid 11$

$\therefore$ $11^{12} \equiv 1 \pmod{13}$ {FLT} .... $(*)$

Thus $11^{204} + 1$

$= (11^{12})^{17} + 1$

$\equiv 1^{17} + 1 \pmod{13}$ {using $*$}

$\equiv 2 \pmod{13}$

$\not\equiv 0 \pmod{13}$

$\therefore$ $11^{204} + 1$ is not divisible by 13.

b 17 is a prime and $17 \nmid 11$

$\therefore$ $11^{16} \equiv 1 \pmod{17}$ {FLT} .... $(*)$

Thus $11^{204}+1$

$= (11^{16})^{12} \times 11^{12} + 1$

$\equiv 1^{12} \times (121)^6 + 1 \pmod{17}$ $\{$using $*\}$

$\equiv 2^6 + 1 \pmod{17}$ $\{17 \times 7 = 119\}$

$\equiv 65 \pmod{17}$

$\equiv 14 \pmod{17}$

$\not\equiv 0 \pmod{17}$

$\therefore$ $11^{204}+1$ is not divisible by 17.

7 **a** $13^{16n+2}+1$

$= (13^{16})^n \times 13^2 + 1$

$\equiv 1^n \times 169 + 1 \pmod{17}$ $\{$FLT$\}$

$\equiv 170 \pmod{17}$

$\equiv 0 \pmod{17}$

$\therefore$ $17 \mid (13^{16n+2}+1)$, $n \in \mathbb{Z}^+$.

b $9^{12n+4} - 9$

$= (9^{12})^n \times 9^4 - 9$

$\equiv 1^n \times (-4)^4 - 9 \pmod{13}$ $\{$FLT$\}$

$\equiv 247 \pmod{13}$

$\equiv 0 \pmod{13}$ $\{247 = 19 \times 13\}$

$\therefore$ $13 \mid (9^{12n+4} - 9)$, $n \in \mathbb{Z}^+$.

8 $7^{100} = (7^2)^{50}$

$= 49^{50}$

$\equiv (-1)^{50} \pmod{10}$

$\equiv 1 \pmod{10}$

$\therefore$ the units digit is 1.

Note: As 10 is not prime we cannot use FLT.

9 **a** If $x \equiv a^{p-2}b \pmod{p}$

then $ax \equiv a^{p-1}b \pmod{p}$

$\therefore$ $ax \equiv (1)b \pmod{p}$ $\{$FLT$\}$

$\therefore$ $ax \equiv b \pmod{p}$ is verified.

b **i** $7x \equiv 12 \pmod{17}$

$\therefore$ $x \equiv 7^{15} \times 12 \pmod{17}$

$\therefore$ $x \equiv (49)^7 \times 7 \times 12 \pmod{17}$

$\therefore$ $x \equiv (-2)^7 \times 84 \pmod{17}$ $\{17 \times 3 = 51\}$

$\therefore$ $x \equiv 32 \times -4 \times 84 \pmod{17}$

$\therefore$ $x \equiv -2 \times -4 \times -1 \pmod{17}$ $\{17 \times 5 = 85\}$

$\therefore$ $x \equiv -8 \pmod{17}$

$\therefore$ $x \equiv 9 \pmod{17}$

Also $4x \equiv 11 \pmod{19}$

$\therefore$ $x \equiv 4^{17} \times 11 \pmod{19}$

$\therefore$ $x \equiv 16^8 \times 4 \times 11 \pmod{19}$

$\therefore$ $x \equiv (-3)^8 \times 6 \pmod{19}$ $\{19 \times 2 = 38\}$

$\therefore$ $x \equiv (81)^2 \times 6 \pmod{19}$

$\therefore$ $x \equiv 5^2 \times 6 \pmod{19}$ $\{19 \times 4 = 76\}$

$\therefore$ $x \equiv 150 \pmod{19}$

$\therefore$ $x \equiv 17 \pmod{19}$ $\{19 \times 7 = 133\}$

Using the Chinese Remainder Theorem, for

$x \equiv 9 \pmod{17}$, $x \equiv 17 \pmod{19}$

$M = 17 \times 19 = 323$

$\therefore$ $M_1 = 19$, $M_2 = 17$.

Now $19x_1 \equiv 1 \pmod{17}$

$\Rightarrow$ $2x_1 \equiv 1 \pmod{17}$

$\Rightarrow$ $x_1 = 9$

and $17x_2 \equiv 1 \pmod{19}$

$\Rightarrow$ $-2x_2 \equiv 1 \pmod{19}$

$\Rightarrow$ $x_2 = 9$

$\therefore$ the solution is

$x \equiv a_1M_1x_1 + a_2M_2x_2 \pmod{323}$

$\therefore$ $x \equiv (9)(19)(9) + (17)(17)(9) \pmod{323}$

$\therefore$ $x \equiv 4140 \pmod{323}$

$\therefore$ $x \equiv 264 \pmod{323}$

ii $2x \equiv 1 \pmod{31}$

$\therefore$ $x \equiv 2^{29} \times 1 \pmod{31}$

$\therefore$ $x \equiv (2^5)^5 \times 2^4 \pmod{31}$

$\therefore$ $x \equiv 1^5 \times 16 \pmod{31}$

$\therefore$ $x \equiv 16 \pmod{31}$

and $6x \equiv 5 \pmod{11}$

$\therefore$ $x \equiv 6^9 \times 5 \pmod{11}$

$\therefore$ $x \equiv (6^2)^4 \times 30 \pmod{11}$

$\therefore$ $x \equiv 3^4 \times (-3) \pmod{11}$

$\therefore$ $x \equiv 3^3 \times -9 \pmod{11}$

$\therefore$ $x \equiv 5 \times 2 \pmod{11}$

$\therefore$ $x \equiv 10 \pmod{11}$

also $3x \equiv 17 \pmod{29}$

$\therefore$ $x \equiv 3^{27} \times 17 \pmod{29}$

$\therefore$ $x \equiv (3^3)^9 \times 17 \pmod{29}$

$\therefore$ $x \equiv (-2)^9 \times 17 \pmod{29}$

$\therefore$ $x \equiv -32 \times 16 \times 17 \pmod{29}$

$\therefore$ $x \equiv -3 \times 16 \times 17 \pmod{29}$

$\therefore$ $x \equiv -24 \times 34 \pmod{29}$

$\therefore$ $x \equiv 5 \times 5 \pmod{29}$

$\therefore$ $x \equiv 25 \pmod{29}$

Using the Chinese Remainder Theorem, as 31, 11, and 29 are relatively prime

$M = 31 \times 11 \times 29 = 9889$

$M_1 = 319$, $M_2 = 899$, $M_3 = 341$.

Now $319x_1 \equiv 1 \pmod{31}$

$\Rightarrow$ $9x_1 \equiv 1 \pmod{31}$

$\Rightarrow$ $x_1 = 7$

and $899x_2 \equiv 1 \pmod{11}$

$\Rightarrow$ $8x_2 \equiv 1 \pmod{11}$

$\Rightarrow$ $x_2 = 7$

and $341x_3 \equiv 1 \pmod{29}$

$\Rightarrow$ $22x_3 \equiv 1 \pmod{29}$

$\Rightarrow$ $x_3 = 4$

$\therefore$ $x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \pmod{9889}$

$\therefore$ $x \equiv (16)(319)(7) + (10)(899)(7)$

$+ (25)(341)(4) \pmod{9889}$

$\therefore$ $x \equiv 132\,758 \pmod{9889}$

$\therefore$ $x \equiv 4201 \pmod{9889}$

10 **a** Since p is an odd prime, then

$1 \leqslant k \leqslant p-1 \Rightarrow p \nmid k$

Thus $k^{p-1} \equiv 1 \pmod{p}$ $\{$FLT$\}$

$$\text{Hence}\quad \sum_{k=1}^{p-1} k^{p-1} \equiv \sum_{k=1}^{p-1} 1 \pmod p$$
$$\equiv p-1 \pmod p$$
$$\equiv -1 \pmod p$$

b Since p is an odd prime, then

$1 \leqslant k \leqslant p-1 \;\Rightarrow\; p \nmid k$

$\therefore\ k^p \equiv k \pmod p$ {Corollary of FLT}

$$\therefore\ \sum_{k=1}^{p-1} k^p \equiv \sum_{k=1}^{p-1} k \pmod p$$
$$\equiv 1+2+3+ \dots + (p-1) \pmod p$$
$$\equiv \frac{(p-1)(p)}{2} \pmod p$$
$$\equiv p\left(\frac{p-1}{2}\right) \pmod p$$
$$\equiv 0 \pmod p \qquad \left\{\text{as } p \text{ is odd, } \frac{p-1}{2} \in \mathbb{Z}^+\right\}$$

11 Suppose $3^{100} = a_n 7^n + a_{n-1}7^{n-1} + \dots + a_2 7^2 + a_1 7 + a_0$

then $3^{100} \pmod 7 = a_0$.

Now $3^{100} \pmod 7$

$$\equiv (3^6)^{16} \times 3^4 \pmod 7$$
$$\equiv 1^{16} \times 9 \times 9 \pmod 7 \qquad \{\text{FLT}\}$$
$$\equiv 2 \times 2 \pmod 7$$
$$\equiv 4 \pmod 7$$

$\therefore$ the last digit is 4.

12 **a** Since $\gcd(7, 11) = 1$ the FLT applies.

$7^{11} \equiv 7 \pmod{11}$

$7^{10} \equiv 1 \pmod{11}$

$7^3 \equiv 2 \pmod{11}$

$7^2 \equiv 5 \pmod{11}$

$\therefore\ X \equiv t(7) + 4(1) + (6-t)(2) + 2t(5) + 7t$
$\quad + 3 \pmod{11}$

$\therefore\ X \equiv 7t + 4 + 12 - 2t + 10t + 7t + 3 \pmod{11}$

$\therefore\ X \equiv 22t + 19 \pmod{11}$

$\therefore\ X \equiv 8 \pmod{11}$

$\therefore\ x_0 = 8.$

b If $t = 1$

$X = 7^{11} + 4 \times 7^{10} + 5 \times 7^3 + 2 \times 7^2 + 7 + 3$

$\therefore\ X = 3\,107\,229\,562_{10}$

11	3 107 229 562	r
11	282 475 414	8
11	25 679 583	1
11	2 334 507	6
11	212 227	10
11	19 293	4
11	1753	10
11	159	4
11	14	5
	1	3

$\therefore\ X = (1\,3\,5\,4\,(10)\,4\,(10)\,6\,1\,8)_{11}$

13 **a** Let $N = (a_n a_{n-1} \dots a_2 a_1 a_0)_{14}$

$\therefore\ N = a_n 14^n + a_{n-1}14^{n-1} + \dots + a_2 14^2$
$\quad + a_1 14 + a_0$

$\therefore\ N = 14A + a_0$ for some $A \in \mathbb{Z}$

$\therefore\ N \equiv a_0 \pmod{14}$

$\therefore\ N^7 \equiv a_0^{\,7} \pmod{14}$ .... (1)

Now $a_0 \equiv 0, 1 \pmod 2$

$\therefore\ a_0^{\,7} \equiv 0^7, 1^7 \pmod 2$

$\therefore\ a_0^{\,7} \equiv 0, 1 \pmod 2$

$\therefore\ a_0^{\,7} \equiv a_0 \pmod 2$ .... (2)

and $a_0^{\,7} \equiv a_0 \pmod 7$ .... (3) {Corollary of FLT}

From (2) and (3),

$a_0^{\,7} - a_0 \equiv 0 \pmod{2 \text{ and } \bmod 7}$

$\therefore\ 2 \mid (a_0^{\,7} - a_0)$ and $7 \mid (a_0^{\,7} - a_0)$

$\therefore\ 14 \mid (a_0^{\,7} - a_0)$ {as $\gcd(2, 7) = 1$}

$\therefore\ a_0^{\,7} \equiv a_0 \pmod{14}$

$\therefore\ N^7 \equiv a_0 \pmod{14}$ {using (1)}

As $N \equiv a_0 \pmod{14}$ and $N^7 \equiv a_0 \pmod{14}$, both N and N^7 have last digit a_0 in base 14.

b Let $N = (a_n a_{n-1} \dots a_2 a_1 a_0)_{21}$

$\therefore\ N = 21B + a_0$ for some $B \in \mathbb{Z}$

$\therefore\ N \equiv a_0 \pmod{21}$

$\therefore\ N^7 \equiv a_0^{\,7} \pmod{21}$ .... (1)

Now $a_0 \equiv 0, 1, \text{ or } 2 \pmod 3$

$\therefore\ a_0^{\,7} \equiv 0^7, 1^7, \text{ or } 2^7 \pmod 3$

$\therefore\ a_0^{\,7} \equiv 0, 1, \text{ or } 128 \pmod 3$

$\therefore\ a_0^{\,7} \equiv 0, 1, \text{ or } 2 \pmod 3$

$\therefore\ a_0^{\,7} \equiv a_0 \pmod 3$ .... (2)

and $a_0^{\,7} \equiv a_0 \pmod 7$ .... (3) {Corollary to FLT}

$\therefore$ from (2) and (3),

$3 \mid (a_0^{\,7} - a_0)$ and $7 \mid (a_0^{\,7} - a_0)$

$\therefore\ 21 \mid (a_0^{\,7} - a_0)$ {as $\gcd(3, 7) = 1$}

$\therefore\ a_0^{\,7} \equiv a_0 \pmod{21}$

$\therefore\ N^7 \equiv a_0 \pmod{21}$ {using (1)}

As $N \equiv a_0 \pmod{21}$ and $N^7 \equiv a_0 \pmod{21}$ both N and N^7 have last digit a_0 in base 21.

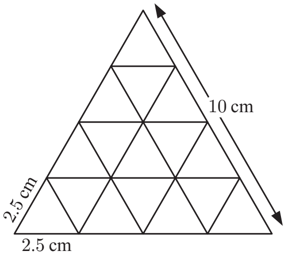
EXERCISE 1J

1 There are 12 months in a year, so by the Pigeonhole Principle there will be at least one month (pigeonhole) which is the birth month of two or more people (pigeons).

2 Divide the dartboard into 6 equal sectors. The maximum distance between any two points in a sector is 10 cm. Since there are 7 darts, at least two must be in the same sector (Pigeonhole Principle). Hence there are two darts which are at most 10 cm apart.

3 Divide the equilateral triangle into 16 identical triangles as shown. The length of each side of the small triangles is 2.5 cm.

If there are 17 points, then at least two must be in the same triangle (Pigeonhole Principle). Hence, there are at least two points which are at most 2.5 cm apart.



4 Suppose they each receive a different number of prizes. Since each child receives at least one prize, the smallest number of prizes there can be is

$1+2+3+4+5+6+7+8+9+10 = 55.$

But there are only 50 prizes. Hence, at least two children must receive the same number.

5 The pairs of numbers 1 & 12, 2 & 11, 3 & 10, 4 & 9, 5 & 8, 6 & 7 all add up to 13. Consider the three numbers which are *not* selected. These can come from at most 3 of the pairs. Hence, there are at least 3 pairs for which both numbers are selected.

6 The maximum number of days in a year is 366. So if 367 or more are present this will ensure that at least two people present have the same birthday.

$\therefore$ the minimum number of people needed = 367. {PHP}

7 **a** There are 2 different colours, so selecting 3 socks will ensure that 2 of the socks are the same colour.

b It is possible that if we select 14 socks all of them could be white.

$\therefore$ if we select 15 this will ensure that two different colours will be selected. {PHP}

8 There are 26 letters in the English alphabet and $27 > 26$. Therefore, at least two words will start with the same letter. {PHP}

9 $\dfrac{90\,000}{366} \approx 245.9$.

$\therefore$ by the PHP there will be a group of 246 people who have the same birthday.

10 The pairs with sum 11 are:

$\{1, 10\}, \{2, 9\}, \{3, 8\}, \{4, 7\}, \{5, 6\}$.

This set of subsets of $\{1, 2, 3, 4, ..., 10\}$ partition the integers $1, 2, 3, 4, ..., 10$.

If the subsets are the pigeonholes and we select any 6 distinct numbers (pigeons) then there will be two such numbers with a sum of 11.

11 A units digit could be one of 10 possibilities, $0, 1, 2, 3, ..., 9$. Let these possibilities be pigeonholes.

If we select 11 integers and place then into a pigeonhole corresponding to its units digit, then by the PHP at least one pigeonhole contains two of the integers and so at least two of them will have the same units digit.

12 Suppose there are $n \geqslant 2$ people at a cocktail party.

Case (1) (Each person has at least 1 acquaintance.)

Each person has $1, 2, 3, 4, ..., n-1$ acquaintances. If these values are the pigeonholes, we place each person in a pigeonhole corresponding to their number of acquaintances.

Since $n > n-1$, by the PHP, there will be two people in the same pigeonhole, that is, with the same number of acquaintances.

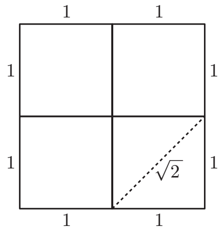
Case (2) (Someone has no acquaintances.)

Each other person can have at most $n-2$ acquaintances at the party.

Thus each of the other $n-1$ people have $1, 2, 3, ..., \text{or } n-2$ acquaintances. We let these $n-2$ values be the pigeonholes.

Then, by the PHP, since $n-1 > n-2$ there will be two people who have the same number of acquaintances.

13



We divide the square into 4 squares which are 1 unit by 1 unit and let these smaller squares be the pigeonholes.

If 5 ($>$ 4) points are arbitrarily placed inside the 2×2 square then by the PHP one smaller square will contain at least two points.

The distance between these points is at most the length of a diagonal of a small square, which is $\sqrt{2}$ units.

$\therefore$ the distance between these two points is at most $\sqrt{2}$ units.

14 Let their test scores 7, 6, 5, or 4 be the pigeonholes. Since there are 25 students and 4 pigeonholes, one pigeonhole contains at least $\frac{25}{4} = 6.25$ students. So, there exists one pigeonhole containing at least 7 students. Thus it is guaranteed that there will be 7 students having the same score.

(Although possible, no greater number can be guaranteed.)

15 There are infinitely many powers of 2 (the pigeons). The 2001 residue classes modulo 2001 are the pigeonholes.

By the PHP there will be two powers of 2 in the same residue class, and they will differ by a multiple of 2001.

16 **a** The 'worst case' is when the red balls are selected last.

$\therefore$ least number $= 8 + 10 + 7 + \underset{\substack{\uparrow\\ \text{red}}}{3} = 28$.

b The 'worst case' is when two of each colour are selected first.

$\therefore$ least number $= 2 + 2 + 2 + 2 + 1 = 9$.

c The 'worst case' is when all green and blue balls are selected first.

$\therefore$ least number $= 10 + 8 + 1 \text{ other} = 19$.

17 **a** When 3 dice are rolled the possible totals are

$\underset{\substack{\uparrow\\ \text{three 1s}}}{3}, 4, 5, 6, 7, ...,\underset{\substack{\uparrow\\ \text{three 6s}}}{18}.$

So, there are 16 different totals.

$\therefore$ by the PHP, 17 rolls are needed to guarantee a repeated total.

b The 'worst case' is when each total appears twice first.

$\therefore$ least number $= 16 \times 2 + 1 = 33$ rolls.

EXERCISE 2A

1 **a** **i** 4 **ii** 4 **iii** 2, 2, 2, 2

b **i** 4 **ii** 6 **iii** 2, 3, 3, 4

c **i** 4 **ii** 6 **iii** 2, 2, 4, 4

d **i** 2 **ii** 1 **iii** 1, 1

e **i** 5 **ii** 4 **iii** 1, 1, 2, 2, 2

f **i** 6 **ii** $5 + 4 + 3 + 2 + 1 = 15$

iii 5, 5, 5, 5, 5, 5

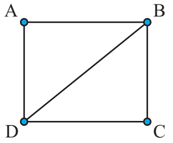
2 **i** Simple: **a**, **d**, **e**, **f**.

ii Connected: **a**, **b**, **c**, **d**, **f**.

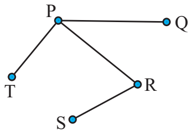
iii Complete: **d**, **f**. {**f** is complete K_6}

3 **a** **Note:** These are *examples only.*

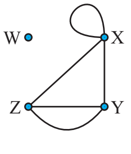
i



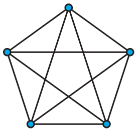
ii



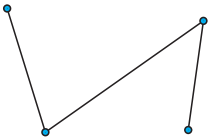
iii



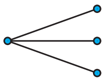
iv



v



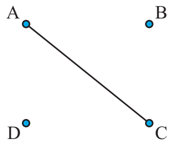
b yes, for example



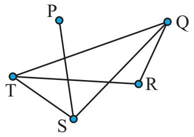
c (1) **i**, **ii**, **iv**, **v** are simple. **(2)** **i**, **ii**, **iv**, **v** are connected.

(3) **iv** is complete.

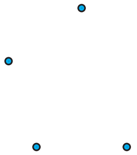
d **i**



ii

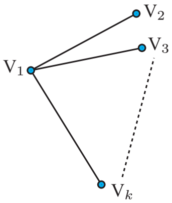


iv



(Called a null graph on 5 vertices.)

4 **a** A simple connected graph of order k can be constructed by joining one vertex to each of the other $(k-1)$ vertices. So, the minimum number of edges is $k-1$.



b Since each edge is determined by a pair of vertices, the number of edges in a complete graph on n vertices (K_n)

$$= \binom{n}{2}$$

$$= \frac{n(n-1)}{2}$$

As the complement of K_n is the null graph on n vertices, it has no edges.

$\therefore$ it has size 0.

c Size of complement $= \binom{n}{2} - e$ or $\frac{n(n-1)}{2} - e$.

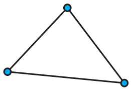
d From **a** and **b**, $e \geqslant n-1$ and $e \leqslant \frac{n(n-1)}{2}$

(if any more edges are added to a complete graph, it is no longer simple.)

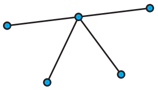
$$\therefore \quad n-1 \leqslant e \leqslant \frac{n(n-1)}{2}$$

$$\therefore \quad 2n-2 \leqslant 2e \leqslant n^2 - n$$

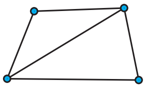
5 **a**



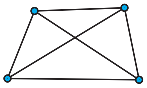
$$\begin{aligned} &\sum \deg(V_i) \\ &= 2+2+2 \\ &= 6 \\ &= 2 \times 3 \\ &= 2e \end{aligned}$$



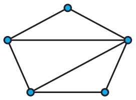
$$\begin{aligned} &\sum \deg(V_i) \\ &= 1+1+1+1+4 \\ &= 8 \\ &= 2 \times 4 \\ &= 2e \end{aligned}$$



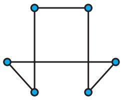
$$\begin{aligned} &\sum \deg(V_i) \\ &= 2+2+3+3 \\ &= 10 \\ &= 2 \times 5 \\ &= 2e \end{aligned}$$



$$\begin{aligned} &\sum \deg(V_i) \\ &= 3+3+3+3 \\ &= 12 \\ &= 2 \times 6 \\ &= 2e \end{aligned}$$



$$\begin{aligned} &\sum \deg(V_i) \\ &= 2+2+3+3+4 \\ &= 14 \\ &= 2 \times 7 \\ &= 2e \end{aligned}$$



$$\begin{aligned} &\sum \deg(V_i) \\ &= 2+2+2+2+2+2 \\ &= 12 \\ &= 2 \times 6 \\ &= 2e \end{aligned}$$

Proposition: $\sum \deg(V_i) = 2e \qquad \{e = \text{size}\}$

Proof:

If V is a vertex and E is an edge incident with V, we count the pairs (V, E) in two different ways.

