

Number theory

1

Objectives

After completing this chapter you should be able to:

- Use the division theorem and the Euclidean algorithm → pages 0–0
- Use the Euclidean algorithm to illustrate Bezout's theorem → pages 0–00
- Understand and use modular arithmetic and congruences → pages 00–00
- Use Fermat's little theorem to find least positive residues → pages 00–00
- Solve simple congruence equations → pages 00–00
- Apply tests for divisibility by 2, 3, 4, 5, 6, 9, 10 and 11 and planes → pages 00–00
- Solve counting problems → pages 00–00
- Use permutations and combinations → pages 00–00

Modular arithmetic is an essential part of modern **public key** cryptography. This is a form of encryption in which anyone can encode a message, but only one person can decode it. It is based on the principle that computers are able to multiply large numbers much more quickly than they are able to factorise them.

Prior knowledge check

- 1 Prove, by contradiction, that there are infinitely many prime numbers.
← Pure Year 2, Chapter 1
- 2 Prove, by induction, that for all $n \in \mathbb{Z}$, $n \geq 7$, $3^n < n!$ ← Core Pure Book 1, Section 8.1
- 3
 - a Write 108 and 180 as products of their prime factors.
 - b Hence find the greatest common divisor and least common multiple of 108 and 180.
← GCSE Mathematics
- 4 Prove, by induction, that for all $n \in \mathbb{Z}^+$, $n^3 + 2n$ is divisible by 3.
← Core Pure Book 1, Section 8.2
- 5 A suitcase combination lock consists of three digits. Each digit is chosen from the set $\{0, 1, 2, 3, 4, 5, 6\}$. Find the number of different possible codes. ← GCSE Mathematics

1.1 The division algorithm

Number theory is the study of systems and properties of numbers. Of particular interest are the system of integers, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, and the system of natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$. The concept of **divisibility** is very important in number theory.

- If a and b are integers with $a \neq 0$, then b is divisible by a if there exists an integer k such that $b = ka$. In this case, we say that a divides b and denote this by $a \mid b$. If a does not divide b then we write $a \nmid b$.

Notation a is called a **divisor** or **factor** of b .

In the past, you may have only considered the positive divisors of a number, but the definition above applies to both positive and negative integers.

Example 1

Given that $a \mid b$, show that $-a \mid b$.

$b = ka$ for some integer k .
If k is an integer, then $-k$ is also an integer,
and $b = (-k)(-a)$ so $-a \mid b$ as required.

This is the definition of divisibility.

Example 2

For each pair of integers below, determine whether the first integer divides the second.

a 11, 143

b -4, 28

c 15, 47

d 3, 2

a $143 = 13 \times 11 \Rightarrow 11 \mid 143$
b $28 = (-7)(-4) \Rightarrow -4 \mid 28$
c $3 \times 15 = 45$ and $4 \times 15 = 60$ so $15 \nmid 47$
d $0 \times 3 = 0$ and $1 \times 3 = 3$ so $3 \nmid 2$

If $a > b$ then $a \nmid b$.

Example 3

Find all the divisors of:

a 8

b 11

a $\pm 1, \pm 2, \pm 4, \pm 8$
b ± 1 and ± 11

11 is a prime number so its divisors are only ± 1 and ± 11 .

You need to be able to apply the following properties of divisibility:

- For any $a, b, c \in \mathbb{Z}$, with $a \neq 0$:
 - $a \mid a$ (every integer divides itself)
 - $a \mid 0$ (0 is divisible by any integer)
 - $a \mid b$ and $b \mid c \Rightarrow a \mid c$
 - $a \mid b$ and $a \mid c \Rightarrow a \mid bn + cm$ for all $m, n \in \mathbb{Z}$
 - $a \mid b \Leftrightarrow an \mid bn$ for all $n \in \mathbb{Z}, n \neq 0$
 - If a and b are positive integers and $a \mid b$ then $a \leq b$

Notation $\Leftrightarrow$ means 'if and only if'.
It means that the implication works in both directions, so $a \mid b \Rightarrow an \mid bn$ and $an \mid bn \Rightarrow a \mid b$

Example 4

Given $a, b, c \in \mathbb{Z}$, prove that if $a \mid b$ and $a \mid c$ then $a \mid bn + cm$ for all $m, n \in \mathbb{Z}$.

$b = ja$ for some $j \in \mathbb{Z}$
 $c = ka$ for some $k \in \mathbb{Z}$
 $bn + cm = (ja)n + (ka)m$
 $\quad = (jn + km)a$
 Since $j, k, n, m \in \mathbb{Z}$, $jn + km \in \mathbb{Z}$, so $a \mid bn + cm$, as required.

Write down the facts you know from the definition of divisibility. Use these facts to show that $bn + cm$ can be written as an integer multiple of a .

Notation The expression $bn + cm$, where $n, m \in \mathbb{Z}$, is called a **linear combination** of b and c .