(1) As each vertex V_i is incident with $\deg(V_i)$ edges, the number of pairs (V, E) $= \sum \deg(V_i)$.

(2) As each edge is incident with 2 vertices, the number of pairs (V, E) $= 2e$

$\therefore \sum \deg(V_i) = 2e. \qquad$ {(1) and (2)}

b

$$\begin{aligned} \sum \deg(V_i) &= 2e \\ \therefore \quad 1+2+2+3+4+5+5 &= 2e \\ \therefore \quad 2e &= 22 \\ \therefore \quad e &= 11 \end{aligned}$$

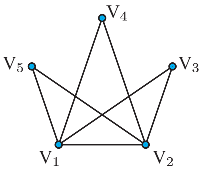
6 $\sum \deg(V_i) = 1+2+3+4+4+5$

$\therefore$ $2e = 19$ which is impossible as $e \in \mathbb{N}$.

7 **a** For a graph to be simple, no vertex can have degree more than $n-1$. Here the order is 5, so we cannot have a vertex of degree 5.

$\therefore$ **no** simple graph exists.

b



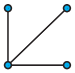
$\deg(V_1) = \deg(V_2) = 4$

$\therefore \deg(V_i) \geqslant 2$ for $i = 3, 4, 5$ and as the degree sequence contains 1, the degree sequence is not possible

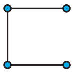
$\therefore$ **no** simple graph exists.

8 **a** **Yes**, the order is the number of values in the degree sequence, and the size is the sum of the degrees of the vertices, divided by 2.

b **No**. For example consider:



and

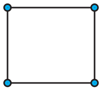


These graphs each have order 4 and size 3 but have different degree sequences.

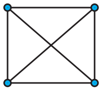
{1, 1, 1, 3 and 1, 1, 2, 2}

9 **Note:** These are examples only.
More than one answer is possible.

a

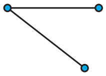


b

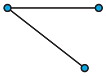


c Impossible as the sum of the degrees must be even.

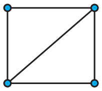
d



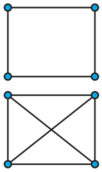
e



f



10



Graph is 2-regular

$p = 4,\ q = 4,\ r = 2;\quad q = \frac{pr}{2}$

$p = 4,\ q = 6,\ r = 3;\quad q = \frac{pr}{2}$

Proof: $\sum \deg(V_i) = 2e = 2q$

But $\sum \deg(V_i)$

$= \text{number of vertices} \times r$

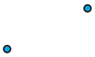
$= \text{order} \times r$

$= pr$

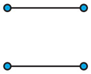
Thus, $2q = pr$

$\therefore\ q = \frac{pr}{q}.$

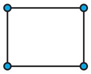
11 **a**



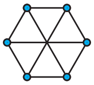
b



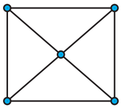
c



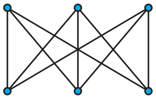
d



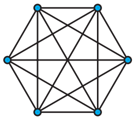
12 **a** W_5



b $K_{3,\,3}$

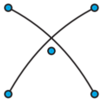


c K_6

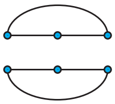


Complements are:

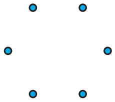
a



b



c



13 **a** Number of edges for $K_{10} = \frac{10 \times 9}{2} = 45$

b Number of edges for $K_{5,\,3} = 5 \times 3 = 15$

c Number of edges for W_8

$= \text{sum of outer and inner edges}$

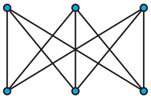
$= 2 \times 7$

$= 14$

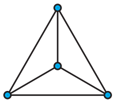
d Number of edges for $K_n = \frac{n(n-1)}{2}$

e Number of edges for $K_{m,\,n} = mn$

14 **a**

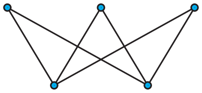


b



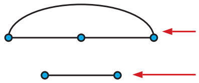
c Not possible

15



$K_{3,\,2}$ has $3 \times 2 = 6$ edges

Its complement is



this is K_3

this is K_2

and has size $3 + 1 = 4$.

The complement of $K_{m,\,n}$ is the disconnected graph containing the subgraphs K_m and K_n

$$\therefore\ \text{has size} = \frac{m(m-1)}{2} + \frac{n(n-1)}{2}$$
$$= \frac{m(m-1) + n(n-1)}{2}.$$

16 G has n vertices and e edges, $n = e$.

G' also has e edges {given}

and G' has $\frac{n(n-1)}{2} - e$ edges {from **4 c**}

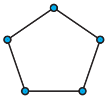
$$\therefore\ e = \frac{n(n-1)}{2} - e$$
$$\therefore\ 2e = \frac{e^2 - e}{2} \qquad \{n = e\}$$
$$\therefore\ 4e = e^2 - e$$
$$\therefore\ e^2 - 5e = 0$$
$$\therefore\ e(e-5) = 0$$
$$\therefore\ e = 0 \text{ or } 5$$

<u>If $n = e = 0$</u>

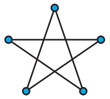
this is when $G = G' =$ the null graph with no edges or vertices.

<u>If $n = e = 5$</u> then for example

G:



and G':



17 **a** If G has order n, G' has order n also

$\therefore$ order (G) + order of $(G') = 2n$.

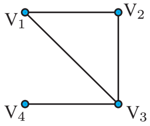
b If G has size e, G' has size $\binom{n}{2} - e$ {from **4 c**}

$\therefore$ size (G) + size $(G') = \binom{n}{2}$ $\left(\text{or } \frac{n(n-1)}{2}\right)$

EXERCISE 2B

1 **a** Can represent a graph.

For example,

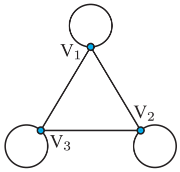


where
$\deg(V_1) = 2$
$\deg(V_2) = 2$
$\deg(V_3) = 3$
$\deg(V_4) = 1$

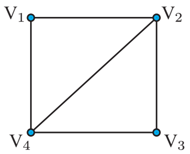
b Cannot represent a graph as the table is not symmetric about its main diagonal.

c Can represent a graph.

For example,



2



Total number of 1s

$= 2 + 3 + 2 + 3$

$= 10$

$\sum \deg(V_i) = 2 + 3 + 2 + 3$

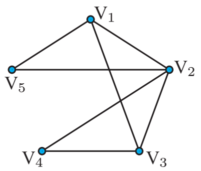
$= 10$ ✓

3 **a**
$$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

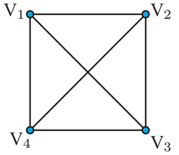
b
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

c
$$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

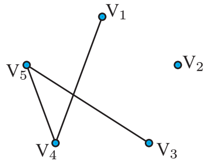
4 **a** **i**



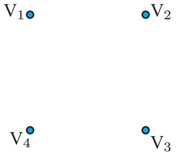
ii



b **i**



ii



$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

c Copy the adjacency table for G and

- keep the main diagonal
- everywhere else swap 0 and 1. That is, $0 \leftrightarrow 1$.

5 **a** Sum of all entries $= 2e$

$\therefore\ 3 + 3 + 3 + 2 + 3 = 2e$

$\therefore\ 2e = 14$

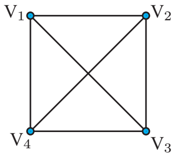
$\therefore\ e = 7$

b Sum of elements on or below main diagonal $= e$

$\therefore\ 3 + 1 + 2 + 3 + 5 = e$

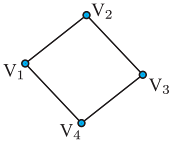
$\therefore\ e = 14$

6 **a** K_4



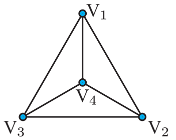
$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

b C_4



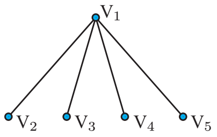
$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

c W_4



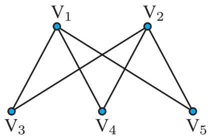
$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

d $K_{1,\,4}$



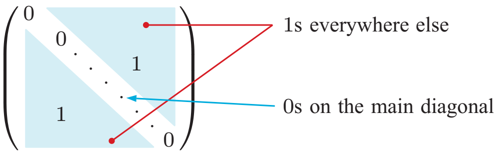
$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

e $K_{2,\,3}$

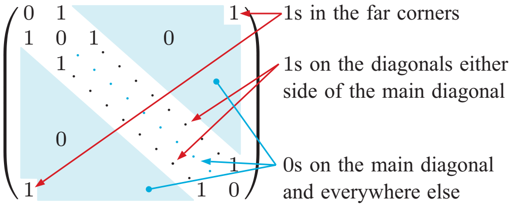


$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

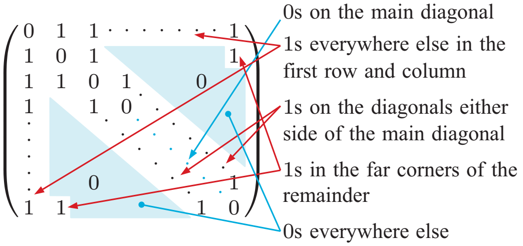
7 **a** $n \times n$ table with:



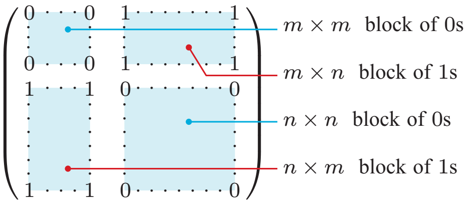
b $n \times n$ table with:


0 1 1
1 0 1 0
1
0
1
1 1 0
1s in the far corners
1s on the diagonals either side of the main diagonal
0s on the main diagonal and everywhere else

c $n \times n$ table with (for example):


0 1 1 1
1 0 1 1
1 1 0 1 0
1 1 0
0
1
1 1 1 0
0s on the main diagonal
1s everywhere else in the first row and column
1s on the diagonals either side of the main diagonal
1s in the far corners of the remainder
0s everywhere else

d $(m + n) \times (m + n)$ table with:



EXERCISE 2C.1

1 These are **examples only**.

a A → C → D

b A → B → C → D

c A → B → C → E → D

d B → C → A → E → C → D

e F ⟶ E ⟶ A ⟶ C ⟶ D ⟶ F

f Impossible, a cycle of length 7 requires 7 distinct vertices.

g A ⟶ B ⟶ C ⟶ A ⟶ E ⟶ F ⟶ D ⟶ A

h F ⟶ E ⟶ A ⟶ C ⟶ E ⟶ D ⟶ C ⟶ B ⟶ A ⟶ D ⟶ F

2 **a** E ⟶ C ⟶ A ⟶ A ⟶ B ⟶ C ⟶ B ⟶ D ⟶ C

b Impossible, for example we cannot include edge EC without traversing it twice.

EXERCISE 2C.2

1 **a** Each vertex is even.
$\therefore$ the graph is Eulerian.

b The graph contains exactly two odd vertices.
$\therefore$ it is semi-Eulerian.

c The graph contains more than two odd vertices.
$\therefore$ it is neither Eulerian nor semi-Eulerian.

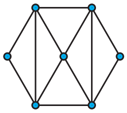
d The graph contains more than two odd vertices.
$\therefore$ it is neither Eulerian nor semi-Eulerian.

e The graph contains exactly two odd vertices.
$\therefore$ it is semi-Eulerian.

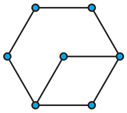
f The graph contains more than two odd vertices.
$\therefore$ it is neither Eulerian nor semi-Eulerian.

2 **Note:** These are examples only.

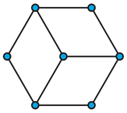
a



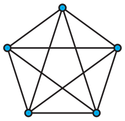
b



c

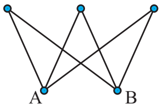


3 **a** K_5



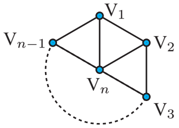
All vertices have degree 4, and the graph is connected. Thus all vertices are even and hence K_5 is Eulerian.

b $K_{2,\,3}$



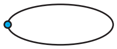
Exactly two vertices have odd degree (A and B)
$\therefore$ $K_{2,\,3}$ is semi-Eulerian.

c W_n

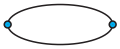


All outer vertices $V_1, V_2, V_3, ..., V_{n-1}$ have odd degree.

Since W_n is defined only for $n \geqslant 4$, W_n always has at least $n-1 \geqslant 3$ odd vertices.
$\therefore$ W_n is neither Eulerian nor semi-Eulerian.

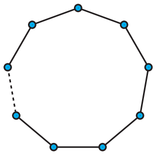
d C_m: C_1 is , one even vertex.

$\therefore$ C_1 is Eulerian.

C_2 is , two even vertices.

$\therefore$ C_2 is Eulerian.

In C_m where $m \geqslant 3$,



Every vertex is even.
{degree 2}
$\therefore$ C_m, $m \geqslant 3$ is Eulerian.

So, C_m is Eulerian for all $m \in \mathbb{Z}^+$.

4 **a** K_n has n vertices each of degree $n-1$.
So, when $n-1$ is even, K_n is Eulerian
$\therefore$ K_n is Eulerian $\Leftrightarrow$ n is odd for $n \geqslant 3$.

b In $K_{m,\,n}$, each vertex has degree m or n.
$\therefore$ $K_{m,\,n}$ is Eulerian $\Leftrightarrow$ m and n are even.

5 **a** Since there are only five vertices, each vertex has degree $\leqslant 4$. That is, $0 \leqslant d \leqslant 4$.
From **Exercise 2A** question **5**,

$\sum \deg(G) = 2e$ $\{e = \text{number of edges}\}$

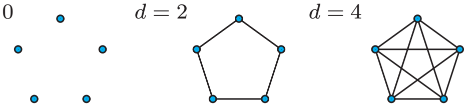
$\therefore$ $5d = 2e$

$\therefore$ $2 \mid d$ {and $5 \mid e$ as 2, 5 are primes}

$\therefore$ $d = 0$, 2, or 4

Each of these exist:

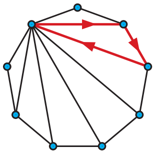
$d = 0$ $d = 2$ $d = 4$



b If G is connected, $d = 2$ or 4.

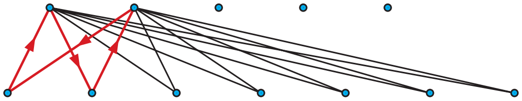
c If G is Eulerian, G is connected and all vertices are even
$\therefore$ $d = 2$ or 4.

6 **a**



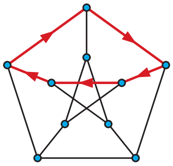
girth
$=$ length of shortest cycle
$= 3$

b



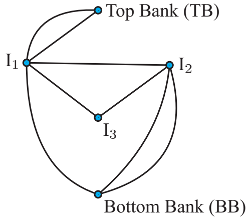
girth $= 4$

c



girth $= 5$

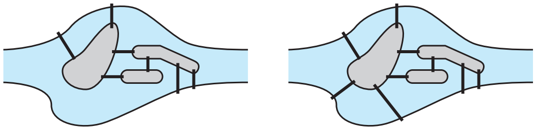
7 **a**



has 1 vertex of order 5, 1 of order 4, 1 of order 3, 2 of order 2.

$\therefore$ it does not have all vertices of even degree
$\therefore$ the circuit is not Eulerian
$\therefore$ a circular walk cannot be performed.

b Removing the bridge from I_1 to BB or adding another bridge from I_1 to BB will create a circuit diagram which is Eulerian (all vertices are now even).



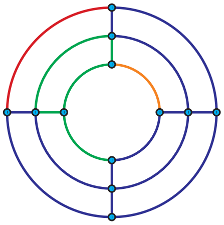
8 For any graph G, the sum of the degrees of the vertices is even.

$\therefore$ there must be an even number of vertices of odd degree.

We can add an edge between any pair of vertices with odd degree, thus reducing the number of vertices with odd degree by 2. We repeat until all vertices have even degree.

Thus, as we obtain a connected graph with all vertices of even degree, the graph G is Eulerian.

9 **a** 4 pen strokes are needed. An example is shown alongside.



b If a graph has 2 vertices of odd degree, it is semi-Eulerian, and the graph can be drawn with a single pen stroke.

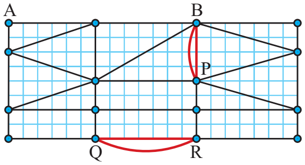
This graph has 8 vertices of odd degree, so we could make the graph semi-Eulerian by adding 3 new edges to the graph.

Equivalently, we can think of adding an edge between two vertices as lifting the pen at one vertex and moving it to the other.

So, an additional 3 pen strokes are required to complete the diagram, making 4 in total.

10 **a** There are 4 vertices of odd degree. These are B, P, Q, and R.

$\therefore$ no matter where we start including A or B the graph is not traversable.



b If we add two new edges BP and QR as shown, the graph obtained is connected with all vertices having even degree. Thus the new graph is Eulerian and so contains an Eulerian circuit starting and ending at any vertex, including A and B.

This is interpreted as:

The most efficient method of traversing all streets, starting and ending at A is to use an Eulerian circuit (which exists by the above reasoning), that traverses BP and QR twice.

11 ($\Rightarrow$) Suppose the graph is bipartite, so there are two disjoint vertex sets A and B. Suppose we are at a particular vertex in set A. In order to form a circuit back to this vertex, we must move to set B then back to set A, and repeat this a certain number of times. Each trip from set A to set B and back adds 2 to the length of the circuit.

Hence, the circuit must have even length.

($\Leftarrow$) Suppose the simple graph contains only even length circuits.

If we choose any vertex $\text{V} \in V(G)$, then we can define sets of vertices:

Set A is the set of vertices with paths of odd length to V.

Set B is the set of vertices with paths of even length to V.

Now if any vertex W belongs to both sets A and B, then there must exist an odd length circuit in the graph. This is a contradiction, so A and B are disjoint sets.

Now suppose vertices $\text{X}, \text{Y} \in A$ are adjacent

$\therefore$ there must exist a path of even length from Y to V via X.

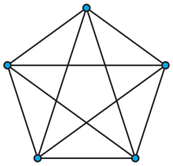
$\therefore$ $\text{Y} \in B$ which is a contradiction since A and B are disjoint.

$\therefore$ no two vertices in set A are adjacent.

Similarly, no two vertices in set B are adjacent.

$\therefore$ the graph is bipartite.

12 Consider K_5, say



Total number of edges

$$= \binom{5}{2}$$

$$= \frac{5 \times 4}{2}$$

and K_4 has $\dfrac{4 \times 3}{2}$ edges.

Thus, any simple subgraph of 4 vertices has at most $\dfrac{4 \times 3}{2}$ edges.

So, if G has more than $\dfrac{4 \times 3}{2}$ edges, the 5th vertex must be connected by an edge to the subgraph K_4.

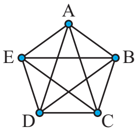
In general, K_n has $\dfrac{n(n-1)}{2}$ edges and K_{n-1} has $\dfrac{(n-1)(n-2)}{2}$ edges.

Thus in a graph G on n vertices, any subgraph on $(n-1)$ vertices has at most $\dfrac{(n-1)(n-2)}{2}$ edges.

Thus if G has more than $\dfrac{(n-1)(n-2)}{2}$ edges, the nth vertex must be connected by an edge to the subgraph containing the remaining vertices.

EXERCISE 2C.3

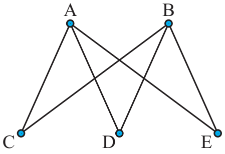
1 **a** K_5



There exists a cycle through each vertex. For example, A → B → C → D → E → A.

$\therefore$ K_5 is Hamiltonian.

b



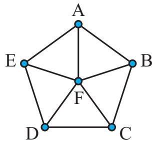
There does not exist a cycle through each vertex.

$\therefore$ $K_{2,\,3}$ is not Hamiltonian.

But D → B → E → A → C is a path which passes through each vertex exactly once.

$\therefore$ $K_{2,\,3}$ is semi-Hamiltonian.

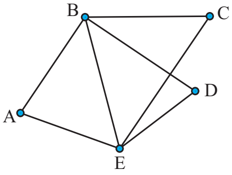
c



F → A → B → C → D → E → F is a path through every vertex.

$\therefore$ W_6 is Hamiltonian.

d



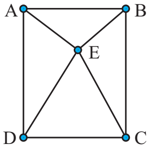
There does not exist a cycle through each vertex.

$\therefore$ the graph is not Hamiltonian.

But A → B → C → E → D is a path through every vertex.

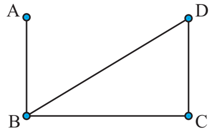
$\therefore$ the graph is semi-Hamiltonian.

e



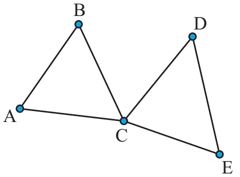
A → B → C → D → E → A is a cycle through every vertex.
∴ the graph is Hamiltonian.

f



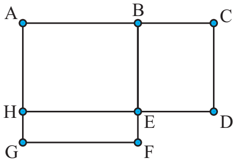
There does not exist a cycle through each vertex.
∴ the graph is not Hamiltonian.
But A → B → C → D is a path through every vertex.
∴ the graph is semi-Hamiltonian.

g



There does not exist a cycle through each vertex.
∴ the graph is not Hamiltonian.
But A → B → C → D → E is a path through every vertex.
∴ the graph is semi-Hamiltonian.

h



A → B → C → D → E → F → G → H → A is a cycle through each vertex.
∴ the graph is Hamiltonian.

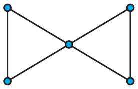
2

	a	b	c	d	e	f	g	h
Theorem 1	✓	✗	✓	✗	✓	✗	✗	✗
Theorem 2	✓	✗	✓	✗	✓	✗	✗	✗
Theorem 3	✓	✗	✗	✗	✓	✗	✗	✗

3 **Note:** These are examples only.

a C_n for all $n \geqslant 3$ **b** W_n for all $n \geqslant 4$

c



d $K_{2,\,3}$

4 m and n must be equal and $m, n \geqslant 2$.

5 **a** K_n has n vertices, each with degree $n - 1$.
From the observation of Dirac, a Hamiltonian cycle exists if $n - 1 \geqslant \frac{1}{2}n, \Rightarrow$ if $n \geqslant 2$
However, K_2 is not Hamiltonian. (Dirac requires $n \geqslant 3$.)
So, K_n contains a Hamiltonian cycle for all $n \geqslant 3$.

b The number of Hamiltonian cycles in K_n

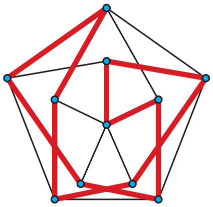
$$= \frac{\text{number of orderings of } n \text{ vertices}}{\underbrace{\text{number of choices for initial vertex}}_{\text{since it is a cycle}} \times 2}$$

since the graph is undirected, clockwise ordering gives the same cycle as anticlockwise

$$= \frac{n!}{n \times 2}$$

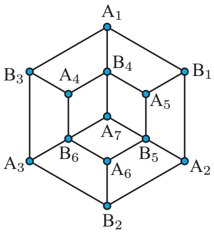
$$= \frac{(n-1)!}{2}$$

6



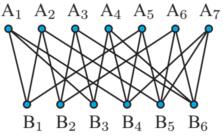
7 **a** From **Exercise 2C.2**, question **11**, a simple graph is bipartite if and only if each of its circuits is of even length.
∴ if a bipartite graph has an odd number of vertices, it cannot contain a circuit visiting *every* vertex.
∴ G cannot be Hamiltonian.

b



If we label each vertex either A or B, we can show that the graph is bipartite.

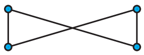
becomes


A_1 A_2 A_3 A_4 A_5 A_6 A_7
B_1 B_2 B_3 B_4 B_5 B_6

Since there are 13 vertices, which is an odd number, the graph is not Hamiltonian.

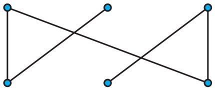
c If each square on a chessboard is represented by a vertex, and vertices are adjacent if a knight can move between them, then the resulting graph is bipartite. The white squares and the black squares form the two disjoint sets. If n is odd then $n \times n$ is also odd. Hence no Hamiltonian cycle exists.
Note: If n is even, a Hamiltonian cycle still does not necessarily exist!

d **i** $K_{2,\,2}$:



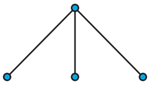
is Hamiltonian.

ii



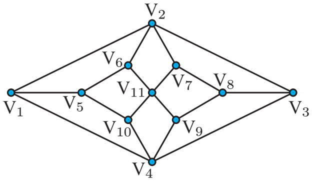
is semi-Hamiltonian but not Hamiltonian.

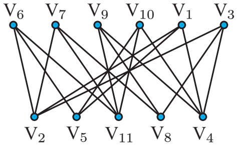
iii $K_{1,\,3}$:



is not Hamiltonian and not semi-Hamiltonian.

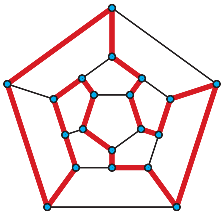
8




V_6 V_7 V_9 V_{10} V_1 V_3
V_2 V_5 V_{11} V_8 V_4

∴ the graph is bipartite with an odd number of vertices.
∴ the graph is not Hamiltonian.

9 For example,



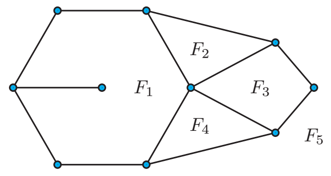
EXERCISE 2D.1

1 **a** $v = 10$

b $e = 13$

c $f = 5$

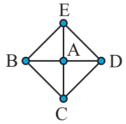
d



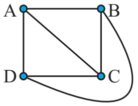
$\deg(F_1) = 8$, $\deg(F_2) = 3$,
$\deg(F_3) = 4$, $\deg(F_4) = 3$,
$\deg(F_5) = 8$

2 For example:

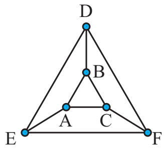
a



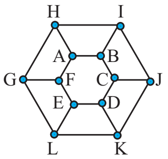
b



c

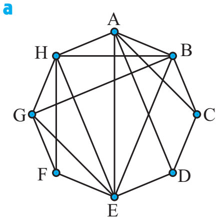


d

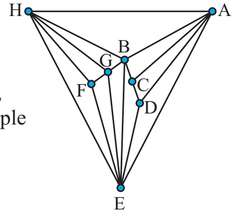


3 **a, b** No, the problem cannot be solved on any surface.

4 **a**

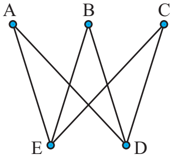


becomes, for example

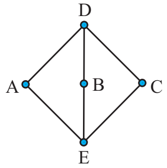


b non-planar

c

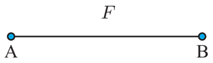


becomes, for example



d non-planar

5 **a**

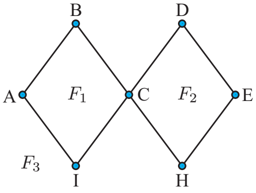


i A → B → A (2)

ii $\deg(F) = 2$

iii $\sum \deg(F) = 2$
$= 2 \times 1$
$= 2e$

b

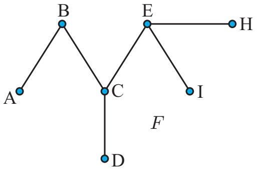


i A → B → C → D → E → H → C → I → A (8)

ii $\deg(F_1) = \deg(F_2) = 4$
$\deg(F_3) = 8$

iii $\sum \deg(F) = 4 + 4 + 8$
$= 16$
$= 2 \times 8$
$= 2e$

c

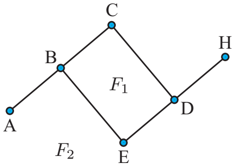


i H → E → I → E → C → D → C → B → A → B → C → E → H (12)

ii $\deg(F) = 12$

iii $\sum \deg(F) = 12$
$= 2 \times 6$
$= 2e$

d

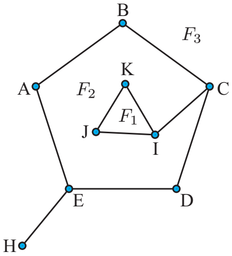


i A → B → E → D → H → D → C → B → A (8)

ii $\deg(F_1) = 4$,
$\deg(F_2) = 8$

iii $\sum \deg(F) = 4 + 8$
$= 12$
$= 2 \times 6$
$= 2e$

e



i H → E → A → B → C → D → E → H (7)

ii $\deg(F_1) = 3$,
$\deg(F_2) = 10$,
$\deg(F_3) = 7$

iii $\sum \deg(F) = 3 + 10 + 7$
$= 20$
$= 2 \times 10$
$= 2e$

6 Each edge is either on the border of one or more finite faces
or only on the border of the infinite face.

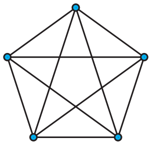
$\therefore$ each edge contributes
either 1 to the degree of two different faces
or 2 to the degree of the infinite face.

$\therefore$ each edge contributes 2 to the sum of the degrees of the faces.

$$\therefore \sum_{F \text{ a face of } G} \deg(F) = 2e.$$

EXERCISE 2D.2

1 K_5



$e = 10$, $v = 5$
Suppose K_5 is planar.
As K_5 is connected, by Euler's formula,
$e + 2 = f + v$
$\therefore f = 10 + 2 - 5$
$\therefore f = 7$

Since $v \geqslant 3$, $\deg(F_i) \geqslant 3$ for any face of K_5
$\therefore \sum \deg(F) \geqslant 21$
$\therefore 2e \geqslant 21$ $\{\sum \deg(F) = 2e\}$
$\therefore e \geqslant 10\frac{1}{2}$
$\therefore e \geqslant 11$ $\{\text{as } e \in \mathbb{Z}^+\}$
a contradiction as $e = 10$.
$\therefore K_5$ is not planar.

2 If G is a simple, connected planar graph with $v \geqslant 3$ then
$\deg(F_i) \geqslant 3$ for every face of G
$\therefore \sum \deg(F) \geqslant 3f$
$\therefore 2e \geqslant 3f$ $\{\sum \deg(F) = 2e\}$
$\therefore 2e \geqslant 3(e + 2 - v)$ {using Euler's formula}
$\therefore 2e \geqslant 3e + 6 - 3v$
$\therefore e \leqslant 3v - 6$

3 If G is a simple, connected graph with each face of degree 4 or more, then

$$\deg(F_i) \geqslant 4 \quad \text{for every face of } G$$
$$\therefore \sum \deg(F) \geqslant 4f$$
$$\therefore \ 2e \geqslant 4f \qquad \{\textstyle\sum \deg(F) = 2e\}$$
$$\therefore \ e \geqslant 2f$$
$$\therefore \ e \geqslant 2(e+2-v) \qquad \{\text{using Euler's formula}\}$$
$$\therefore \ e \geqslant 2e+4-2v$$
$$\therefore \ e \leqslant 2v-4$$

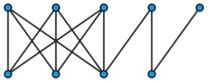
4 In a bipartite graph, each cycle has even length. In fact each cycle has length at least 4.

$\therefore$ $\deg(F_i) \geqslant 4$ for every face of G

$\therefore$ by question **3**, $e \leqslant 2v - 4$.

Note: $e \leqslant 2v - 4$ is a necessary but not a sufficient condition for a bipartite graph to be planar.

For example,



is a connected bipartite graph but not planar. However, it has $e = 12$ and $v = 9$, so $e \leqslant 2v - 4$ is satisfied.

5 **a** In K_5; $e = 10$, $v = 5$

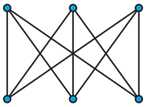
Thus in $e \leqslant 3v - 6$, $10 \leqslant 9$ which is false

$\therefore$ K_5 is not planar.

In $K_{3,\,3}$; $e = 9$, $v = 6$

Thus in $e \leqslant 2v - 4$, $9 \leqslant 8$ which is false

$\therefore$ $K_{3,\,3}$ is not planar.

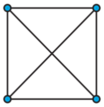


Note: Bipartite graph is planar $\Rightarrow e \leqslant 2v - 4$

$\therefore$ $e > 2v - 4 \Rightarrow$ bipartite graph not planar (contrapositive).

b K_4 is connected with $v = 4$ vertices

$\therefore$ $v \geqslant 3$

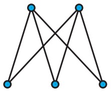


has $e = 6$ edges

and $e \leqslant 3v - 6$

$\therefore$ $6 \leqslant 6$

Likewise $K_{2,\,3}$ is connected with $v = 5$



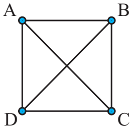
and $e = 6$

$\therefore$ $e \leqslant 2v - 4$

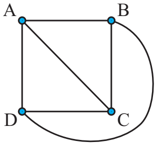
$\therefore$ $6 \leqslant 6$

Thus both K_4 and $K_{2,\,3}$ may or may not be planar, both inconclusive.

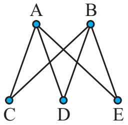
c K_4 is planar as, for example,



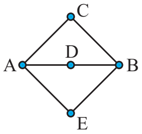
becomes



$K_{2,\,3}$ is planar as, for example,



becomes



6 If the length of the shortest cycle in a connected planar graph G is 5 then,

$$\deg(F_i) \geqslant 5 \quad \text{for every face of } G$$
$$\therefore \sum \deg(F) \geqslant 5f \quad \text{for } f \text{ faces in } G$$
$$\therefore \ 2e \geqslant 5f \qquad \{\textstyle\sum \deg(F) = 2e\}$$
$$\therefore \ 2e \geqslant 5(e+2-v) \qquad \{\text{using Euler's formula}\}$$
$$\therefore \ 2e \geqslant 5e+10-5v$$
$$\therefore \ 3e \leqslant 5v-10 \quad \text{....} \ (\,*\,)$$

For the connected Petersen graph, $v = 10$, $e = 15$ and the length of the shortest cycle is 5.

In $*$, $3 \times 15 \leqslant 5 \times 10 - 10$ is not satisfied

as 45 40

$\therefore$ the Petersen graph is not planar.

7 As g is the length of the shortest cycle then $\deg(F_i) \geqslant g$ for each finite face and $\therefore$ $\deg(F_{\text{inf}}) \geqslant g$ for the infinite face also.

Hence $\sum \deg(F) \geqslant gf$

$\therefore$ $2e \geqslant gf$ $\quad \{\sum \deg(F) = 2e\}$

But for a connected simple planar graph,

$f = e + 2 - v$ $\quad$ {Euler's formula}

Hence, $2e \geqslant ge + 2g - vg$

$\therefore$ $e(g-2) \leqslant g(v-2)$

Note: For simple graphs, $g \geqslant 3$.

8 **a** Let G be a simple connected planar graph on v vertices where $v \geqslant 3$.

From question **2**, $e \leqslant 3v - 6$.

Suppose each vertex of G has degree $\geqslant 6$.

$\therefore$ $\sum \deg(V) \geqslant 6v$

But $\sum \deg(V) = 2e$

Hence $2e \geqslant 6v$

$\therefore$ $e \geqslant 3v$

$\therefore$ $e \geqslant 3v \geqslant e + 6$ a contradiction

$\therefore$ G must have at least one vertex of degree $\leqslant 5$.

b Suppose the simple, connected, complete graph K_n is planar.

By question **2**, $e \leqslant 3v - 6$.

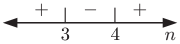
But $e = \dfrac{n(n-1)}{2}$ for K_n and $v = n$.

Hence, $\dfrac{n(n-1)}{2} \leqslant 3n - 6$

$\therefore$ $n^2 - n \leqslant 6n - 12$

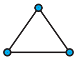
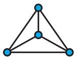
$\therefore$ $n^2 - 7n + 12 \leqslant 0$

$\therefore$ $(n-3)(n-4) \leqslant 0$



$\therefore$ $3 \leqslant n \leqslant 4$

$\therefore$ $n = 3$ or 4

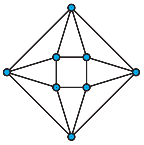
and as K_3  and K_4  exist, for $n \geqslant 3$,

K_n is planar $\Leftrightarrow n = 3$ or 4.

Also K_1 and K_2 are planar.

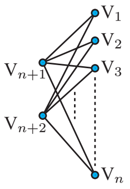
Thus the only complete graphs K_n which are planar are K_1, K_2, K_3, and K_4.

9

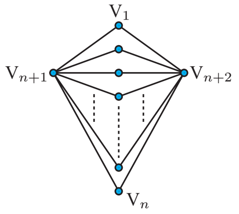


10 Consider the complete bipartite graph $K_{2,\,n}$.

By construction, $K_{2,\,n}$



becomes



$\therefore$ $K_{2,\,n}$ is planar.

11 The complete bipartite graph $K_{s,\,t}$ has $v = s + t$ and $e = st$.

By question **4**, if $K_{s,\,t}$ is planar then

$$e \leqslant 2v - 4$$
$$\therefore \; st \leqslant 2(s+t) - 4$$
$$\therefore \; st - 2s - 2t + 4 \leqslant 0$$
$$\therefore \; (s-2)(t-2) \leqslant 0 \quad .... \; (*)$$

$\therefore$ $K_{s,\,t}$ is not planar if

$$(s-2)(t-2) > 0$$
$$\therefore \; s > 2, \; t > 2 \qquad \{s, t > 1\}$$
$$\therefore \; s \geqslant 3, \; t \geqslant 3$$

12 G has v vertices where $v \geqslant 11$ and e edges

$\therefore$ G' has v vertices and $\dfrac{v(v-1)}{2} - e$ edges.

{as together G, G' partition all $\dfrac{v(v-1)}{2}$ edges}

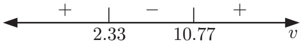
Suppose both G and G' are planar.

Then from question **2**,

$$e \leqslant 3v - 6 \quad \text{and} \quad \frac{v(v-1)}{2} - e \leqslant 3v - 6$$
$$\therefore \; e \geqslant \frac{v(v-1)}{2} - 3v + 6$$

Thus
$$\frac{v(v-1)}{2} - 3v + 6 \leqslant 3v - 6$$
$$\therefore \; \frac{v(v-1)}{2} \leqslant 6v - 12$$
$$\therefore \; v^2 - v \leqslant 12v - 24$$
$$\therefore \; v^2 - 13v + 24 \leqslant 0 \quad .... \; (*)$$

$v^2 - 13v + 24 = 0 \;\Leftrightarrow\; v \approx 2.33$ or 10.77



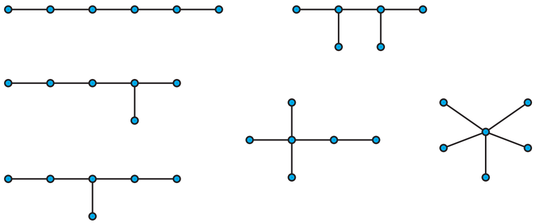
Thus for $v \geqslant 11$, $v^2 - 13v + 24 > 0$ which contradicts $*$.

$\therefore$ G and G' cannot both be planar.

EXERCISE 2E.1

1 **a** and **c** are trees.
b and **d** contain loops, $\therefore$ are not trees.

2



3 Only K_2 is a tree. K_n where $n > 2$ contains at least one cycle.

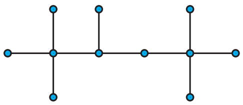
4 **a** From property **4**,
T is a tree $\Leftrightarrow$ it is connected and has $n - 1$ edges.

$$\therefore \; \sum \deg(V) = 2e$$
$$= 2(n-1)$$

b **i** $\sum \deg(V) = 2 \times 4 + 1 \times 3 + 1 \times 2 + (n-4) \times 1$

$$\therefore \; 2(n-1) = n + 9$$
$$\therefore \; 2n - 2 = n + 9$$
$$\therefore \; n = 11 \qquad \text{So, it has 11 vertices.}$$

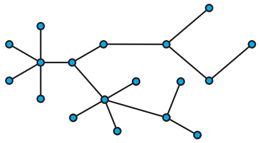
ii One example is:



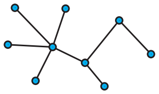
c **i** Likewise,

$$2(n-1) = 2 \times 5 + 3 \times 3 + 2 \times 2 + (n-7) \times 1$$
$$\therefore \; 2n - 2 = n + 16$$
$$\therefore \; n = 18 \qquad \text{So, it has 18 vertices.}$$

ii One example is:



5 One example is:



6 The complete bipartite graph $K_{m,\,n}$ has mn edges and $m + n$ vertices.

But a tree of order k has $k - 1$ edges

$$\therefore \; mn = m + n - 1$$
$$\therefore \; mn - m - n + 1 = 0$$
$$\therefore \; (m-1)(n-1) = 0$$
$$\therefore \; m = 1 \text{ or } n = 1$$

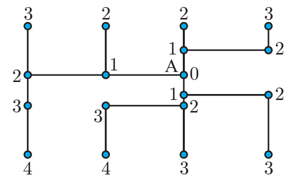
$\therefore$ $K_{m,\,n}$ is a tree if $m = 1$ or $n = 1$.

7 As a tree is a connected graph, no vertex can have a degree 0.
Now if every vertex has degree 2, the sum of the degrees of the n vertices is $2n$.
But a tree with n nodes has $n - 1$ edges and so the sum of the degrees is $2(n-1) = 2n - 2$ which is $< 2n$
$\therefore$ at least 2 vertices must have degree one.

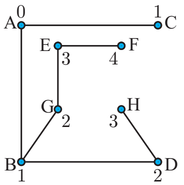
EXERCISE 2E.2

1 These are examples only.

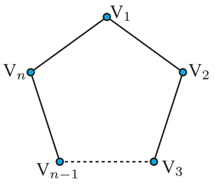
a

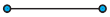
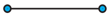


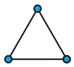
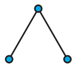
b

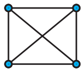


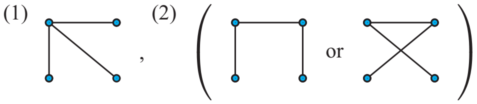
2 C_n has n vertices and n edges.
Removing any one of the n edges will result in a spanning tree.
So, there are n different spanning trees for C_n, $n \geqslant 3$.

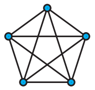


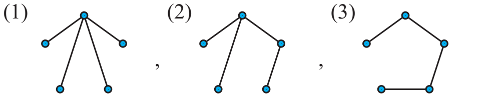
3 **a** **i** K_2:  has spanning tree: 

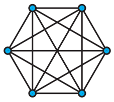
ii K_3:  has spanning tree: 

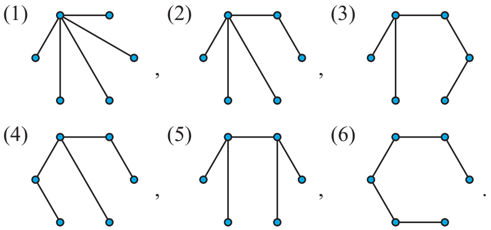
iii K_4:  has spanning trees:



iv K_5:  has spanning trees:



v K_6:  has spanning trees:



b Let D_n represent "the vertex of degree n".

i For K_2, there is **1** spanning tree.

For K_3, there are **3** different ways of choosing the D_2.

For K_4,

In (1), there are 4 ways of choosing D_3.

In (2), there are $\binom{4}{2}$ ways of choosing D_2s *and* there are 2 ways to join them to the remaining 2 vertices.

$\therefore$ total $= 4 + \binom{4}{2} \times 2 = \mathbf{16}$

For K_5,

In (1), there are 5 ways of choosing D_4.

In (2), there are 5 ways of choosing D_3 *and* 4 ways of choosing D_2 *and* 3 ways of choosing the vertex it joins to.

In (3), there are $\frac{1}{2} \times 5!$ ways

{reverse order gives the same spanning tree}

$$\therefore \text{ total} = 5 + 5 \times 4 \times 3 + \tfrac{1}{2}(5!)$$
$$= \mathbf{125}$$

For K_6,

In (1), there are 6 ways of choosing D_5.

In (2), there are 6 choices for choosing D_4 *and* 5 ways of choosing D_2 *and* 4 ways of choosing the vertex it joins to.

In (3), there are 6 ways of choosing D_3 *and* $5 \times 4 \times 3$ ways of choosing the path of length 3 from D_3.

In (4), there are 6 ways of choosing V *and* $\binom{5}{2}$ ways of choosing the D_2s *and* 3! ways of joining the remaining 3 vertices.

In (5), there are $\binom{6}{2}$ ways to choose the D_3s *and* $\binom{4}{2}$ ways of pairing up the 4 remaining vertices.

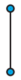
In (6), there are $\frac{1}{2} \times 6!$ ways.

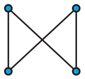
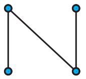
$$\therefore \text{ total} = 6 + 6 \times \binom{5}{2} \times 2 + 6 \times 5 \times 4 \times 3$$
$$+ 6 \times \binom{5}{2} \times 3! + \binom{6}{2}\binom{4}{2} + \frac{1}{2} \times 6!$$
$$= \mathbf{1296}$$

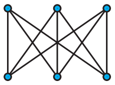
ii Since K_2 has $1 = 2^0$ spanning tree
K_3 has $3 = 3^1$ spanning trees
K_4 has $16 = 4^2$ spanning trees
K_5 has $125 = 5^3$ spanning trees
and K_6 has $1296 = 6^4$ spanning trees

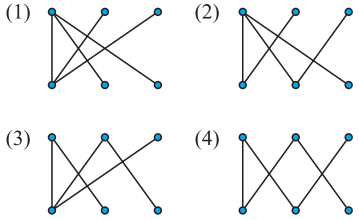
we postulate that:

K_n has n^{n-2} spanning trees, $n \geqslant 2$.