When you multiply, add or subtract two integers, the result is always an integer. However, the quotient of two integers is not necessarily an integer.

Notation You can say that $\mathbb{Z}$ is **closed** under the operations of addition, subtraction and multiplication, but not closed under the operation of division.

Because of this, it is helpful to define division within the integers more rigorously. The **division algorithm** allows you to find a unique **quotient** and **remainder** for any two integers:

If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.

- 1 Begin with values of a and b .
- 2 Set q equal to the greatest integer that is less than or equal to $\frac{a}{b}$.
- 3 Set $r = a - bq$.

Notation You call q the **quotient** and r the **remainder**. You also call a the **dividend** and b the **divisor**.

Note that a is divisible by b if and only if the remainder, r , in the division algorithm is zero.

Example 5

Use the division algorithm to find integers q and r such that:

a $94 = 13q + r$

b $-232 = 11q + r$

a $\frac{94}{13} = 7.23\dots$ so $q = 7$
 $r = a - bq = 94 - 13 \times 7 = 3$
 So $94 = 13 \times 7 + 3$

b $\frac{-232}{11} = -21.09\dots$ so $q = -22$
 $r = a - bq = -232 - 11 \times (-22) = 10$
 So $-232 = 11 \times (-22) + 10$

$a = 94$ and $b = 13$

q must be less than or equal to $\frac{a}{b}$. The greatest integer less than or equal to $-21.09\dots$ is -22 .

Watch out There are other integers that satisfy $a = bq + r$, such as $94 = 13 \times 5 + 29$, but there is only one pair of values that satisfies this relationship **and** where $0 \leq r < b$.

Example 6

Use the division algorithm to prove that, for all integers n , n^2 leaves a remainder of 0 or 1 when divided by 4.

$n = 4q + r$, where $q \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3\}$
 Consider $n^2 = (4q + r)^2 = 16q^2 + 8qr + r^2$
 $r = 0 \Rightarrow n^2 = 16q^2 = 4(4q^2)$, so remainder is 0 when divided by 4.
 $r = 1 \Rightarrow n^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1$, so remainder is 1 when divided by 4.
 $r = 2 \Rightarrow n^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1)$, so remainder is 0 when divided by 4.
 $r = 3 \Rightarrow n^2 = 16q^2 + 24q + 9 = 4(4q^2 + 6q + 2) + 1$, so remainder is 1 when divided by 4.
 Therefore, in all cases, the remainder when n^2 is divided by 4 is 0 or 1.

Problem-solving

From the division algorithm, you know that n must be able to be written in this form. Consider each possible value of r separately. This is an example of a **proof by exhaustion**. ← Pure Year 1, Section 7.5

Because of the division algorithm, you know that you have covered all possible cases for n .

Exercise 1A

1 For each pair of integers below, determine whether the first divides the second:

a 7, 21

b 8, 2

c -25, 25

d 12, 140

2 If $n \in \mathbb{Z}$ and $n \mid 15$, write down all the possible values of n .

3 Find all the divisors of:

a 12

b 20

c -6

d 1

(P) **4** Prove, for positive integers a and b , that $a \mid b \Rightarrow an \mid bn$ for all $n \in \mathbb{Z}$, $n \neq 0$.

(P) **5** Prove that if $a \mid b$ and $b \mid c$ then $a \mid c$.

6 For each of the following integer pairs (a, b) find integers q and r such that $a = qb + r$, where $0 \leq r < b$:

a (121, 9)

b (-148, 12)

c (51, 9)

d (-51, 9)

e (544, 84)

f (-544, 84)

g (44, 84)

h (5723, 100)

7 Find the quotient and remainder when:

a 200 is divided by 7

b -52 is divided by 3

c 22 000 is divided by 13

d 752 is divided by 57

(P) 8 Prove that the cube of any integer has one of the following forms, for some $k \in \mathbb{Z}$.

$9k, 9k + 1, 9k + 8$

Hint By the division algorithm, any integer can be written in the form $3q, 3q + 1$ or $3q + 2$ for some $q \in \mathbb{Z}$.

(P) 9 Show that the square of an odd integer is of the form $8k + 1$ for some integer k .

(P) 10 Use the division algorithm to prove that the fourth power of any integer is either of the forms $5k$ or $5k + 1$ for some $k \in \mathbb{Z}$.

(P) 11 Show that for all integers $a \geq 1$, $\frac{a(a^2 + 2)}{3}$ is an integer.

Challenge

a Prove that there exist unique integers p and s such that $a = bp + s$

with $-\frac{|b|}{2} < s \leq \frac{|b|}{2}$

b Find p and s given that $a = 49$ and $b = 26$.

1.2 The Euclidean algorithm

You can use the definition of divisibility to write formal definitions of common divisors and greatest common divisors.

■ If a, b , and c are integers and $c \neq 0$, then c is called a **common divisor** of a and b if $c \mid a$ and $c \mid b$.

If a and b are integers with at least one of them not equal to zero, then you define the **greatest common divisor** of a and b , as the largest positive integer which divides a and b .