4 **a** **i** $K_{1,\,1}$: has spanning tree: 

ii $K_{2,\,2}$:  has spanning tree: 

iii $K_{3,\,3}$:  has spanning trees:



b For $K_{1,\,1}$, there is **1** spanning tree.

For $K_{2,\,2}$,

there are 2 choices for D_2 from one set *and* 2 from the other.

$\therefore$ total $= 2 \times 2 = \mathbf{4}$

For $K_{3,\,3}$,

In (1), there are 3 ways to choose D_3 on the top *and* 3 ways to choose D_3 on the bottom.

In (2), there are 3 ways to choose D_3 on the top *and* 3 ways to choose D_1 on the bottom *and* 2 ways to choose how the D_2s on the bottom connect to the D_1s on top.

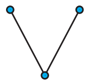
In (3), we have the symmetric case to (2).

In (4), there are 3 ways to choose D_1 on top *and* 3 ways to choose D_1 on bottom *and* 2 ways to choose which vertex D_1 on top connects to *and* 2 ways to choose which vertex D_1 on the bottom connects to.

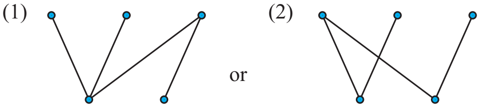
$$\text{total number} = 3 \times 3 + 2(3 \times 3 \times 2) + 3 \times 3 \times 2 \times 2$$
$$= \mathbf{81}$$

Since $K_{1,\,1}$ has $1 = 1^0$ spanning trees
$K_{2,\,2}$ has $4 = 2^2$ spanning trees
$K_{3,\,3}$ has $81 = 3^4$ spanning trees
$K_{4,\,4}$ has $4096 = 4^6$ spanning trees
we postulate that:
$K_{n,\,n}$ has n^{2n-2} spanning trees.

5 For $K_{2,\,1}$ we have only 1 tree;



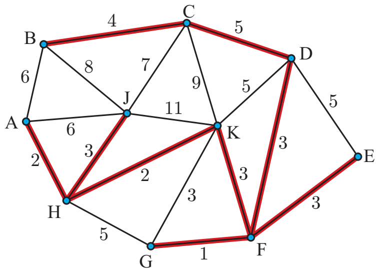
By symmetry $K_{1,\,2}$ also has 1 tree.
For $K_{3,\,2}$ we may have:



In (1), there are 2 ways to choose D_3 below *and* 3 ways to choose which vertex D_1 on the bottom connects to.
In (2), there are 3 ways to choose D_2 on top *and* 2 ways to choose how the top D_1s connect to the bottom vertices.
$\therefore$ $K_{3,\,2}$ has $2 \times 3 + 3 \times 2 = 12$ spanning trees.
So, using question **4**, we have:
$K_{1,\,1}$ has $1 = 1^0 \times 1^0$ spanning tree
$K_{1,\,2}$ has $1 = 1^1 \times 2^0$ spanning tree
$K_{2,\,1}$ has $1 = 2^0 \times 1^1$ spanning tree
$K_{2,\,2}$ has $4 = 2^1 \times 2^1$ spanning trees
$K_{3,\,2}$ has $12 = 3^1 \times 2^2$ spanning trees
$K_{3,\,3}$ has $81 = 3^2 \times 3^2$ spanning trees
Hence, we postulate that:
$K_{m,\,n}$ has $m^{n-1}n^{m-1}$ spanning trees.

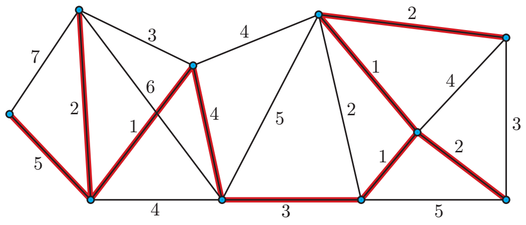
EXERCISE 2E.3

1 There are other (minor) variations.



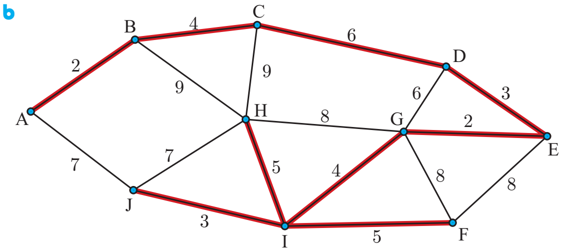
$\therefore$ minimum is \$26 million.

2 **a**



$\therefore$ minimum weight
$= 5+2+1+4+3+1+2+1+2$
$= 21$

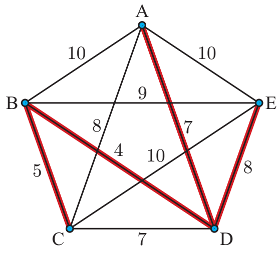
b



$\therefore$ minimum weight $= 2+4+6+3+2+4+5+3+5$
$= 34$

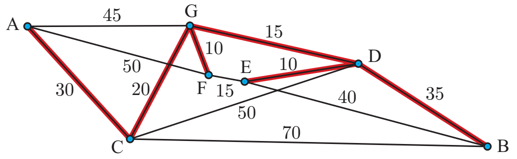
3 **a** There is a weight for every edge from every node to every other node.

b



c The minimum weight
$= 5+4+7+8$
$= 24$

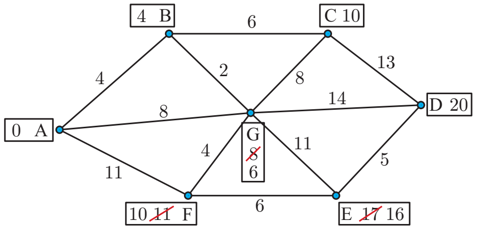
4



A variation is EF instead of DG.
The minimum weight $= 10+35+15+10+20+30$
$= 120$

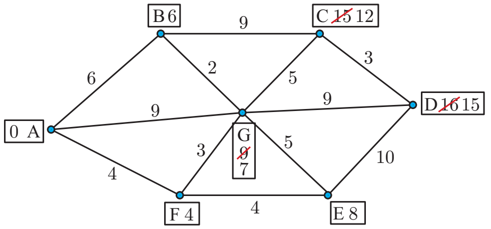
EXERCISE 2E.4

1 **a**



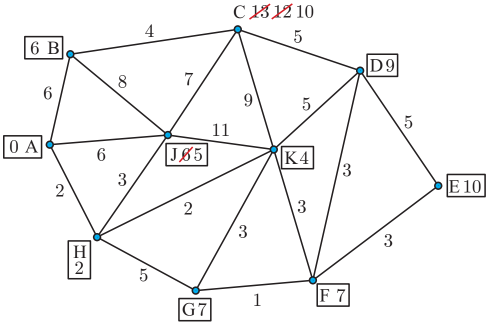
A ⟶ B ⟶ G ⟶ D, weight 20

b



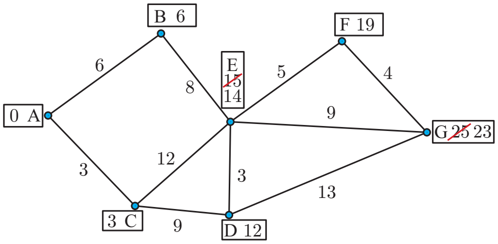
A ⟶ F ⟶ G ⟶ C ⟶ D, weight 15

2



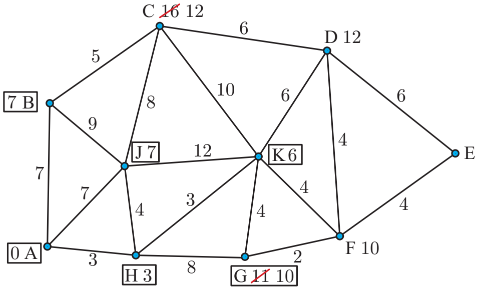
A → H → K → F → E, 10 hours

3 **a**



A → B → E → G or A → B → E → F → G, both weight 23

b



A → H → K → G, weight 10

EXERCISE 2F

1 Vertices A and C have odd degrees.

∴ not Eulerian, and so we have to travel between A and C twice.

The sum of the lengths of all the roads is 21 km, and the shortest path from A to C is 3 km.

So, the shortest distance the snowplough must travel is 24 km.

2 **a** A, B, C, and D have odd degrees. Since the graph is complete, exactly two sections must be repeated.

b Repeating AB and CD is $6 + 5 = 11$ km
Repeating AC and BD is $7 + 4 = 11$ km
Repeating AD and BC via D is $9 + 9 = 18$ km
The sum of the lengths of the paths is 43 km.
∴ the shortest distance to be travelled is 54 km, repeating either AB and CD or AC and BD.
An example route is:
A → B → D → C → A → B → C → D → A

c Repeating AB and CD is $4 + 7 = 11$ hours
Repeating AC and BD is $4 + 3 = 7$ hours
Repeating AD and BC is $6 + 6 = 12$ hours
The sum of the times of all edges is 30 hours.
∴ the shortest total time is 37 hours, repeating AC and BD.
An example route is:
A → C → B → D → C → A → D → B → A

3 **a** **i** Vertices B, F, G, and H have odd degrees.
∴ the graph is not Eulerian.

ii Repeating BF and GH has smallest distance
$7 + 2 = 9$ units
Repeating BG and FH has smallest distance
$5 + 3 = 8$ units
Repeating BH and FG has smallest distance
$4 + 5 = 9$ units
The sum of the distances of all the edges is 55 units.
∴ the shortest distance to be travelled is
$55 + 8 = 63$ units, travelling BG and FH twice.

b A possible route is:
A → B → C → D → E → C → H → E → F → H →
B → A → G → F → H → G → A

4 The vertices with odd degrees are A, D, E, and I.

Repeating AD and EI has smallest distance
$4 + 8 = 12$ units

Repeating AE and DI has smallest distance
$7 + 8 = 15$ units

Repeating AI and DE has smallest distance
$9 + 5 = 14$ units

∴ Peter should repeat AD (via B) and EI (via F) to walk $59 + 12 = 71$ units.

An example route is:
A → B → C → D → B → D → F → E → C → G → E →
F → G → I → H → F → I → F → B → A

5 **a** AB and CD, AC and BD, AD and BC.

b Repeating AB and CD has smallest distance
$3.5 + 6 = 9.5$ km
Repeating AC and BD has smallest distance
$6 + 5.5 = 11.5$ km
Repeating AD and BC has smallest distance
$5 + 5 = 10$ km
The sum of the distances of all the roads is 32.5 km.
∴ the shortest distance to be travelled is
$32.5 + 9.5 = 42$ km, travelling AB (via E) and CD twice.
This can be achieved by starting at any vertex.
An example route starting at E is:
E → A → B → E → A → D → C → B → E → D →
C → E

6 The vertices with odd degrees are C, D, E, and F.

Repeating CD and EF has smallest cost
$1.3 + 1.5 = 2.8$ ten thousand dollars

Repeating CE and DF has smallest cost
$2.3 + 2.6 = 4.9$ ten thousand dollars

Repeating CF and DE has smallest cost
$1.4 + 1.1 = 2.5$ ten thousand dollars

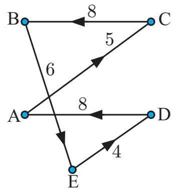
The sum of the costs for all routes is 13.6 ten thousand $s.

∴ the lowest cost solution is to travel CF (via B) and DE twice, and this costs $136 000 + $25 000 = $161 000.

An example route is:
A → B → F → G → D → E → F → B → E → D → C →
B → C → A

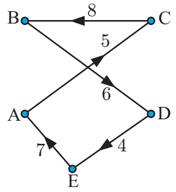
EXERCISE 2G

1 **a** **i**



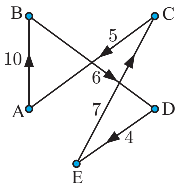
BEDACB has weight 31.
$\therefore\ m \leqslant 31$

or



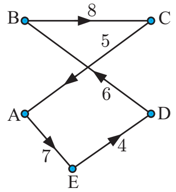
BDEACB has weight 30.
$\therefore\ m \leqslant 30$

or



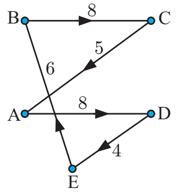
BDECAB has weight 32.
$\therefore\ m \leqslant 32$

ii



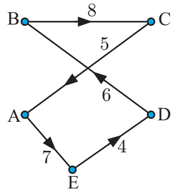
CAEDBC has weight 30.
$\therefore\ m \leqslant 30$

iii



DEBCAD has weight 31.
$\therefore\ m \leqslant 31$

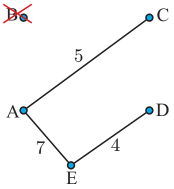
iv



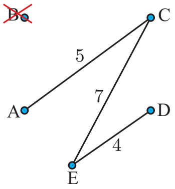
EDBCAE has weight 30.
$\therefore\ m \leqslant 30$

$\therefore$ the *best upper bound* is 30.

b **i** MST:

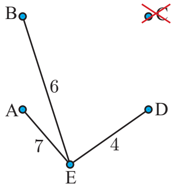


or

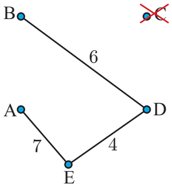


They both have weight 16.
wt{BE} = 6 and wt{BD} = 6
$\therefore\ m \geqslant 16 + 6 + 6$
$\therefore\ m \geqslant 28$

ii MST:

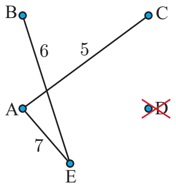


or

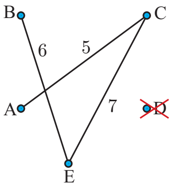


They both have weight 17.
wt{CA} = 5 and wt{CE} = 7
$\therefore\ m \geqslant 17 + 5 + 7$
$\therefore\ m \geqslant 29$

iii MST:

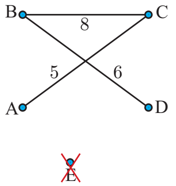


or

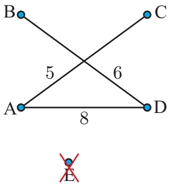


They both have weight 18.
wt{DE} = 4 and wt{DB} = 6
$\therefore\ m \geqslant 18 + 4 + 6$
$\therefore\ m \geqslant 28$

iv MST:



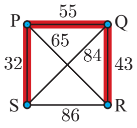
or



They both have weight 19.
wt{ED} = 4 and wt{EB} = 6
$\therefore\ m \geqslant 19 + 4 + 6$
$\therefore\ m \geqslant 29$

$\therefore$ the *best lower bound* is $m \geqslant 29$.

2 **a**



minimum spanning tree has weight 130
$\therefore$ upper bound is 260.
$\therefore\ m \leqslant 260$

b SPQRS gives a Hamiltonian cycle of weight $130+86 = 216$
$\therefore\ m \leqslant 216$

c

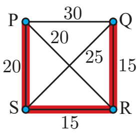
Vertex deleted	*MST length*	*2 shortest deleted edges*	*Total*
P	$43 + 84 = 127$	32, 55	214
Q	$32 + 65 = 97$	55, 43	195
R	$55 + 32 = 87$	43, 65	195
S	$55 + 43 = 98$	32, 84	214

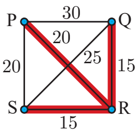
$\therefore$ the best lower bound is $m \geqslant 214$.

d PSQRP has weight 224, $\therefore\ m \leqslant 224$

e SPQRS is a Hamiltonian cycle of least weight 216.

3 **a**





Both minimum spanning trees have length 50
$\therefore$ upper bound is 100, and so $m \leqslant 100$

b QRSPQ gives a Hamiltonian cycle of weight $50 + 30 = 80$
$\therefore \quad m \leqslant 80$

c

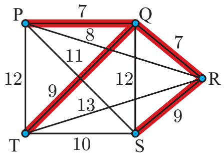
Vertex deleted	*MST length*	*2 shortest deleted edges*	*Total*
P	30	20, 20	70
Q	35	15, 25	75
R	45	15, 15	75
S	35	15, 20	70

$\therefore$ the greatest lower bound obtained is 75
$\therefore \quad m \geqslant 75$

d PSRQP has weight 80, $\quad \therefore \quad m \leqslant 80$
or PRSQP has weight 90, $\quad \therefore \quad m \leqslant 90$
or PRQSP has weight 80, $\quad \therefore \quad m \leqslant 80$

e PSRQP and PRQSP are both Hamiltonian cycles of minimum weight 80.

4 **a**



Minimum spanning tree has length 32.
$\therefore$ upper bound is 64.
$\therefore \quad m \leqslant 64$

b We find, for example, a Hamiltonian cycle PQTSRP of length $7 + 9 + 10 + 9 + 8 = 43$
$\therefore$ new upper bound $= 43$
$\therefore \quad m \leqslant 43$

c

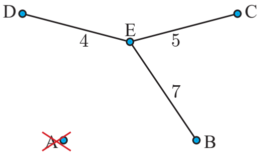
Vertex deleted	*MST length*	*2 shortest deleted edges*	*Total*
P	25	7, 8	40
Q	27	7, 7	41
R	26	7, 8	41
S	23	9, 10	42
T	23	9, 10	42

The greatest lower bound obtained is 42
$\therefore \quad m \geqslant 42$

d PRQTSP has a weight of 45, $\quad \therefore \quad m \leqslant 45$

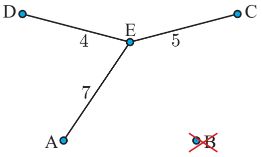
e The Hamiltonian cycle PQTSRP has the minimum possible weight 43.

5 **a** With A removed
MST is:



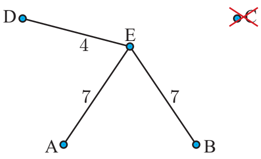
$\therefore \quad m \geqslant 4 + 5 + 7 + \text{wt}\{AE\} + \text{wt}\{AB\}$
$\therefore \quad m \geqslant 16 + 7 + 8$
$\therefore \quad m \geqslant 31$

With B removed
MST is:



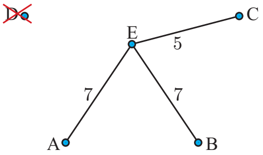
$\therefore \quad m \geqslant 4 + 5 + 7 + \text{wt}\{BE\} + \text{wt}\{BA\}$
$\therefore \quad m \geqslant 16 + 7 + 8$
$\therefore \quad m \geqslant 31$

With C removed
MST is:



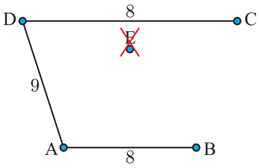
$\therefore \quad m \geqslant 4 + 7 + 7 + \text{wt}\{CE\} + \text{wt}\{CD\}$
$\therefore \quad m \geqslant 18 + 5 + 8$
$\therefore \quad m \geqslant 31$

With D removed
MST is:



$\therefore \quad m \geqslant 5 + 7 + 7 + \text{wt}\{DE\} + \text{wt}\{DC\}$
$\therefore \quad m \geqslant 19 + 4 + 8$
$\therefore \quad m \geqslant 31$

With E removed
MST is:



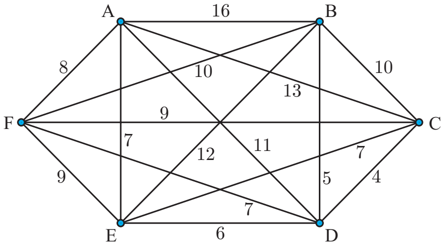
$\therefore \quad m \geqslant 8 + 8 + 9 + \text{wt}\{ED\} + \text{wt}\{EC\}$
$\therefore \quad m \geqslant 25 + 4 + 5$
$\therefore \quad m \geqslant 34$
$\therefore$ the best lower bound is $m \geqslant 34$.

b The Hamiltonian cycle is AEDCBA with weight $7 + 4 + 8 + 9 + 8 = 36$
$\therefore \quad m \leqslant 36$

c **i** Town E, as the roads between E and the other towns are the shortest on the graph.

ii EDCBAE has weight 36
$\therefore \quad m \leqslant 36$

6



AEDCFBA is the cycle using the nearest neighbour algorithm, which has weight $7 + 6 + 4 + 9 + 10 + 16 = 52$

7 **a** $\text{T} \xrightarrow{244} \text{B} \xrightarrow{247} \text{P} \xrightarrow{212} \text{O} \xrightarrow{297} \text{D} \xrightarrow{192} \text{L} \xrightarrow{59} \text{S} \xrightarrow{309} \text{M} \xrightarrow{1067} \text{C} \xrightarrow{996} \text{T}$
$\therefore$ the Hamiltonian cycle is TBPODLSMCT with total distance 3623 km.

b $\text{C} \xrightarrow{421} \text{O} \xrightarrow{212} \text{P} \xrightarrow{247} \text{B} \xrightarrow{244} \text{T} \xrightarrow{405} \text{M} \xrightarrow{309} \text{S} \xrightarrow{59} \text{L} \xrightarrow{192} \text{D} \xrightarrow{543} \text{C}$
$\therefore$ the Hamiltonian cycle is COPBTMSLDC with total distance 2632 km.

c It makes no difference. The cycles given in **a** and **b** are not necessarily optimal, and any cycle starting and ending in Calais could also be travelled starting and ending in Toulouse.

REVIEW SET A

1 **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$7^n + 3^n + 2$ is divisible by 4" for all $n \in \mathbb{N}$.

(1) If $n = 0$, $7^0 + 3^0 + 2 = 1 + 1 + 2 = 4$ and as $4 = 1(4)$, P_0 is true.

(2) If P_k is true, then $7^k + 3^k + 2 = 4A$, $A \in \mathbb{Z}$ .... $(*)$

Now $7^{k+1} + 3^{k+1} + 2$

$$\begin{aligned}
&= 7(7^k) + 3(3^k) + 2 \\
&= 7(4A - 3^k - 2) + 3(3^k) + 2 \qquad \{\text{using } *\} \\
&= 28A - 7(3^k) - 14 + 3(3^k) + 2 \\
&= 28A - 4(3^k) - 12 \\
&= 4(7A - 3^k - 3) \quad \text{where } 7A - 3^k - 3 \in \mathbb{Z}
\end{aligned}$$

$\therefore$ $7^{k+1} + 3^{k+1} + 2$ is divisible by 4.

Thus, P_0 is true, and P_{k+1} is true whenever P_k is true.

$\therefore$ P_n is true for all $n \in \mathbb{N}$.

2 $a_0 = 1$ and $a_{n+1} = \dfrac{n+2}{n+1} a_n$ for all $n \in \mathbb{N}$.

$$\begin{aligned}
\therefore\ a_n &= \frac{n+1}{n} a_{n-1} \\
&= \frac{n+1}{n} \times \frac{n}{n-1} a_{n-2} \\
&= \frac{n+1}{\cancel{n}} \times \frac{\cancel{n}}{\cancel{n-1}} \times \frac{\cancel{n-1}}{\cancel{n-2}} \times \dots \times \frac{\cancel{2}}{1} a_0 \\
&= (n+1)1 \\
&= n+1
\end{aligned}$$

$\therefore$ closed form solution is $a_n = n + 1$, $n \in \mathbb{N}$.

For $n = 0$, $a_0 = 0 + 1 = 1$ ✓

If $a_k = k + 1$

$$\begin{aligned}
a_{k+1} &= \frac{k+2}{k+1} a_k \\
&= \frac{k+2}{{}_1\cancel{k+1}} \cancel{(k+1)} \\
&= k+2 \\
&= (k+1) + 1
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = n + 1$ for all $n \in \mathbb{N}$.

3 $a_0 = 3$, $a_n = 4a_{n-1} - 8$, $n \geqslant 1$

a $a_0 = 3$

$$\begin{aligned}
a_1 &= 4a_0 - 8 & a_2 &= 4a_1 - 8 \\
&= 4(3) - 8 & &= 4(4) - 8 \\
&= 4 & &= 8 \\
a_3 &= 4a_2 - 8 & a_4 &= 4a_3 - 8 \\
&= 4(8) - 8 & &= 4(24) - 8 \\
&= 24 & &= 88
\end{aligned}$$

b inhomogeneous with constant coefficient $r \neq 1$

$\therefore$ $a_n = r^n c + b\left(\dfrac{r^n - 1}{r - 1}\right)$ where $c = 3$, $r = 4$, $b = -8$

$$\begin{aligned}
\therefore\ a_n &= 4^n \times 3 - 8\left(\frac{4^n - 1}{4 - 1}\right) \\
&= 4^n(3) - \tfrac{8}{3}(4^n - 1) \\
&= 4^n(3 - \tfrac{8}{3}) + \tfrac{8}{3} \\
&= 4^n(\tfrac{1}{3}) + \tfrac{8}{3}
\end{aligned}$$

$\therefore$ $a_n = \dfrac{4^n + 8}{3}$ for all $n \in \mathbb{N}$.

For $n = 0$, $a_0 = \dfrac{4^0 + 8}{3} = \dfrac{9}{3} = 3$ ✓

If $a_k = \dfrac{4^k + 8}{3}$

$$\begin{aligned}
\text{then}\quad a_{k+1} &= 4a_k - 8 \\
&= 4\left(\frac{4^k + 8}{3}\right) - 8 \\
&= \frac{4^{k+1} + 32}{3} - 8 \\
&= \frac{4^{k+1} + 32 - 24}{3} \\
&= \frac{4^{k+1} + 8}{3}
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = \dfrac{4^n + 8}{3}$ for all $n \in \mathbb{N}$.

4 **a** **i** $a_1 = 0.978a_0$ grams

ii $a_2 = 0.978a_1 = 0.978^2 a_0$

$\vdots$

$a_5 = 0.978^5 a_0$ grams

b $a_n = 0.978a_{n-1}$ and $a_0 = a_0$

homogeneous with constant coefficients

$\therefore$ $a_n = r^n c$ where $c = a_0$, $r = 0.978$

$\therefore$ $a_n = 0.978^n a_0$, $n \in \mathbb{N}$.

For $n = 0$, $a_0 = 0.978^0 a_0 = a_0$ ✓

If $a_k = 0.978^k a_0$

$$\begin{aligned}
\text{then}\quad a_{k+1} &= 0.978a_k \\
&= 0.978(0.978)^k a_0 \\
&= (0.978)^{k+1} a_0
\end{aligned}$$

which is of the required form.

$\therefore$ by the principle of (weak) induction, $a_n = 0.978^n a_0$, $n \in \mathbb{N}$.

c $a_{10} = 1.7$

$\therefore$ $0.978^{10} a_0 = 1.7$

$\therefore$ $a_0 = \dfrac{1.7}{0.978^{10}}$

$\therefore$ $a_0 \approx 2.12$

$\therefore$ an initial mass of ≈ 2.12 g would be necessary.

5 **a** $a_n = 4a_{n-1} - 3a_{n-2}$ for $n \geqslant 2$, $n \in \mathbb{Z}$ with $a_0 = 1$, $a_1 = -1$ has characteristic equation

$\lambda^2 - 4\lambda + 3 = 0$

$\therefore$ $(\lambda - 1)(\lambda - 3) = 0$

$\therefore$ $\lambda = 1$ or 3, distinct real roots

$\therefore$ the general solution is $a_n = c_1 1^n + c_2 3^n$, $n \in \mathbb{N}$.

Using the initial conditions:

$a_0 = 1$ $\therefore$ $c_1 + c_2 = 1$ .... (1)

and $a_1 = -1$ $\therefore$ $c_1 + 3c_2 = -1$ .... (2)

Solving (1) and (2) gives $c_1 = 2$ and $c_2 = -1$

$\therefore$ $a_n = 2 - 3^n$, $n \in \mathbb{N}$.

b $a_n = 4a_{n-1} - 4a_{n-2}$, $n \geqslant 2$, $n \in \mathbb{Z}$, $a_0 = 1$, $a_1 = -1$ has characteristic equation

$\lambda^2 - 4\lambda + 4 = 0$

$\therefore$ $(\lambda - 2)^2 = 0$

$\therefore$ $\lambda = 2$, a repeated root

$\therefore$ the general solution is $a_n = (c_1 + nc_2)2^n$, $n \in \mathbb{N}$.

Using the initial conditions:

$$a_0 = 1 \qquad \therefore\ c_1 2^0 = 1 \qquad \therefore\ c_1 = 1$$

and $a_1 = -1 \quad \therefore\ (c_1 + c_2)2 = -1 \quad \therefore\ c_1 + c_2 = -\frac{1}{2}$

$\therefore\ c_1 = 1$ and $c_2 = -\frac{3}{2}$

$$\therefore\ a_n = \left(1 - \frac{3n}{2}\right)2^n, \quad n \in \mathbb{N}.$$

That is, $a_n = (2-3n)2^{n-1}, \quad n \in \mathbb{N}.$

c $a_n = 4a_{n-1} - 5a_{n-2}, \quad n \geqslant 2, \quad n \in \mathbb{Z}, \quad a_0 = 0, \quad a_1 = 1$ has characteristic equation

$\lambda^2 - 4\lambda + 5 = 0$

$$\therefore\ \lambda = \frac{4 \pm \sqrt{16 - 4(1)(5)}}{2}$$

$\therefore\ \lambda = 2 \pm i$, complex conjugate roots

$\therefore$ the general solution is

$$a_n = c_1(2+i)^n + c_2(2-i)^n, \quad n \in \mathbb{N}.$$

Using initial conditions:

$a_0 = 0 \qquad \therefore\ c_1 + c_2 = 0 \qquad$ .... (1)

and $a_1 = 1 \quad \therefore\ c_1(2+i) + c_2(2-i) = 1$

$\therefore\ 2(c_1 + c_2) + i(c_1 - c_2) = 1 \qquad$ .... (2)

Substituting (1) into (2) gives $\quad i(c_1 - c_2) = 1$

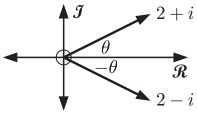
$$\therefore\ c_1 - c_2 = \frac{1}{i} \times \frac{i}{i} = -i$$

$$c_1 - c_2 = -i$$
$$c_1 + c_2 = 0$$

Adding, $\qquad 2c_1 = -i$

$$c_1 = -\frac{i}{2} \quad \text{and} \quad c_2 = \frac{i}{2}$$

$$\therefore\ a_n = -\frac{i}{2}(2+i)^n + \frac{i}{2}(2-i)^n$$
$$= -\frac{i}{2}\left[(2+i)^n - (2-i)^n\right]$$



$r = \sqrt{5}, \quad \theta = \arctan(\frac{1}{2})$

$$\begin{aligned}
\therefore\ a_n &= -\frac{i}{2}\left[(\sqrt{5}\operatorname{cis}\theta)^n - (\sqrt{5}\operatorname{cis}(-\theta))^n\right] \\
&= -\frac{i}{2}\left[5^{\frac{n}{2}}\operatorname{cis} n\theta - 5^{\frac{n}{2}}\operatorname{cis}(-n\theta)\right] \\
&= -\frac{i}{2}\left[5^{\frac{n}{2}}(\operatorname{cis}(n\theta) - \operatorname{cis}(-n\theta))\right] \\
&= -\frac{i}{2}5^{\frac{n}{2}}\left[\cos n\theta + i\sin n\theta - [\cos n\theta - i\sin n\theta]\right] \\
&= -\frac{i}{2}5^{\frac{n}{2}}\left[2i\sin n\theta\right] \\
&= 5^{\frac{n}{2}}\sin n\theta \quad \text{where} \quad \theta = \arctan(\tfrac{1}{2})
\end{aligned}$$

$$\therefore\ a_n = 5^{\frac{n}{2}}\sin(n\arctan(\tfrac{1}{2}))$$

6 Instead of showing $3 \mid a^2 + b^2 \Rightarrow 3 \mid a$ and $3 \mid b$, we will prove the contrapositive $3 \nmid a$ and $3 \nmid b \Rightarrow 3 \nmid a^2 + b^2$.

If $3 \nmid a$,

then $a = 3p + 1$ or $a = 3p + 2$

$\Rightarrow\ a^2 = 9p^2 + 6p + 1$ or $a^2 = 9p^2 + 12p + 4$

$\Rightarrow\ a^2 = 3(3p^2 + 2p) + 1$ or $a^2 = 3(3p^2 + 4p + 1) + 1$

Similarly, $3 \nmid b \Rightarrow b^2 = 3(3q^2 + 2q) + 1$ or

$b^2 = 3(3q^2 + 4q + 1) + 1$

If $3 \nmid a$ and $3 \nmid b$,

then $a^2 + b^2 = 3(3p^2 + 2p) + 1 + 3(3q^2 + 2q) + 1,$

$3(3p^2 + 2p) + 1 + 3(3q^2 + 4q + 1) + 1,$

$3(3p^2 + 4p + 1) + 1 + 3(3q^2 + 2q) + 1,$ or

$3(3p^2 + 4p + 1) + 1 + 3(3q^2 + 4q + 1) + 1$

$\Rightarrow\ a^2 + b^2 = 3(3p^2 + 2p + 3q^2 + 2q) + 2,$

$3(3p^2 + 2p + 3q^2 + 4q + 1) + 2,$

$3(3p^2 + 4p + 3q^2 + 2q + 1) + 2,$ or

$3(3p^2 + 4p + 3q^2 + 4q + 2) + 2$

$\Rightarrow\ a^2 + b^2 = 3k + 2$ where $k \in \mathbb{Z}$

$\Rightarrow\ 3 \nmid a^2 + b^2$

Hence $3 \nmid a$ and $3 \nmid b \Rightarrow 3 \nmid a^2 + b^2$, and therefore $3 \mid a^2 + b^2 \Rightarrow 3 \mid a$ and $3 \mid b$. {contrapositive}

7 **a** $6m + 5 = 6m + 3 + 2, \quad m \in \mathbb{Z}$

$= 3(2m+1) + 2$ where $2m + 1 \in \mathbb{Z}$

$= 3n + 2$ where $n \in \mathbb{Z}$

b $32 = 3(10) + 2$ has form $3n + 2, \quad n \in \mathbb{Z}$

but $32 = 6(5) + 2$ is not in the form $6m + 5$.

8 **a** 144_5

$= 1 \times 5^2 + 4 \times 5 + 4$

$= 25 + 20 + 4$

$= 49_{10}$

2	49	r
2	24	1
2	12	0
2	6	0
2	3	0
	1	1

$\therefore\ 49_{10} = 110\,001_2$

b

8	49	r
	6	1

$\therefore\ 144_5 = 61_8$

9 In any set of 5 consecutive integers, one of them must be divisible by 5 and one of them must be divisible by 3.

Also at least one of them is divisible by 2 and another by 4

$\therefore\ P$ is divisible by $2 \times 4 \times 3 \times 5$

$\therefore\ P$ is divisible by 120.

10 **a** $552 = 2 \times 208 + 136$

$208 = 1 \times 136 + 72$

$136 = 1 \times 72 + 64$

$72 = 1 \times 64 + 8$

$64 = 8 \times 8$

$\therefore\ \gcd(552, 208) = 8$

b $8 = 72 - 1 \times 64$

$= 72 - (136 - 72)$

$= -136 + 2 \times 72$

$= -136 + 2(208 - 136)$

$= 2 \times 208 - 3 \times 136$

$= 2 \times 208 - 3(552 - 2 \times 208)$

$= 2 \times 208 - 3 \times 552 + 6 \times 208$

$= -3 \times 552 + 8 \times 208$

$\therefore\ m = -3$ and $n = -8$

11 **a** $m = (n+1)! + 2, \quad n \in \mathbb{Z}^+, \quad n \geqslant 2$

$\therefore\ m = (n+1)n(n-1) .... \times 4 \times 3 \times 2 \times 1 + 2$

$\therefore\ m + 1 = (n+1)n(n-1) .... \times 4 \times 3 \times 2 \times 1 + 3$

$\therefore\ m + 1 = 3[(n+1)n(n-1) .... \times 4 \times 2 \times 1] + 3$

$\therefore\ m + 1 = 3[(n+1)n(n-1) .... \times 4 \times 2 \times 1 + 1]$

$\therefore\ 3 \mid m + 1$

Also $(n+1)!$ is even for $n \geqslant 2$

$\therefore$ $(n+1)!+2$ is even.

b $\quad m = (n+2)!+2, \ n \in \mathbb{Z}^+, \ n \geqslant 3$

$$\begin{aligned} \therefore \ m+1 &= (n+2)!+3 \\ &= (n+2)(n+1)n.... \times 4 \times 3 \times 2 \times 1 + 3 \\ &= 3[(n+2)(n+1)n.... \times 4 \times 2 \times 1 + 1] \end{aligned}$$

$\therefore \ 3 \mid m+1$

and $\quad m+2 = (n+2)!+4$

$$= 4[(n+2)(n+1).... \times 5 \times 3 \times 2 \times 1 + 1]$$

$\therefore \ 4 \mid m+2$

and $(n+2)!$ is even for $n \geqslant 3$

$\therefore \ m = (n+2)!+2$ is even.

c As in **a**, **b**

$m = (n+3)!+2, \ (n+4)!+2, \ ...., \ (n+n)!+2$ are composites

$\therefore \ m = (n+1)!+2, \ (n+2)!+2, \ ...., \ (n+n)!+2$

are a sequence of n numbers which are all composite.

12 **a**

$$\begin{array}{r|r} 5 & 1040 \\ \cline{2-2} 2 & 208 \\ \cline{2-2} 2 & 104 \\ \cline{2-2} 2 & 52 \\ \cline{2-2} 2 & 26 \\ \cline{2-2} & 13 \end{array}$$

$\therefore \ 1040 = 2^4 \times 5^1 \times 13^1$

b

$$\begin{array}{r|r} 5 & 18\,360 \\ \cline{2-2} 2 & 3672 \\ \cline{2-2} 2 & 1836 \\ \cline{2-2} 2 & 918 \\ \cline{2-2} 3 & 459 \\ \cline{2-2} 3 & 153 \\ \cline{2-2} 3 & 51 \\ \cline{2-2} & 17 \end{array}$$

$$\begin{aligned} \therefore \quad & 18\,360 \\ &= 2^3 \times 3^3 \times 5^1 \times 17^1 \end{aligned}$$

c

$$\begin{array}{r|r} 5 & 19\,845 \\ \cline{2-2} 3 & 3969 \\ \cline{2-2} 3 & 1323 \\ \cline{2-2} 3 & 441 \\ \cline{2-2} 3 & 147 \\ \cline{2-2} 7 & 49 \\ \cline{2-2} & 7 \end{array}$$

$\therefore \ 19\,845 = 3^4 \times 5^1 \times 7^2$

13 **a**

$$\begin{aligned} & 23^{12} \pmod 5 \\ \equiv\ & 3^{12} \pmod 5 \\ \equiv\ & (3^4)^3 \pmod 5 \\ \equiv\ & 81^3 \pmod 5 \\ \equiv\ & 1^3 \pmod 5 \\ \equiv\ & 1 \pmod 5 \end{aligned}$$

b

$$\sum_{k=1}^{30} k! \pmod{20}$$

$\equiv 1!+2!+3!+4! \pmod{20}$

$\{5! = 120 \quad \therefore \ 20 \mid 5! \quad$ Hence $\ 20 \mid 6!, \ 20 \mid 7!, \ $ etc.$\}$

$\equiv 1+2+6+24 \pmod{20}$

$\equiv 9+4 \pmod{20}$

$\equiv 13 \pmod{20}$

14 Any integer must have one of these forms:

$6n, \ 6n+1, \ 6n+2, \ 6n+3, \ 6n+4, \ 6n+5$

Thus any prime $p \geqslant 5$ must have form $6n+1$ or $6n+5$

{the other forms are composite}

Thus $\ p^2-1 = (6n+1)^2 \ $ or $\ (6n+5)^2-1$

$\therefore \ p^2-1 = 36n^2+12n \ $ or $\ 36n^2+60n+24$

$\therefore \ p^2-1 = 12(3n^2+n) \ $ or $\ 12(3n^2+5n+2)$

where $3n^2+n, \ 3n^2+5n+2 \in \mathbb{Z}$

$\therefore \ 12 \mid p^2-1$

15 Let e be a common divisor of a and c

$\therefore \ c = ke$ for some $k \in \mathbb{Z}$.

$\therefore \ bc = (bk)e$ and so $e \mid bc$.

So, e is a common divisor of a and bc .... $(*)$

Now let f be a common divisor of a and bc

$\therefore \ a = mf$ and $bc = nf$ for some $m, n \in \mathbb{Z}$.

Since $\ \gcd(a, b) = 1, \quad ax+by = 1 \quad$ for $x, y \in \mathbb{Z}$

$\therefore \ cax+cby = c$

$\therefore \ c(mf)x+(nf)y = c$

$\therefore \ f(cmx+ny) = c \quad$ and so $f \mid c$

So, f is a common divisor of a and c .... $(**)$

From $(*)$ and $(**)$, $\gcd(a, c) = \gcd(a, bc)$.

16 **a** $(bba) = 100b+10b+a = 110b+a$

If the sum of the digits is divisible by 12 then $2b+a = 12k$ for $k \in \mathbb{Z}$

$$\begin{aligned} \therefore \ (bba) &= 110b+12k-2b \\ &= 108b+12k \\ &= 12(9b+k) \quad \text{where } 9b+k \in \mathbb{Z} \end{aligned}$$

$\therefore \ (bba)$ is divisible by 12 also.

b $(bab) = 100b+10a+b = 10a+101b$

If $k \mid (bab)$ and $k \mid a+2b, \ k \in \mathbb{Z}, \ 1 < k < 10$

then $10a+101b = mk$ and $a+2b = nk$ .... (1)

for some $m, n \in \mathbb{Z}$

$\therefore \ 10(nk-2b)+101b = mk$

$\therefore \ 10nk-20b+101b = mk$

$\therefore \ k(m-10n) = 81b$

$\therefore \ k \mid 81$ or $k \mid b$

$\therefore \ k = 3$ or 9 or k is a divisor of b .... (2)

In (1), $\ a+2b = nk$

$\therefore \ a+2lk = nk, \ l \in \mathbb{Z}$ if $k \mid b$

$\therefore \ a = k(n-2l)$

$\therefore \ k \mid a$

Thus in (2), $k = 3$ or 9 or k is a divisor of a and b.

17 $57x \equiv 20 \pmod{13}$

$\therefore \ 5x \equiv 7 \pmod{13}$

As 13 is a prime there is a unique solution.

It is $x \equiv 4 \pmod{13}$.

18 **a** If $n \not\equiv 0 \pmod 5$ then $n \equiv \pm1, \ \pm2 \pmod 5$

$\therefore \ n^2 \equiv 1, 4 \pmod 5$

$\therefore \ n^2 \equiv 1, -1 \pmod 5$

$\therefore \ n^2 \equiv \pm1 \pmod 5$

b $n^5+5n^3+4n = n(n^4+5n^2+4)$

$$\begin{aligned} &\equiv \pm1(1+5(\pm1)+4) \pmod 5 \\ &\quad \text{or} \quad \pm2(1+5(\pm1)+4) \pmod 5 \\ &= \pm1(10 \text{ or } 0) \pmod 5 \\ &\quad \text{or} \quad \pm2(10 \text{ or } 0) \pmod 5 \\ &\equiv 0 \pmod 5 \end{aligned}$$

$\therefore \ n^5+5n^3+4n$ is divisible by 5 for all $n \in \mathbb{Z}$.

19 4 and 5 are relatively prime. ✓

$M = 4 \times 5 = 20$

$\therefore \ M_1 = \frac{20}{4} = 5 \ $ and $\ M_2 = \frac{20}{5} = 4$

x_1 is the solution to $5x_1 \equiv 1 \pmod 4 \ \Rightarrow \ x_1 = 1$

x_2 is the solution to $4x_2 \equiv 1 \pmod 5 \ \Rightarrow \ x_2 = 4$

Now $x \equiv a_1M_1x_1 + a_2M_2x_2 \pmod{20}$

$\therefore\ x \equiv 2 \times 5 \times 1 + 4 \times 4 \times 4 \pmod{20}$

$\therefore\ x \equiv 14 \pmod{20}$

20 If $\sqrt{6} = \frac{a}{b}$ where $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = 1$

then $a^2 = 6b^2$

$\therefore\ 6 \mid a^2$

$\therefore\ 6 \mid a$

$\therefore\ a$ is even $\{2 \mid a\}$

$\therefore\ a = 2k$ say, $k \in \mathbb{Z}$

$\therefore\ 4k^2 = 6b^2$

$\therefore\ 3b^2 = 2k^2$

$\therefore\ b^2$ is even

$\therefore\ b$ is also even

$\therefore\ a$ and b have 2 as a common factor, which is a contradiction

$\therefore\ \sqrt{6}$ is irrational.

21 $11^{87} + 3 \pmod{17}$

$\equiv (11^{16})^5 \times 11^7 + 3 \pmod{17}$

$\equiv 1^5 \times (121)^3 \times 11 + 3 \pmod{17}$ {FLT}

$\equiv 2^3 \times 11 + 3 \pmod{17}$ $\{119 = 17 \times 7\}$

$\equiv 91 \pmod{17}$

$\equiv 6 \pmod{17}$

$\therefore$ when $11^{87} + 3$ is divided by 17, the remainder is 6.

22 The garden can be divided into $9 \times 11 = 99$ squares which are 4 m by 4 m.

As there are 100 trees to be planted, by the PHP there exists at least one 4 m by 4 m square containing at least two trees.

23 Every integer $a \equiv 0$, 1, or $2 \pmod 3$

Since there are 4 integers; x, y, z, and t and 3 residue classes modulo 3, by the PHP there exists one residue containing at least 2 of these integers.

That is, at least two of x, y, z, t are congruent modulo 3.

Suppose they are x and y

$\therefore\ x \equiv y \pmod 3$

$\therefore\ x - y \equiv 0 \pmod 3$

$\therefore\ 3 \mid (x - y)$

$\therefore$ the product $(x-y)(x-z)(x-t)(y-z)(y-t)(z-t)$

$\equiv 0 \pmod 3$

24 **a** Only for $m = 2$ **b** Only for $m = 2$

c W_m is never bipartite.

25 $\sum \deg(V) = 2e$ {Handshaking Lemma}

Now if the minimum degree of a vertex is m and the maximum is M, then, $mv \leqslant 2e \leqslant Mv$

$\therefore\ m \leqslant \frac{2e}{v} \leqslant M$

26 The $(n-1)$ outer vertices of W_n form a cycle with $(n-1)$ edges.

The centre vertex is joined to the outer vertices by $(n-1)$ edges.

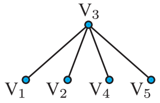
$\therefore\ W_n$ has $2(n-1)$ edges.

K_n has $\binom{n}{2} = \frac{n(n-1)}{2}$ edges

$\therefore$ the complement of W_n has $\frac{n(n-1)}{2} - 2(n-1)$ edges.

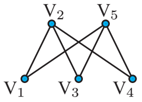
27 **a** **i** $\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

ii Yes, $K_{1,\,4}$



b **i** $\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$

ii Yes, $K_{2,\,3}$

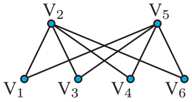


c **i** $\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$

ii No

d **i** $\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$

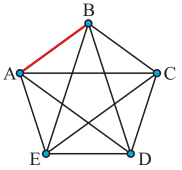
ii Yes, $K_{2,\,4}$



e **i** $\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$

ii No

28



Suppose A and B are the given (fixed) vertices.

a Any path from A to B (or B to A) must go through C, D, or E for path length 2.

$\therefore$ the number of paths is 3.

b One such path is ACDB, so we need to choose any two of C, D, E and this can be done in $3 \times 2 = 6$ ways.

$\therefore$ 6 paths.

c One such path is ACDEB, so we need to choose from all orderings of C, D, E and this can be done in $3 \times 2 \times 1 = 6$ ways.

$\therefore$ 6 paths.

29 A simple graph is bipartite $\Leftrightarrow$ each of its circuits is of even length.

$\therefore$ if a bipartite graph has an odd number of vertices, it cannot contain a circuit visiting *every* vertex.

$\therefore$ G cannot be Hamiltonian.

30 **a** If there are 28 edges, then there are 56 ends of edges.

$\therefore$ the sum of the degrees of the vertices is 56.

If there are m vertices of degree 3, and $12 - m$ vertices of degree 4, then

$3m + 4(12 - m) = 56$

$\therefore\ -m + 48 = 56$

$\therefore\ m = -8$, which is impossible

Hence, no such graphs exist.

b Using the same argument as in **a**, suppose there are m vertices of degree 5 and $12 - m$ vertices of degree 6.

$$\therefore \quad 5m + 6(12 - m) = 56$$
$$\therefore \quad -m + 72 = 56$$
$$\therefore \quad m = 16$$

which is impossible as there would be $12 - 16 = -4$ vertices of degree 6.

Hence, no such graphs exist.

31 If the shortest cycle has length 5, then each face has at least 5 edges.

$$\therefore \quad \sum \deg(F) \geqslant 5f$$
$$\therefore \quad 2e \geqslant 5f \qquad \{\textstyle\sum \deg(F) = 2e\}$$
$$\therefore \quad f \leqslant \frac{2e}{5}$$

But $e + 2 = v + f$ {Euler's formula}

$$\therefore \quad e + 2 \leqslant v + \tfrac{2}{5}e$$
$$\therefore \quad \tfrac{3}{5}e \leqslant v - 2$$
$$\therefore \quad 3e \leqslant 5v - 10$$
$$\therefore \quad e \leqslant \frac{5v - 10}{3}$$

32 Since the connected graph is planar,

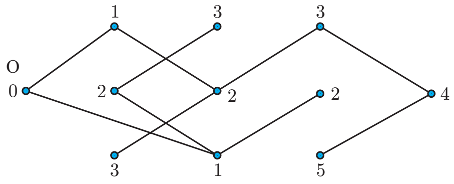
$e + 2 = v + f$ {Euler's formula}

Now if there are 8 vertices of degree 3, there are 24 ends of edges.

$$\therefore \quad e = 12$$
$$\therefore \quad 12 + 2 = 8 + f$$
$$\therefore \quad f = 6$$

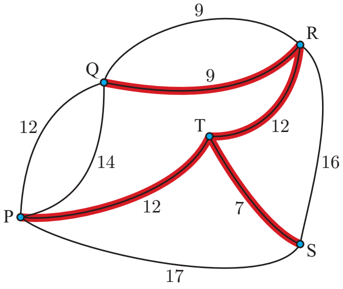
That is, there are 6 faces.

33



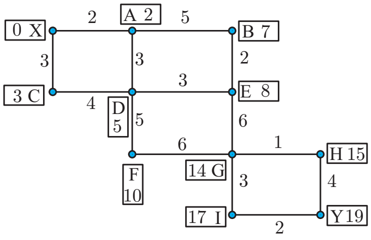
34 For example, 4 edges are chosen in order:

TS, QR, TR, TP.



minimum weight
$= 7 + 9 + 12 + 12$
$= 40$

35 Using Dijkstra's algorithm:



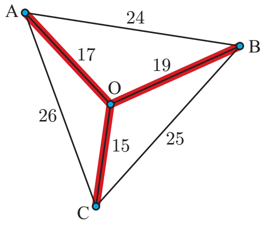
Minimum connector has length 19.

Either O ⟶ A ⟶ D ⟶ E ⟶ G ⟶ H ⟶ Y

or O ⟶ A ⟶ D ⟶ E ⟶ G ⟶ I ⟶ Y

36 Let m be the weight of the minimum weight Hamiltonian cycle in the graph.

a Using Kruskal



minimum length
$= 15 + 17 + 19$
$= 51$
$\therefore$ upper bound is 102
$\therefore \quad m \leqslant 102$

b For example, $C \xrightarrow{15} O \xrightarrow{19} B \xrightarrow{24} A \xrightarrow{26} C$ gives an upper bound of 84, $\therefore \quad m \leqslant 84$

c

Vertex deleted	*MST length*	*2 shortest deleted edges*	*Total*
A	34	17, 24	75
B	32	19, 24	75
C	36	15, 25	76
O	49	15, 17	81

$\therefore$ best lower bound is 81, $\therefore \quad m \geqslant 81$.

d The Hamiltonian cycle O ⟶ A ⟶ B ⟶ C ⟶ O gives minimum weight 81 units.

So, $m = 81$.

REVIEW SET B

1 **Proof:** (By the Principle of Mathematical Induction)

P_n is that "$2^n < n!$" for $n \geqslant 4, \ n \in \mathbb{Z}^+$

(1) If $n = 4$, $2^4 = 16$ and $4! = 24$ and as $16 < 24$, P_4 is true.

(2) If P_k is true, then $2^k < k!$

$$\begin{aligned}
\therefore \quad & (k+1)! - 2^{k+1} \\
&= (k+1)k! - 2 \times 2^k \\
&> (k+1)2^k - 2 \times 2^k \\
&> 2^k(k-1) \\
&> 0 \qquad \{\text{as } 2^k > 0, \ k - 1 \geqslant 3\}
\end{aligned}$$

$$\therefore \quad 2^{k+1} < (k+1)!$$

Thus P_4 is true, and P_{k+1} is true whenever P_k is true.

$\therefore \quad P_n$ is true for all $n \geqslant 4, \ n \in \mathbb{Z}^+$.

2 **a** $L_{k+2} = L_{k+1} + L_k$ with $L_1 = 1, \ L_2 = 2, \ L_3 = 3,$ $L_4 = 5, \ L_5 = 8, \ L_6 = 13, \ L_7 = 21, \ L_8 = 34,$ $L_9 = 55, \ L_{10} = 89$

b If $n = 1$, $\displaystyle\sum_{k=1}^{n} L_k = L_1 = 1 = 3 - 2$

If $n = 2$, $\displaystyle\sum_{k=1}^{n} L_k = L_1 + L_2 = 3 = 5 - 2$

If $n = 3$, $\displaystyle\sum_{k=1}^{n} L_k = L_1 + L_2 + L_3 = 6 = 8 - 2$

If $n = 4$, $\displaystyle\sum_{k=1}^{n} L_k = 11 = 13 - 2$

If $n = 5$, $\displaystyle\sum_{k=1}^{n} L_k = 19 = 21 - 2$

$\therefore$ we postulate that: $\displaystyle\sum_{k=1}^{n} L_k = L_{k+2} - 2$
for all $n \in \mathbb{Z}^+$.

c **Proof:** (By the Principle of Mathematical Induction)
P_n is that
"if $L_1 = 1$, $L_2 = 2$, and $L_{k+2} = L_{k+1} + L_k$,
then $\displaystyle\sum_{k=1}^{n} L_k = L_{k+2} - 2$".

(1) P_1 is true. {shown in **b**}

(2) Suppose P_t is true.

$$\begin{aligned}\therefore\ \sum_{k=1}^{t+1} L_k &= \sum_{k=1}^{t} L_k + L_{t+1}\\ &= L_{t+2} - 2 + L_{t+1}\\ &= L_{t+2} + L_{t+1} - 2\\ &= L_{t+3} - 1\end{aligned}$$

Thus P_1 is true, and P_{t+1} is true whenever P_t is true.
$\therefore$ P_n is true for all $n \in \mathbb{Z}^+$.

3 **a** $a_0 = 4000$

$$\begin{aligned}a_1 &= 4000 \times \left(1 + \frac{0.05}{12}\right) + 100\\ &= \left(\frac{1205}{1200}\right) \times a_0 + 100\\ &\approx 4116.67\\ a_2 &= \left(\frac{1205}{1200}\right) \times a_1 + 100\\ &\approx 4233.82\\ a_3 &= \left(\frac{1205}{1200}\right) \times a_2 + 100\\ &\approx 4351.46\end{aligned}$$

b The recurrence relation is $a_0 = 4000$, $a_n = ra_{n-1} + 100$,
$n \geqslant 1$ where $r = \dfrac{1205}{1200}$

Thus $a_n = r^n 4000 + 100\left(\dfrac{r^n - 1}{r - 1}\right)$ {summary table}

c After 2.5 years, $n = 30$ months

$$a_{30} = \left(\frac{1205}{1200}\right)^{30} \times 4000 + 100\left[\frac{\left(\frac{1205}{1200}\right)^{30} - 1}{\left(\frac{1205}{1200}\right) - 1}\right]$$

$$\approx 7719.92$$

$\therefore$ after 2.5 years it amounts to €7719.92

d If $10\,000 = \left(\dfrac{1205}{1200}\right)^{n} \times 4000 + 100\left[\dfrac{\left(\frac{1205}{1200}\right)^{n} - 1}{\left(\frac{1205}{1200}\right) - 1}\right]$

then $n \approx 46.69$ {technology}
$\therefore$ it will take 47 months, or 3 years and 11 months, to reach €10 000.

4 $a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} = 0$, $n \geqslant 3$
$\therefore$ $a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3}$,
where $a_0 = a_1 = 0$, $a_2 = 2$

a
$$\begin{aligned}a_3 &= 3a_2 - 3a_1 + a_0\\ &= 3 \times 2 - 3 \times 0 + 0\\ &= 6\\ a_4 &= 3a_3 - 3a_2 + a_1\\ &= 3 \times 6 - 3 \times 2 + 0\\ &= 12\\ a_5 &= 3a_4 - 3a_3 + a_2\\ &= 3 \times 12 - 3 \times 6 + 2\\ &= 20\\ a_6 &= 3a_5 - 3a_4 + a_3\\ &= 3 \times 20 - 3 \times 12 + 6\\ &= 30\end{aligned}$$

b
$$\begin{aligned}a_0 &= 0 &&= -1 \times 0\\ a_1 &= 0 &&= 0 \times 1\\ a_2 &= 2 &&= 1 \times 2\\ a_3 &= 6 &&= 2 \times 3\\ a_4 &= 12 &&= 3 \times 4\\ a_5 &= 20 &&= 4 \times 5\\ a_6 &= 30 &&= 5 \times 6\end{aligned}$$

$\therefore$ we conjecture that $a_n = n(n-1)$, $n \in \mathbb{N}$.

c From **b**, $a_0 = 0(-1)$, $a_1 = 1(0)$, and $a_2 = 2(1)$ ✓
If the conjecture is true for $r < k$ then

$$\begin{aligned}a_k &= 3a_{k-1} - 3a_{k-2} + a_{k-3}\\ &= 3(k-1)(k-2) - 3(k-2)(k-3)\\ &\quad + (k-3)(k-4)\\ &= 3(k^2 + 3k + 2) - 3(k^2 - 5k + 6)\\ &\quad + k^2 - 7k + 12\\ &= \cancel{3k^2} - 9k + \cancel{6} - \cancel{3k^2} + 15k - \cancel{18}\\ &\quad + k^2 - 7k + \cancel{12}\\ &= k^2 - k\\ &= k(k-1)\end{aligned}$$

$\therefore$ by the Principle of (strong) Mathematical Induction,
$a_n = n(n-1)$ for all $n \in \mathbb{N}$.

5 $a_{n+2} = 2a_{n+1} - 3a_n$, $n \in \mathbb{N}$, $a_0 = a_1 = 2$
has characteristic equation
$\lambda^2 - 2\lambda + 3 = 0$

$$\therefore\ \lambda = \frac{2 \pm \sqrt{4 - 4(1)(3)}}{2}$$

$$\therefore\ \lambda = \frac{2 \pm 2\sqrt{2}i}{2}$$

$$\therefore\ \lambda = 1 \pm \sqrt{2}i$$

$\therefore$ $a_n = c_1(1 + \sqrt{2}i)^n + c_2(1 - \sqrt{2}i)^n$
If $n = 0$, $a_0 = c_1 + c_2 = 2$
If $n = 1$, $a_1 = c_1(1 + \sqrt{2}i) + c_2(1 - \sqrt{2}i) = 2$

$$\therefore\ \cancel{(c_1 + c_2)} + (c_1 - c_2)\sqrt{2}i = \cancel{2}_{0}$$

$$\therefore\ (c_1 - c_2)\sqrt{2}i = 0$$

$$\therefore\ c_1 = c_2 = 1$$

$\therefore$ $a_n = (1 + \sqrt{2}i)^n + (1 - \sqrt{2}i)^n$

Alternatively, using polar form with $r = \sqrt{1^2 + (\sqrt{2})^2} = \sqrt{3}$
and $\theta = \arctan(\sqrt{2})$,

$a_n = (\sqrt{3})^n(\operatorname{cis} n\theta + \operatorname{cis}(-n\theta))$
$\therefore$ $a_n = 2(\sqrt{3})^n \cos(n\theta)$, $n \in \mathbb{N}$.

6 a has the form $a = 3m$ *or* $a = 3m + 1$ *or* $a = 3m + 2$, $m \in \mathbb{Z}^+$

$$\begin{aligned}\therefore\ a^3 + 5a = a(a^2 + 5) &= 3m((3m)^2 + 5)\\ &= 3(9m^3 + 5m)\\ \textit{or}\quad &= (3m+1)((3m+1)^2 + 5)\\ &= (3m+1)(9m^2 + 6m + 6)\\ &= (3m+1)3(3m^2 + 2m + 2)\end{aligned}$$

$$\begin{aligned} \textit{or} \quad &= (3m+2)((3m+2)^2+5) \\ &= (3m+2)(9m^2+12m+9) \\ &= (3m+2)3(3m^2+4m+3) \end{aligned}$$

So, $3 \mid a^3+5a$ for all $a \in \mathbb{Z}^+$.

7 We need to prove or disprove that $12 \mid n^2 \Rightarrow 12 \mid n$

This is not true as $12 \mid 6^2$ but $12 \nmid 6$.

8 n has the form $4m$, $4m+1$, $4m+2$, or $4m+3$

$$\begin{aligned} \therefore \quad n^2-1 &= (4m)^2-1 \\ &= 16m^2-1 \\ &= 4(4m^2-1)+3 \\ \textit{or} \quad &= (4m+1)^2-1 \\ &= 16m^2+8m \\ &= 4(4m^2+2m) \\ \textit{or} \quad &= (4m+2)^2-1 \\ &= 16m^2+16m+3 \\ &= 4(4m^2+4m)+3 \\ \textit{or} \quad &= (4m+3)^2-1 \\ &= 16m^2+24m+8 \\ &= 4(4m^2+6m+2) \end{aligned}$$

$\therefore$ n^2-1 is divisible by 4, or is of the form $4k+3$.

9 **a**

$$\begin{aligned} &\gcd(a+b,\ a+2b) \\ &= \gcd(a+2b,\ a+b) \\ &= \gcd(a+2b-(a+b),\ a+b) \\ &= \gcd(b,\ a+b) \\ &= \gcd(a+b,\ b) \\ &= \gcd(a+b-b,\ b) \\ &= \gcd(a,\ b) \\ &= 1 \end{aligned}$$

b $\gcd(a,\ b) = 1$

Let $d = \gcd(2a+b,\ a+2b)$

$$\begin{aligned} \therefore \quad d &= \gcd(2a+b-(a+2b),\ a+2b) \\ &= \gcd(a-b,\ a+2b) \\ &= \gcd(a+2b,\ a-b) \\ &= \gcd(a+2b-(a-b),\ a-b) \\ &= \gcd(3b,\ a-b) \quad \text{.... (1)} \\ &= \gcd(3b+3(a-b),\ a-b) \\ &= \gcd(3a,\ a-b) \quad \text{.... (2)} \end{aligned}$$

From (1), (2): $d \mid 3a$ and $d \mid 3b$

$\therefore$ $d \mid 3$ {as a, b are relatively prime}

$\therefore$ $d = 1$ or 3

10

$$\begin{aligned} 31 &= 17(1)+14 \\ 17 &= 14(1)+3 \\ 14 &= 3(4)+2 \\ 3 &= 2(1)+1 \end{aligned}$$

$$\begin{aligned} \therefore \quad 1 &= 3-2 \\ &= 3-(14-3(4)) \\ &= 5 \times 3 - 14 \\ &= 5(17-14)-14 \\ &= 5 \times 17 - 6 \times 14 \\ &= 5 \times 17 - 6(31-17) \\ &= 11 \times 17 - 6 \times 31 \end{aligned}$$

$\therefore$ $x_0 = 11$, $y_0 = -6$ is one solution, and $\gcd(17, 31) = 1$.

$\therefore$ solutions are $x = 11+31t$, $y = -6-17t$, $t \in \mathbb{Z}$.

11 **a** $12x - 15y = 42$

$\therefore$ $4x - 5y = 14$ where $\gcd(4, 5) = 1$

One solution is $x_0 = 1$, $y_0 = -2$

$\therefore$ solutions are $x = x_0 + bt$, $y = y_0 - at$

$\therefore$ $x = 1 - 5t$, $y = -2 - 4t$

b $32x + 24y = 144$

$\therefore$ $4x + 3y = 18$ where $\gcd(4, 3) = 1$

One solution is $x_0 = 0$, $y_0 = 6$

$\therefore$ solutions are $x = 3t$, $y = 6 - 4t$, $t \in \mathbb{Z}$.

c $18x + 11y = 196$ where $\gcd(18, 11) = 1$

One solution is $x_0 = 6$, $y_0 = 8$ {by inspection}

$\therefore$ solutions are $x = 6 + 11t$, $y = 8 - 18t$, $t \in \mathbb{Z}$.

12

$$\begin{array}{cccccccc} & 7 & 2 & 0 & 3 & 8 & 4 & 2_9 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ = & 21 & 02 & 00 & 10 & 22 & 11 & 02 \end{array}$$

0 → 00	6 → 20
1 → 01	7 → 21
2 → 02	8 → 22
3 → 10	
4 → 11	
5 → 12	

$\therefore$ $7\,203\,842_9$

$= 21\,020\,010\,221\,102_3$

13

$$\begin{aligned} n^5 - n &= n(n^4-1) \\ &= n(n^2+1)(n^2-1) \\ &= (n-1)n(n+1)(n^2+1) \end{aligned}$$

$n(n+1)$ is the product of 2 consecutive integers one of which is even

$\therefore$ $2 \mid n(n+1)$ .... (1)

$(n-1)n(n+1)$ is the product of 3 consecutive integers one of which is a multiple of 3

$\therefore$ $3 \mid (n-1)n(n+1)$ .... (2)

Now $n \equiv 0, 1, 2, 3, 4 \pmod 5$

$\therefore$ $n - 1 \equiv 4, 0, 1, 2, 3 \pmod 5$

$n + 1 \equiv 1, 2, 3, 4, 0 \pmod 5$

$n^2 + 1 \equiv 1, 2, 0, 0, 2 \pmod 5$

$\therefore$ $(n-1)n(n+1)(n^2+1) \equiv 0 \pmod 5$

$\therefore$ $5 \mid (n-1)n(n+1)(n^2+1)$ .... (3)

From (1), (2), and (3), $2 \times 3 \times 5 \mid (n-1)n(n+1)(n^2+1)$

$\Rightarrow$ $30 \mid n^5 - n$ for all $n \in \mathbb{Z}^+$.

14 $22x \equiv 41 \pmod{17}$ has $\gcd(22, 17) = 1$ and $1 \mid 41$,

$\therefore$ it has a unique solution.

$22x \equiv 41 \pmod{17}$

$\therefore$ $5x \equiv 7 \pmod{17}$

$\therefore$ $x = 15$

15 $n \equiv 3 \pmod{19}$ and $n \equiv 2 \pmod{11}$

19 and 11 are relatively prime ✓

$M = 19 \times 11 = 209$

$\therefore$ $M_1 = 11$ and $M_2 = 19$

Now $11x_1 \equiv 1 \pmod{19} \Rightarrow x_1 = 7$

$19x_2 \equiv 1 \pmod{11} \Rightarrow x_2 = 7$

$\therefore$ $x \equiv (3)(11)(7) + (2)(19)(7) \pmod{209}$

$\therefore$ $x \equiv 497 \pmod{209}$

$\therefore$ $x \equiv 79 \pmod{209}$

So, the smallest positive n is $n = 79$.

16

$$\begin{aligned} 2 \mid a \quad &\Rightarrow \quad a \equiv 0 \pmod 2 \\ 3 \mid a+2 \quad &\Rightarrow \quad a+2 \equiv 0 \pmod 3 \\ 5 \mid a+3 \quad &\Rightarrow \quad a+3 \equiv 0 \pmod 5 \\ 7 \mid a+4 \quad &\Rightarrow \quad a+4 \equiv 0 \pmod 7 \end{aligned}$$

So, $a \equiv 0 \pmod{2}$, $a \equiv 1 \pmod{3}$, $a \equiv 2 \pmod{5}$, $a \equiv 3 \pmod{7}$

2, 3, 5, and 7 are relatively prime and $M = 2 \times 3 \times 5 \times 7 = 210$

$\therefore$ $M_1 = 105$, $M_2 = 70$, $M_3 = 42$, $M_4 = 30$

Now $105x_1 \equiv 1 \pmod{2} \Rightarrow x_1 = 1$

$70x_2 \equiv 1 \pmod{3} \Rightarrow x_2 = 1$

$42x_3 \equiv 1 \pmod{5} \Rightarrow x_3 = 3$

$30x_4 \equiv 1 \pmod{7} \Rightarrow x_4 = 4$

Now $x \equiv 0 + (1)(70)(1) + (2)(42)(3) + (3)(30)(4) \pmod{210}$

$\therefore$ $x \equiv 682 \pmod{210}$

$\therefore$ $x \equiv 52 \pmod{210}$

$\therefore$ the smallest $a > 2$ is $a = 52$.

17 $4^{35}(47) - 50 \pmod{3}$

$\equiv 1^{35}(2) - 2 \pmod{3}$

$\equiv 2 - 2 \pmod{3}$

$\equiv 0 \pmod{3}$

$\therefore$ $4^{35}(47) - 50$ is divisible by 3.

18 *Statement*: $a^2 \equiv b^2 \pmod{n} \Rightarrow a \equiv b \pmod{n}$

a $4^2 \equiv 2^2 \pmod{12} \not\Rightarrow 4 \equiv 2 \pmod{12}$

$\therefore$ the statement is false.

b The converse is true.

Proof:

If $a \equiv b \pmod{n}$

$\Rightarrow$ $a = b + kn$ for some $k \in \mathbb{Z}$

$\Rightarrow$ $a^2 = (b + kn)^2 = b^2 + 2bkn + k^2n^2$

$\Rightarrow$ $a^2 = b^2 + n(2bk + k^2n)$

$\Rightarrow$ $a^2 \equiv b^2 \pmod{n}$ $\{$as $2bk + k^2n \in \mathbb{Z}\}$

c $3^2 \equiv 2^2 \pmod{5} \not\Rightarrow 3 \equiv 2 \pmod{5}$

$\therefore$ the statement is not true for n a prime.

19 If $ab \equiv 0 \pmod{n}$

$\therefore$ $ab = kn$ for $k \in \mathbb{Z}$

So, if $n = p$, a prime

then $p \mid a$ or $p \mid b$

thus $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$

That is, n would have to be prime.

20 Let $S = n^5 - 37n^3 + 36n$

$\equiv n^5 + 3n^3 \pmod{4}$

$\equiv n^3(n^2 + 3) \pmod{4}$

But $n \equiv 0, 1, 2, 3 \pmod{4}$

$\therefore$ $n^3 \equiv 0^3, 1^3, 2^3, 3^3 \pmod{4}$

$\therefore$ $n^3 \equiv 0, 1, 0, 3 \pmod{4}$

and $n^2 + 3 \equiv 3, 0, 3, 0 \pmod{4}$

$\therefore$ $n^3(n^2 + 3) \equiv 0 \pmod{4}$

$\therefore$ $S \equiv 0 \pmod{4}$

$\therefore$ $n^5 - 37n^3 + 36n$ is divisible by 4 for all $n \in \mathbb{Z}^+$.

21 $\displaystyle\sum_{k=1}^{p-1} k^p \pmod{p}$

$\equiv 1 + k + k^2 + k^3 + \dots + k^{p-1} \pmod{p}$

$\equiv \dfrac{1 - k^p}{1 - k} \pmod{p}$ $\{$sum of a geometric series$\}$

$\equiv \dfrac{1 - k}{1 - k} \pmod{p}$ $\{$FLT$\}$

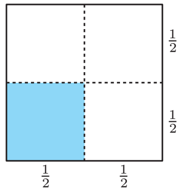
$\equiv 1 \pmod{p}$

22 There are 4 suits in a pack of cards.

These are ♥, ♦, ♣, ♠. (pigeonholes)

$\therefore$ in a hand of 5 cards, at least two will be in the same suit.

23

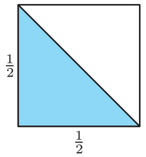


We divide the unit square into 4 squares which are $\frac{1}{2} \times \frac{1}{2}$.

Since 9 points lie in the unit square, one square must contain at least 3 points. Let it be the shaded one.

Cases:

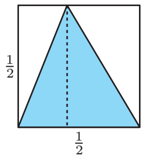
(1)



max. area $= \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$

$\therefore$ $A \leqslant \frac{1}{8}$

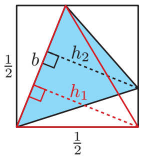
(2)



max. area $= \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$

$\therefore$ $A \leqslant \frac{1}{8}$

(3) Any other $\triangle$



Area of blue $\triangle = \frac{1}{2}bh_2$

Area of red $\triangle = \frac{1}{2}bh_1 = \frac{1}{8}$ $\{$Case (2)$\}$

where $h_2 < h_1$

$\therefore$ area of blue $\triangle <$ area of red $\triangle$

$\therefore$ area of blue $\triangle \leqslant \frac{1}{8}$

$\therefore$ we have a triangle formed by 3 points within the 1×1 square where the area is not more than $\frac{1}{8}$.

24 **a** K_m has m vertices and $\dbinom{m}{2} = \dfrac{m(m-1)}{2}$ edges.

b C_m has m vertices and m edges.

c W_m has m vertices and $2(m-1)$ edges.

d $K_{m,\,n}$ has $m + n$ vertices and mn edges.

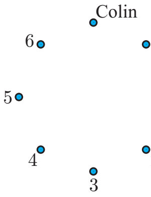
25 Consider the following graph on 8 vertices corresponding to the 8 people present.

An edge between vertices corresponds to a handshake between two people.

The 7 different answers Colin received correspond to the degrees of 7 vertices.

Since no one shakes hands with their partner the maximum $\deg(V) = 6$

$\therefore$ the 7 degrees are: 0, 1, 2, 3, 4, 5, 6.



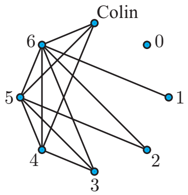
6 must shake hands with everyone except 6 and 0.

$\therefore$ 6 and 0 must be partners.

5 must shake hands with everyone except 5, 0, and 1.

$\therefore$ 5 and 1 must be partners.

Continuing in this way until all vertices have correct degree, we have



4 must partner 2, so Colin must partner 3.

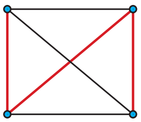
$\therefore$ **a** 3 **b** 3

26 **a** $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ **b** $\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$

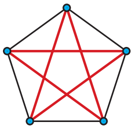
c $\begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$

27 These are examples only.

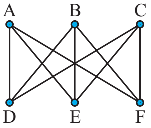
a



b



28 $K_{3,\,3}$



a 0

b For a path of length 3 between A and D, say, the path has the form A ⟶ V_1 ⟶ V_2 ⟶ D, where V_1 is E or F, and V_2 is B or C.
So, there are $2 \times 2 = 4$ different paths.

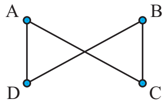
c 0

29 **a** **i** $m = n$ and $m, n > 1$.

ii m, n must both be even.

iii $m = n$, $m, n > 1$ **and** m, n both even.

b $K_{2,\,2}$



A ⟶ C ⟶ B ⟶ D ⟶ A is both a Hamiltonian cycle and an Eulerian circuit.

30 For a simple connected graph to have as many edges as possible, we consider the complete graphs K_n.

For n vertices, they have $\dfrac{n(n-1)}{2}$ edges.

Hence, we seek the lowest n such that $\dfrac{n(n-1)}{2} \geqslant 500$

$$\therefore \quad n(n-1) \geqslant 1000$$

If $n = 31$, $n(n-1) = 930$

If $n = 32$, $n(n-1) = 992$

If $n = 33$, $n(n-1) = 1056$

$\therefore$ the number of vertices must be $\geqslant 33$.

31 Since the graph is planar, $e + 2 = v + f$. {Euler's formula}

A 4-regular graph has all vertices of degree 4.

6 vertices of degree 4 $\Rightarrow$ 24 ends of edges
$\Rightarrow$ 12 edges

Thus $12 + 2 = 6 + f$
$\therefore$ $f = 8$

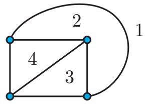
So, the graph has 8 faces.

32 G is connected planar and 3-regular. If G has order v, then the sum of the degrees of its vertices is $3v$, and so it has $\dfrac{3v}{2}$ edges.

Using Euler's formula, $e + 2 = f + v$

$$\therefore \quad \frac{3v}{2} + 2 = f + v$$

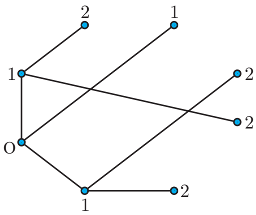
$$\therefore \quad f = \frac{v}{2} + 2$$



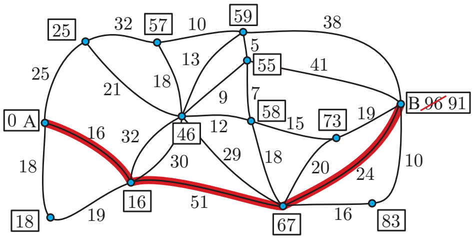
Check: K_4 has 4 vertices and 4 faces.

$\dfrac{v}{2} + 2 = \dfrac{4}{2} + 2 = 4 = f$ ✓

33



34



Shortest distance is 91 km, via the path shown.

35 There are 4 vertices with odd degrees: A, B, C, and D.

Repeating AB and CD has minimum length $10 + 13 = 23$.

Repeating AC and BD has minimum length $25 + 24 = 49$.

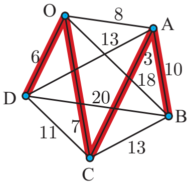
Repeating AD and BC has minimum length $22 + 15 = 37$.

Thus, we repeat AB and CD. The sum of the length of all roads is 113 $\Rightarrow$ the minimum distance $= 113 + 23 = 136$ units.

For example, this closed walk is used:

O ⟶ A ⟶ E ⟶ B ⟶ A ⟶ B ⟶ C ⟶ E ⟶ D ⟶ C ⟶ D ⟶ O

36 **a** Use Kruskal.



minimum length $= 26$

$\therefore$ upper bound 52

$\therefore$ $m \leqslant 52$

b For example, B ⟶ A ⟶ C ⟶ O ⟶ D ⟶ B gives an upper bound of 46.

$\therefore$ $m \leqslant 46$

c

Vertex deleted	*MST length*	*2 shortest deleted edges*	*Total*
A	26	3, 8	37
B	16	10, 13	39
C	24	3, 7	34
D	20	6, 11	37
O	24	6, 7	37

$\therefore$ lower bound is 39

$\therefore$ $m \geqslant 39$

d A minimum weight Hamiltonian cycle is

$\text{O} \to \text{C} \to \text{A} \to \text{B} \to \text{D} \to \text{O}$ with length 46 units

$\therefore$ $m = 46$

REVIEW SET C

1 $a_n = a_{n-1} + n - 2$ for $n \in \mathbb{Z}^+$, $a_0 = 2$

a $a_1 = a_0 - 1 = 2 - 1 = 1$ $\qquad a_2 = a_1 + 0 = 1$ $\qquad a_3 = a_2 + 1 = 2$

$a_4 = a_3 + 2 = 4$ $\qquad a_5 = a_4 + 3 = 7$

b
$$\begin{aligned} a_n &= a_{n-1} + n - 2 \\ &= (a_{n-2} + n - 3) + n - 2 \\ &= a_{n-3} + (n-4) + (n-3) + (n-2) \\ &\ \ \vdots \\ &= a_2 + 1 + 2 + 3 + \dots + (n-2) \\ &= 1 + \frac{(n-2)(n-1)}{2} \\ &= \frac{2 + n^2 - 3n + 2}{2} \\ &= \frac{n^2 - 3n + 4}{2} \end{aligned}$$

c For $n = 0$, $a_0 = \frac{4}{2} = 2$ ✓

If $a_k = \dfrac{k^2 - 3k + 4}{2}$

then
$$\begin{aligned} a_{k+1} &= \frac{k^2 - 3k + 4}{2} + k - 1 \\ &= \frac{k^2 - 3k + 4 + 2k - 2}{2} \\ &= \frac{k^2 - k + 2}{2} \\ &= \frac{k^2 + 2k + 1 - 3k - 3 + 4}{2} \\ &= \frac{(k+1)^2 - 3(k+1) + 4}{2} \end{aligned}$$

$\therefore$ by the principle of (weak) induction,

$a_n = \dfrac{n^2 - 3n + 4}{2}$ for all $n \in \mathbb{N}$.

d $a_{20} = \dfrac{20^2 - 3(20) + 4}{2} = 172$

2
$$f_{n+1} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}$$

$$\therefore \ f_{2a+1} = \sum_{k=0}^{\lfloor \frac{2a}{2} \rfloor} \binom{2a-k}{k}$$

$$\begin{aligned} &= \sum_{k=0}^{a} \binom{2a-k}{k} \\ &= \binom{2a}{0} + \binom{2a-1}{1} + \binom{2a-2}{2} \\ &\quad + \dots + \binom{a}{a} \end{aligned}$$

and
$$\begin{aligned} f_{2a} &= \sum_{k=0}^{a-1} \binom{2a-1-k}{k} \\ &= \binom{2a-1}{0} + \binom{2a-2}{1} + \binom{2a-3}{2} \\ &\quad + \dots + \binom{a}{a-1} \end{aligned}$$

When $a = 0$, $f_1 = \binom{0}{0} = 1$ ✓

When $a = 1$, $f_2 = \binom{1}{0} = 1$ ✓

and $f_3 = \binom{2}{0} + \binom{1}{1} = 1 + 1 = 2$ ✓

When $a = 2$, $f_4 = \binom{3}{0} + \binom{2}{1}$
$= 1 + 2 = 3$ ✓

and $f_5 = \binom{4}{0} + \binom{3}{1} + \binom{2}{2}$
$= 1 + 3 + 1 = 5$ ✓

Proof:
(By the Principle of Mathematical Induction (strong form))

P_n is that "$f_{n+1} = \displaystyle\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}$" for $n \geqslant 0$.

(1) We have seen that P_0 and P_1 are true.

(2) *Case 1*: k even

Assume P_r is true for all $r \leqslant k$.

Now $f_{k+2} = f_{2a+2}$ for some $a \in \mathbb{Z}$ $\qquad \{k \text{ even}\}$

$$\begin{aligned} &= f_{2a+1} + f_{2a} \\ &= \binom{2a}{0} + \underbrace{\binom{2a-1}{0} + \binom{2a-1}{1}} \\ &\quad + \underbrace{\binom{2a-2}{1} + \binom{2a-2}{2}} \\ &\quad + \underbrace{\binom{2a-3}{2} + \binom{2a-3}{3}} \\ &\quad + \dots + \underbrace{\binom{a}{a-1} + \binom{a}{a}} \\ &= \binom{2a+1}{0} + \binom{2a}{1} + \binom{2a-1}{2} \\ &\quad + \binom{2a-2}{3} + \dots + \binom{a+1}{a} \end{aligned}$$

which is of the required form.

Note: $\binom{2a+1}{0} = \binom{2a}{0} = 1$

Case 2: k odd

Assume P_r is true for all $r \leqslant k$.

$$\text{Now } f_{k+2} = f_{2a+1} \quad \text{for some } a \in \mathbb{Z} \qquad \{k \text{ odd}\}$$
$$= f_{2a} + f_{2a-1}$$
$$= \binom{2a-1}{0} + \underbrace{\binom{2a-2}{0} + \binom{2a-2}{1}}_{}$$
$$+ \underbrace{\binom{2a-3}{1} + \binom{2a-3}{2}}_{}$$
$$+ \underbrace{\binom{2a-4}{2} + \binom{2a-4}{3}}_{} + \ldots.$$
$$+ \underbrace{\binom{a}{a-2} + \binom{a}{a-1}}_{} + \binom{a-1}{a-1}$$
$$= \binom{2a}{0} + \binom{2a-1}{1} + \binom{2a-2}{2}$$
$$+ \binom{2a-3}{3} + \ldots. + \binom{a+1}{a-1} + \binom{a}{a}$$

which is of the required form.

Note: $\binom{2a}{0} = \binom{2a-1}{0} = 1$ and

$$\binom{a}{a} = \binom{a-1}{a-1} = 1$$

Thus P_0 and P_1 are true, and $P_0, P_1, \ldots., P_k \Rightarrow P_{k+1}$ is true.

$\therefore$ P_n is true for all $n \in \mathbb{N}$.

3 a i $a_0 = 120\,000$

$$a_1 = \left(1 + \frac{0.049}{12}\right)a_0 - 1000$$
$$= \left(\frac{12.049}{12}\right)a_0 - 1000$$
$$= 119\,490$$
$$a_2 = \left(\frac{12.049}{12}\right)a_1 - 1000$$
$$\approx 118\,977.92$$
$$a_3 \approx \left(\frac{12.049}{12}\right)a_2 - 1000$$
$$\approx 118\,463.74$$

ii $a_n = \left(\dfrac{12.049}{12}\right)a_{n-1} - 1000$

$a_0 = 120\,000$

iii $a_n = ra_{n-1} + b$ with $a_0 = c$ has closed form solution

$$a_n = r^n c + b\left(\frac{r^n - 1}{r - 1}\right), \quad r \neq 1$$

$$\therefore\ a_n = \left(\frac{12.049}{12}\right)^n 120\,000 - 1000\left[\frac{\left(\frac{12.049}{12}\right)^n - 1}{\left(\frac{12.049}{12}\right) - 1}\right],$$

$n \in \mathbb{N}$.

iv Loan will be repaid when $a_n = 0$

$$\therefore\ \left(\frac{12.049}{12}\right)^n 120\,000 - 1000\left[\frac{\left(\frac{12.049}{12}\right)^n - 1}{\left(\frac{12.049}{12}\right) - 1}\right] = 0$$

$\therefore$ $n \approx 165.237$ {technology}

$\therefore$ it will take 166 months or 13 years 10 months to repay the loan.

v Total interest paid = total paid − £120 000

$$\approx £165\,237 - £120\,000$$
$$\approx £45\,237$$

b i $n = 10$ years $= 120$ months

$$\text{Now } r^{120}(120\,000) + b\left(\frac{r^{120} - 1}{r - 1}\right) = 0$$
$$\therefore\ b = \frac{-r^{120}(120\,000)(r-1)}{r^{120} - 1}$$
$$\left\{n = 120,\ r = \frac{12.049}{12}\right\}$$
$$\therefore\ b \approx -1266.93$$

$\therefore$ the payment is £1266.93 per month.

ii Total interest paid ≈ £1266.93 × 120 − £120 000

≈ £32 032

4 $a_0 = 1,\ a_n = na_{n-1} + n!3^n,\ n \in \mathbb{Z}^+$

$$a_1 = a_0 + 1!3^1$$
$$= 1 + 3$$
$$= 4$$
$$a_2 = 2a_1 + 2!3^2$$
$$= 2(4) + 2 \times 9$$
$$= 26$$
$$a_3 = 3a_2 + 3!3^3$$
$$= 3(26) + 6 \times 27$$
$$= 240$$

$$a_n = na_{n-1} + n!3^n$$
$$= n[(n-1)a_{n-2} + (n-1)!3^{n-1}] + n!3^n$$
$$= n(n-1)a_{n-2} + n!3^{n-1} + n!3^n$$
$$= n(n-1)[(n-2)a_{n-3} + (n-2)!3^{n-2}] + (3^{n-1} + 3^n)n!$$
$$= n(n-1)(n-2)a_{n-3} + n!(3^{n-2} + 3^{n-1} + 3^n)$$
$$\vdots$$
$$= n!a_0 + n!(3^n + 3^{n-1} + 3^{n-2} + \ldots. + 3^2 + 3)$$
$$= n!(1 + 3 + 3^2 + \ldots. + 3^n)$$
$$= n!\left(\frac{3^{n+1} - 1}{3 - 1}\right)$$
$$= \frac{n!}{2}(3^{n+1} - 1)$$

Check: $a_0 = \frac{1}{2}(3^1 - 1) = 1$ ✓

$a_1 = \frac{1}{2}(3^2 - 1) = 4$ ✓

$a_2 = \frac{2}{2}(3^3 - 1) = 26$ ✓

$a_3 = \frac{6}{2}(3^4 - 1) = 240$ ✓

5 reds 🟥 blues 🟦🟦 greens 🟩🟩🟩

a Let a_n = number of different lines of blocks with length n units.

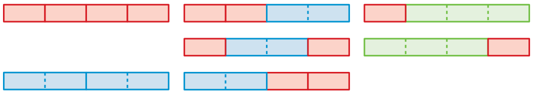
$a_1 = 1$ 🟥 (one red)

$a_2 = 2$ 🟥🟥 , 🟦🟦

$a_3 = 4$ 🟥🟥🟥 , 🟥🟦🟦 , 🟦🟦🟥 , 🟩🟩🟩

If the first block is red the remainder of the block ($n - 1$ units) can be constructed in a_{n-1} ways.
If the first block is blue, the remainder of the block ($n - 2$ units) can be constructed in a_{n-2} ways.
If the first block is green the remainder of the block ($n - 3$ units) can be constructed in a_{n-3} ways.

Thus $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ where $a_1 = 1$, $a_2 = 2$, and $a_3 = 4$ for all $n \geqslant 3$, $n \in \mathbb{Z}^+$.
Check:



$\therefore$ $a_4 = 7$ as predicted by $a_4 = a_3 + a_2 + a_1 = 7$ ✓

b $a_5 = 2 + 4 + 7 = 13$

$a_6 = 4 + 7 + 13 = 24$

$a_7 = 7 + 13 + 24 = 44$

$a_8 = 13 + 24 + 44 = 81$

$a_9 = 24 + 44 + 81 = 149$

$a_{10} = 44 + 81 + 149 = 274$

$\therefore$ there are 274 different block arrangements of length 10 units.

6 If n^2 is divisible by 5, then $5 \mid n^2$

$\therefore$ either $5 \mid n$ or $5 \mid n$ {Euclid's Lemma}

$\therefore$ $5 \mid n$ and so n is divisible by 5.

7 **a** If n is even, $n(7n^2 - 1)$ must be even.

If n is odd, n^2 is odd

$\therefore$ $7n^2 - 1$ is even

$\therefore$ $n(7n^2 - 1)$ is even.

b $n \equiv 0, 1, \text{ or } 2 \pmod 3$ for all $n \in \mathbb{Z}$

$\therefore$ $n(7n^2 - 1) \equiv 0(7 \times 0^2 - 1) \pmod 3$

or $1(7 \times 1^2 - 1) \pmod 3$

or $2(7 \times 2^2 - 1) \pmod 3$

$\therefore$ $n(7n^2 - 1) \equiv 0, 6, \text{ or } 54 \pmod 3$

$\therefore$ $n(7n^2 - 1) \equiv 0 \pmod 3$

$\therefore$ $3 \mid n(7n^2 - 1)$

c From **a** and **b**, both 2 and 3 are factors of $n(7n^2 - 1)$

$\therefore$ $6 \mid n(7n^2 - 1)$.

d $n \equiv 0, 1, 2, 3, 4, \text{ or } 5 \pmod 6$

$\therefore$ $n(7n^2 - 1) \equiv 0(7 \times 0^2 - 1) \pmod 6$

or $1(7 \times 1^2 - 1) \pmod 6$

or $2(7 \times 2^2 - 1) \pmod 6$

or $3(7 \times 3^2 - 1) \pmod 6$

or $4(7 \times 4^2 - 1) \pmod 6$

or $5(7 \times 5^2 - 1) \pmod 6$

$\therefore$ $n(7n^2 - 1) \equiv 0, 6, 54, 186, 444, \text{ or } 870 \pmod 6$

$\equiv 0 \pmod 6$

$\{54 = 9 \times 6,\ 186 = 31 \times 6,\ 444 = 74 \times 6,\ 870 = 145 \times 6\}$

8 If $7 \mid p^2$ then $7 \mid p$ or $7 \mid p$ {Euclid's Lemma}

Thus $7 \mid p^2 \ \Rightarrow\ 7 \mid p$ .... $(*)$

Suppose $\sqrt{7}$ is rational

$\therefore$ $\sqrt{7} = \dfrac{p}{q}$ where $\gcd(p, q) = 1$, $q \neq 0$

$\therefore$ $p^2 = 7q^2$ .... $(**)$

$\therefore$ $7 \mid p^2$ $\{q^2 \in \mathbb{Z}^+\}$

$\therefore$ $7 \mid p$ {from $*$}

$\therefore$ $p = 7k$, $k \in \mathbb{Z}^+$

$\therefore$ $49k^2 = 7q^2$ {from $**$}

$\therefore$ $q^2 = 7k^2$

$\therefore$ $7 \mid q^2$ $\{k^2 \in \mathbb{Z}^+\}$

$\therefore$ $7 \mid q$ {from $*$}

Thus $7 \mid p$ and $7 \mid q$ which contradicts the fact that $\gcd(p, q) = 1$.

$\therefore$ $\sqrt{7}$ must be irrational.

9 $d = \gcd(378, 168)$

Now $378 = 168(2) + 42$

and $168 = 42(4) + 0$

$\therefore$ $d = \gcd(378, 168) = 42$

Now $42 = 378 - 168(2)$

$\therefore$ $42 = 378(1) + 168(-2)$

So, $x = 1$, $y = -2$

10 Let $d = \gcd(a, b)$

$\therefore$ $d \mid a$ and $d \mid b$ and $d \geqslant 1$

$\therefore$ $a = dr$ and $b = ds$ for $r, s \in \mathbb{Z}^+$

Consider $m = \dfrac{ab}{d}$ .... $(*)$

$\therefore$ $m = \dfrac{drb}{d} = bd$ and $m = \dfrac{ads}{d} = as$

$\therefore$ m is a positive common multiple of a and b .... (1)

Now let c be any positive integer multiple of both a and b.

$\Rightarrow$ $c = au$ and $c = bv$ for $u, v \in \mathbb{Z}^+$ .... (2)

Since $d = \gcd(a, b)$, there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$

$\therefore$ $\dfrac{c}{m} = c\left(\dfrac{d}{ab}\right) = \dfrac{c(ax + by)}{ab}$

$\therefore$ $\dfrac{c}{m} = \left(\dfrac{c}{b}\right)x + \left(\dfrac{c}{a}\right)y$

$\therefore$ $\dfrac{c}{m} = vx + uy$ {from (2)}

$\therefore$ $c = (vx + uy)m$

$\therefore$ $m \mid c$ $\{vx + uy \in \mathbb{Z}\}$

$\therefore$ $m \leqslant c$

$\therefore$ $m = \operatorname{lcm}(a, b)$

Thus $\operatorname{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$

$\therefore$ $\operatorname{lcm}(a, b)\gcd(a, b) = ab$

11 Let s = number of small statues bought,
m = number of medium statues bought,
l = number of large statues bought.

$\therefore$ $s + m + l = 50$ .... (1)

and $40s + 100m + 250l = 11\,240$

(1) $\times$ -250 gives

$$-250s - 250m - 250l = -12\,500$$
$$40s + 100m + 250l = 11\,240$$

adding $-210s - 150m = -1260$

$\Rightarrow$ $21s + 15m = 126$

First we notice, $\gcd(21, 15) = 3$ and $3 \mid 126$

$\therefore$ integer solutions exist.

Now $21 = 15(1) + 6$

$15 = 6(2) + 3$

$$\begin{aligned}
\text{Thus}\quad 3 &= 15 - 6(2)\\
\therefore\quad 3 &= 15 - (21-15)\times 2\\
\therefore\quad 3 &= -2\times 21 + 3\times 15\\
\therefore\quad 126 &= -84\times 21 + 126\times 15
\end{aligned}$$

$\therefore$ one solution is $s_0 = -84,\ m_0 = 126$

Thus $s = s_0 + (\frac{15}{3})t,\quad m = m_0 - (\frac{21}{3})t$

$\therefore\ s = -84 + 5t,\quad m = 126 - 7t,\ t\in\mathbb{Z}$

But $s \geqslant 0$ and $m \geqslant 0$

$$\begin{aligned}
\therefore\quad -84+5t &\geqslant 0 &&\textit{and} & 126-7t &\geqslant 0\\
\therefore\quad 5t &\geqslant 84 &&\textit{and} & 7t &\leqslant 126\\
\therefore\quad t &\geqslant 16.8 &&\textit{and} & t &\leqslant 18
\end{aligned}$$

$\therefore\ t = 17$ or 18

Thus $s = 1,\ m = 7$ or $s = 6,\ m = 0$

$\therefore\ s = 1,\ m = 7,\ l = 42$ or
$s = 6,\ m = 0,\ l = 44$

$\therefore$ buy 1 small, 7 medium, 42 large or
6 small, 0 medium, 44 large.

12 **a** By the Fundamental Theorem of Arithmetic,

$$a = {p_1}^{a_1}{p_2}^{a_2}{p_3}^{a_3}\ldots.{p_k}^{a_k}$$

$$\therefore\ a^3 = {p_1}^{3a_1}{p_2}^{3a_2}{p_3}^{3a_3}\ldots.{p_k}^{3a_k}$$

So if $p \mid a^3$ then p is one of the p_i
where $i = 1, 2, 3, \ldots., k$
and as ${p_i}^3 \mid a$, then $p^3 \mid a^3$.

b Likewise if $p \mid a^3$ then p is one of the p_i and as all $p_i \mid a$ then $p \mid a$.

13 If $n = 1$, $\text{LHS} = 6^1 \equiv 6 \pmod{25}$
$\text{RHS} = 1 + 5 \equiv 6 \pmod{25}$ ✓

If $6^k \equiv 1 + 5k \pmod{25}$,

$$\begin{aligned}
\text{then}\quad & 6^{k+1} - 1 - 5(k+1)\\
&= 6(6^k) - 1 - 5k - 5\\
&\equiv 6(1+5k) - 5k - 6 \pmod{25}\\
&\equiv 6 + 30k - 5k - 6 \pmod{25}\\
&\equiv 25k \pmod{25}\\
&\equiv 0 \pmod{25}
\end{aligned}$$

$\therefore\ 6^{k+1} \equiv 1 + 5(k+1) \pmod{25}$

So, by induction, $6^n \equiv 1 + 5n \pmod{25}$ for $n \in \mathbb{Z}^+$.

14 $165x \equiv 105 \pmod{51}$

$\therefore\ 12x \equiv 3 \pmod{51}$ where $\gcd(3, 51) = 3$

Thus $12x \equiv 3 \pmod{51}$ has 3 mutually incongruent solutions.

One solution is $x_0 = 13$

The other solutions are $13 + \frac{51}{3},\ 13 + 2(\frac{51}{3})$

$\therefore$ the 3 mutually incongruent solutions are: 13, 30, and 47.

15 An integer is divisible by 36 if it is divisible by both 4 and 9.

If $N = 14\,975\,028\,526\,645\,824$ then

(1) N ends in 24 which is divisible by 4
$\therefore$ N is divisible by 4.

(2) N has digit sum $= 78$ where $9 \nmid 78$
$\therefore$ N is not divisible by 9.

Thus N is not divisible by 36.

16 $260 = 4\times 5\times 13$ where 4, 5, and 13 are pairwise relatively prime.

So, we need to solve:

$19x \equiv 99 \pmod 4,\ \ 19x \equiv 99 \pmod 5,\ \ 19x \equiv 99 \pmod{13}$

That is

$3x \equiv 3 \pmod 4,\quad 4x \equiv 4 \pmod 5,\quad 6x \equiv 8 \pmod{13}$

or $x \equiv 1 \pmod 4,\quad x \equiv 1 \pmod 5,\quad x \equiv 10 \pmod{13}$

We solve these using the Chinese Remainder Theorem.

$M = 4\times 5\times 13 = 260$

$\therefore\ M_1 = 65,\ M_2 = 52,\ M_3 = 20$

$$\begin{aligned}
65x_1 &\equiv 1 \pmod 4 &&\Rightarrow\ x_1 = 1\\
52x_2 &\equiv 1 \pmod 5 &&\Rightarrow\ x_2 = 3\\
20x_3 &\equiv 1 \pmod{13} &&\Rightarrow\ x_3 = 2
\end{aligned}$$

$$\begin{aligned}
\therefore\ x &\equiv (1)(65)(1) + (1)(52)(3) + (10)(20)(2) \pmod{260}\\
\therefore\ x &\equiv 621 \pmod{260}\\
\therefore\ x &\equiv 101 \pmod{260}
\end{aligned}$$

17 $14x + 17 \equiv 27 \pmod 6$

$$\begin{aligned}
\therefore\ 14x &\equiv 10 \pmod 6\\
\therefore\ 2x &\equiv 4 \pmod 6\\
\therefore\ x &\equiv 2 \pmod 3
\end{aligned}$$

$\therefore$ the solutions are $x = 2, 5, 8, \ldots.$

18

$$\begin{aligned}
& 3^{2014}\\
&= (3^2)^{1007}\\
&= 9^{1007}\\
&\equiv (-1)^{1007} \pmod{10}\\
&\equiv -1 \pmod{10}\\
&\equiv 9 \pmod{10}
\end{aligned}$$

$\therefore$ the units digit is 9.

19 $m \mid n\ \Rightarrow\ n = km$ for some $k \in \mathbb{Z}$ where $k > 1$ as $m < n$

$$\begin{aligned}
\text{Now}\quad \frac{N_n}{N_m} &= \frac{1 + 10 + 10^2 + \ldots. + 10^{n-1}}{1 + 10 + 10^2 + \ldots. + 10^{m-1}}\\
&= \frac{10^n - 1}{\cancel{10-1}} \times \frac{\cancel{10-1}}{10^m - 1}\quad \{\text{sum of geometric series}\}\\
&= \frac{10^{km} - 1}{10^m - 1}\\
&= \frac{a^k - 1}{a - 1}\quad \text{for } a = 10^m\\
&= 1 + a + a^2 + \ldots. + a^{k-1}\\
&\quad\ \text{which is an integer } > 2
\end{aligned}$$

Thus $N_n = AN_m$ for $A \in \mathbb{Z}^+,\ A > 2$

$\therefore\ N_m \mid N_n$

20 **a** Let $N = 2\,504\,304$

(1) The sum of digits $= 18$ which is divisible by 3
$\therefore$ N is divisible by 3.

$$\begin{aligned}
(2)\quad 7 \mid N &\Leftrightarrow 7 \mid 250\,430 - 2(4)\\
&\Leftrightarrow 7 \mid 250\,422\\
&\Leftrightarrow 7 \mid 25\,042 - 2(2)\\
&\Leftrightarrow 7 \mid 25\,038\\
&\Leftrightarrow 7 \mid 2503 - 2(8)\\
&\Leftrightarrow 7 \mid 2487\\
&\Leftrightarrow 7 \mid 248 - 2(7)\\
&\Leftrightarrow 7 \mid 234\\
&\Leftrightarrow 7 \mid 23 - 2(4)\\
&\Leftrightarrow 7 \mid 15 \qquad \text{which is not true}
\end{aligned}$$

$\therefore$ N is not divisible by 7.

(3) Sum of digits in odd positions − sum in even positions

$= (2+0+3+4) - (5+4+0)$

$= 9 - 9$

$= 0$ which is divisible by 11

$\therefore$ N is divisible by 11.

(4) $13 \mid N \Leftrightarrow 13 \mid 250\,430 - 9(4)$

$\Leftrightarrow 13 \mid 250\,394$

$\Leftrightarrow 13 \mid 25\,039 - 9(4)$

$\Leftrightarrow 13 \mid 25\,003$

$\Leftrightarrow 13 \mid 2500 - 9(3)$

$\Leftrightarrow 13 \mid 2473$

$\Leftrightarrow 13 \mid 247 - 9(3)$

$\Leftrightarrow 13 \mid 220$

$\Leftrightarrow 13 \mid 22 - 9(0)$

$\Leftrightarrow 13 \mid 22$

which is not true

$\therefore$ N is not divisible by 13.

b Let $N = 1\,703\,702$

(1) Sum of digits $= 20$ which is not divisible by 3.

$\therefore$ N is not divisible by 3.

(2) $7 \mid N \Leftrightarrow 7 \mid 170\,370 - 2(2)$

$\Leftrightarrow 7 \mid 170\,366$

$\Leftrightarrow 7 \mid 17\,036 - 2(6)$

$\Leftrightarrow 7 \mid 17\,024$

$\Leftrightarrow 7 \mid 1702 - 2(4)$

$\Leftrightarrow 7 \mid 1694$

$\Leftrightarrow 7 \mid 169 - 2(4)$

$\Leftrightarrow 7 \mid 161$

$\Leftrightarrow 7 \mid 16 - 2(1)$

$\Leftrightarrow 7 \mid 14$

which is true

$\therefore$ N is divisible by 7.

(3) Sum of digits in odd positions − sum in even positions

$= (1+0+7+2) - (7+3+0)$

$= 0$ which is divisible by 11

$\therefore$ N is divisible by 11.

(4) $13 \mid N \Leftrightarrow 13 \mid 170\,370 - 9(2)$

$\Leftrightarrow 13 \mid 170\,352$

$\Leftrightarrow 13 \mid 17\,035 - 9(2)$

$\Leftrightarrow 13 \mid 17\,017$

$\Leftrightarrow 13 \mid 1701 - 9(7)$

$\Leftrightarrow 13 \mid 1638$

$\Leftrightarrow 13 \mid 163 - 9(8)$

$\Leftrightarrow 13 \mid 91$

which is true

$\therefore$ N is divisible by 13.

21 $7^{80} = (7^{10})^8$

$\equiv 1^8 \pmod{11}$ {FLT}

$\equiv 1 \pmod{11}$

$\therefore$ the last digit of 7^{80} is 1 in base 11.

22 Split the first 100 positive integers into 50 groups of 2:
(1, 2), (3, 4), (5, 6), ..., (97, 98), (99, 100).
In selecting 51 integers, there must be at least one group with both numbers selected {PHP}, and these numbers are consecutive.

23 A contains $2^{15} - 1 = 32\,767$ non-empty subsets.
The highest possible sum of the elements in a non-empty subset is $199 + 198 + 197 + ... + 185 = 2880$
So, there are 2880 possible sums of non-empty subsets.
Since $32\,767 > 2880$, by the PHP there are two distinct subsets which have the same sum (lie in the same pigeonhole).

24 Suppose the graph has v vertices. The sum of the edges of G and G' is the number of edges of K_v.

$$\therefore \quad 17 + 11 = \frac{v(v-1)}{2}$$

$$\therefore \quad v(v-1) = 56$$

$$\therefore \quad v^2 - v - 56 = 0$$

$$\therefore \quad (v-8)(v+7) = 0$$

$$\therefore \quad v = 8 \quad \{\text{as } v > 0\}$$

$\therefore$ G has 8 vertices.

25 Since G is bipartite, it has two disjoint sets of vertices.
Suppose there are m vertices in one set and $v - m$ vertices in the other.
If G is simple, the total number of edges possible is $m(v-m) = -m^2 + mv$, which is a quadratic in m whose maximum occurs when $m = \dfrac{-v}{2(-1)} = \dfrac{v}{2}$.

$\therefore$ the maximum possible number of edges is $\dfrac{v}{2} \times \dfrac{v}{2} = \dfrac{v^2}{4}$,

that is, $e \leqslant \dfrac{v^2}{4}$.

Or, alternatively:

In $K_{m,\,n}$, $v = m + n$ and $e = mn$

Now $v^2 - 4e = m^2 + 2mn + n^2 - 4mn$

$= m^2 - 2mn + n^2$

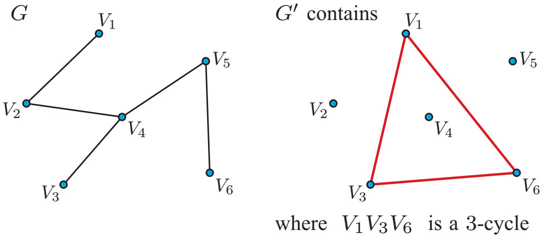
$= (m-n)^2$

$\geqslant 0$ for all $m, n \in \mathbb{Z}^+$

$\therefore$ $v^2 \geqslant 4e$

$\therefore$ $e \leqslant \dfrac{v^2}{4}$

26 **a** For example:



where $V_1V_3V_6$ is a 3-cycle

b For such a group of 6 people, we define a graph on 6 vertices where each person corresponds to a distinct vertex.
Two vertices are adjacent $\Leftrightarrow$ the two people are known to each other.
By **a**, such a graph either contains a 3-cycle or has 3 mutually non-adjacent vertices.
That is, either there is a group of 3 people who are mutually known to each other *or* the 3 are mutual strangers.

27 Suppose there are n vertices, each of different degree.
For the graph to be simple, the highest degree that any vertex can be is $n - 1$.
Hence the degrees must be $0, 1, 2, ..., n-1$.

However, this is a contradiction because if a simple graph has a vertex with degree $n-1$ then it must be connected, yet we also have a vertex with degree 0.

$\therefore$ there are at most $n-1$ different degrees.

Case 1: The $n-1$ degrees are $0, 1, 2, 3, ..., n-2$ (a disconnected graph).

Case 2: The $n-1$ degrees are $1, 2, 3, ..., n-1$ (a connected graph).

Since there are n vertices (pigeons) and at most $n-1$ distinct possible degrees (pigeonholes), by the PHP there exist 2 vertices of the same degree.

28 **a** **i** Eulerian **ii** Hamiltonian

b **i** semi-Eulerian **ii** semi-Hamiltonian

c **i** neither **ii** Hamiltonian

d **i** Eulerian **ii** Hamiltonian

29 **a** G has v vertices and e edges.

G' has v vertices and $\binom{v}{2} - e$ edges.

$$\therefore\ e = \binom{v}{2} - e$$

$$\therefore\ 2e = \frac{v(v-1)}{2}$$

$$\therefore\ e = \frac{v(v-1)}{4}$$

b From **a**, $v(v-1) = 4e$

$$\Rightarrow\ 4 \mid v(v-1)$$

But v and $v-1$ are consecutive integers which cannot both be even.

$\therefore\ 4 \mid v$ or $4 \mid v-1$

$\therefore\ v = 4k$ or $v - 1 = 4k$ for some $k \in \mathbb{Z}$

$\therefore\ v \equiv 0 \pmod 4$ or $v \equiv 1 \pmod 4$

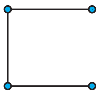
c From **b**, $v = 4, 8, 12, 16, 20$ or $1, 5, 9, 13, 17$

v	e
~~1~~	~~0~~
4	3
5	5
8	14
9	18

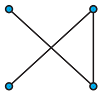
v	e
12	33
13	39
16	60
17	68
20	95

d For $v = 4$, $e = 3$ $\{v = 1$ and $e = 0$ is trivial$\}$

G:



and G':



30 **a** For a tree, $f = 1$ and $e = v - 1$

$$\therefore\ v + f - e = v + 1 - (v-1)$$
$$= 2$$

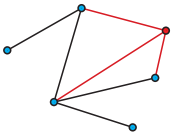
b Consider a connected, planar graph is n vertices, f_n faces, and e_n edges.

Proof: (By the Principle of Mathematical Induction)

P_n is that "$n + f_n - e_n = 2$" for $n \geqslant 1$.

(1) If $n = 1$, G is a single vertex ●
where $v = 1$, $f = 1$, $e = 0$
$\therefore\ v + f - e = 2$ ✓
$\therefore\ P_1$ is true.

(2) Assume that, for a graph with k vertices, $k + f_k - e_k = 2$.
Now consider adding a $(k+1)$th vertex to the graph. Suppose c of the existing vertices are joined to the new vertex.



This increases the number of edges by c, and the number of faces by $c - 1$ (adding 1 edge does not create a new face, but each extra edge after that creates a new cycle, and hence a new face).

$$\begin{aligned}\therefore\ \ & (k+1) + f_{k+1} - e_{k+1} \\ &= k + 1 + (f_k + c - 1) - (e_k + c) \\ &= k + f_k - e_k \\ &= 2\end{aligned}$$

Thus, by induction, P_n is true for all $n \in \mathbb{N}$.

31 **a** As each finite face is bordered by at least a 3-cycle, then each finite face has degree $\geqslant 3$.

Each infinite face has degree $\geqslant 3$ also.

$\therefore$ every face has degree $\geqslant 3$

$$\therefore\ \sum \deg(F) \geqslant 3f$$
$$\therefore\ 2e \geqslant 3f$$
$$\therefore\ 3f \leqslant 2e$$

By Euler's formula, $v + f - e = 2$

$$\therefore\ 3v + 3f - 3e = 6$$
$$\therefore\ 3e - 3v + 6 \leqslant 2e$$
$$\therefore\ e \leqslant 3v - 6$$

b G and G' both have 11 vertices.

For G, $v = 11$, $e_G = e$

For G', $v = 11$, $e_{G'} = \binom{11}{2} - e$

$$\therefore\ e_{G'} = 55 - e$$

If G is planar, $e \leqslant 3v - 6$ {from **a**}

$\therefore\ e \leqslant 27$ $\{v = 11\}$

$$\therefore\ 55 - e \geqslant 28$$
$$\therefore\ e_{G'} \geqslant 28$$

$\therefore$ G' is not planar.

32 Suppose G has order n. Together, G and G' have the same number of edges as K_n, that is $\binom{n}{2} = \frac{n(n-1)}{2}$.

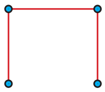
However, if G and G' are both trees, then they both must have $n - 1$ edges.

$$\text{Thus, } \frac{n(n-1)}{2} = 2(n-1)$$
$$\therefore\ n(n-1) = 4(n-1)$$
$$\therefore\ (n-1)(n-4) = 0$$
$$\therefore\ n = 1 \text{ or } 4$$

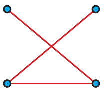
But $n = 1$ is not a particularly sensible solution.

So, G has order 4.

G



G'



33 **a** The graph has two vertices with odd degree, B and C.

$\therefore$ while it it not Eulerian, it is semi-Eulerian.

$\therefore$ if we start and finish at B and C (either order), we can walk around all tunnels without having to repeat any.

b B → A → E → B → C → E → D → C

c **i** BC

ii The sum of the lengths of the tunnels

$= 126 + 110 + 147 + 146 + 133 + 95 + 74$ m

$= 831$ m

$\therefore$ minimum distance $= 831 + 146$

$= 977$ m

INDEX