■ The **greatest common divisor** of two integers a and b is a positive integer d that satisfies the two conditions:

• $d \mid a$ and $d \mid b$

• If c is a common divisor of a and b , then $c \leq d$

Notation The greatest common divisor of a and b is written as $\gcd(a, b)$. It is also sometimes called the **highest common factor** of a and b .

Example 7

Find:

a $\gcd(3, 12)$

b $\gcd(25, 25)$

c $\gcd(90, 84)$

a $\gcd(3, 12) = 3$

b $\gcd(25, 25) = 25$

c $90 = 2 \times 3^2 \times 5 \quad 84 = 2^2 \times 3 \times 7$
So $\gcd(90, 84) = 2 \times 3 = 6$

If $a \mid b$, then $\gcd(a, b) = a$

$\gcd(a, a) = a$

In GCSE mathematics, you found greatest common divisors by writing numbers as products of their prime factors. However, writing a number as a product of prime factors can be very time consuming, especially if the number does not have small prime factors.

The **Euclidean algorithm** provides a method for quickly finding the greatest common divisor of any two integers.

Given positive integers a and b with $a \geq b$:

- 1 Apply the division algorithm to a and b to find integers q_1 and r_1 such that $a = q_1b + r_1$, where $0 \leq r_1 < b$. If $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$.
- 2 If $r_1 \neq 0$, apply the division algorithm to b and r_1 to find integers q_2 and r_2 such that $b = q_2r_1 + r_2$ where $0 \leq r_2 < r_1$. If $r_2 = 0$, then $\gcd(a, b) = r_1$.
- 3 If $r_2 \neq 0$, continue the process. This results in the system of equations:

$$a = q_1b + r_1$$

$$b = q_2r_1 + r_2$$

$$r_1 = q_3r_2 + r_3$$

$$\vdots$$

$$r_{n-2} = q_nr_{n-1} + r_n$$

$$r_{n-1} = q_{n+1}r_n + 0$$

The last non-zero remainder in this process, r_n , is the greatest common divisor of a and b : $\gcd(a, b) = r_n$.

Problem-solving

This is an iterative process. At the k th step you are applying the division algorithm to r_{k-1} and r_{k-2} to find q_k and r_k such that $r_{k-2} = q_kr_{k-1} + r_k$. By the division algorithm, the remainder must be strictly less than the divisor ($r_k < r_{k-1}$), so the sequence of remainders $r_1, r_2, r_3, \dots$ must be strictly decreasing. Since all the remainders are non-negative integers, this means that this sequence must terminate at 0 in a finite number of steps. The last **non-zero** remainder in the sequence is the greatest common divisor of a and b .

Example 8

Use the Euclidean algorithm to find the greatest common divisor of 306 and 657.

$$657 = 2 \times 306 + 45$$

$$306 = 6 \times 45 + 36$$

$$45 = 1 \times 36 + 9$$

$$36 = 4 \times 9 + 0$$

$$\text{So } \gcd(306, 657) = 9$$

Apply the division algorithm to 306 and 657.

Apply the division algorithm again, using the original divisor and your remainder.

Watch out You must show every application of the division algorithm, including the final step with a remainder of 0.

9 is the last non-zero remainder.

You can use the Euclidean algorithm and back substitution to write the greatest common divisor of two numbers as a **linear combination** of those two numbers.

- **Bezout's identity states that if a and b are non-zero integers, then there exist integers x and y such that $\gcd(a, b) = ax + by$.**

Problem-solving

The gcd of two integers a and b is the **smallest** positive integer that can be written as a linear combination of a and b .

→ Exercise 1B, Challenge

Example 9

Use the Euclidean algorithm to find integers x and y such that $306x + 657y = 9$.

From Example 8, $\gcd(306, 657) = 9$, and

$$45 = 1 \times 36 + 9$$

$$\text{So } 9 = 45 - 1(36)$$

$$= 45 - (306 - 6(45))$$

$$= 7 \times 45 - 1(306)$$

$$= 7(657 - 2(306)) - 1(306)$$

$$= 7(657) - 14(306) - 1(306)$$

$$= -15(306) + 7(657)$$

$$\text{Hence } x = -15 \text{ and } y = 7$$

9 is the gcd of 306 and 657 so Bezout's identity states that x and y must exist.

Work backwards through the steps of the Euclidean algorithm from Example 8.
Rearrange $45 = 36 \times 1 + 9$

Rearrange $306 = 45 \times 6 + 36$ to write 36 as a linear combination of 306 and 45. You can then use this result to write 9 as a linear combination of 306 and 45.

Rearrange $657 = 306 \times 2 + 45$ to write 45 as a linear combination of 657 and 306. You can then substitute and rearrange to write 9 as a linear combination of 657 and 306, as required.

Example 10

Use the Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that $\gcd(143, 252) = 143x + 252y$.

$$252 = 1 \times 143 + 109$$

$$143 = 1 \times 109 + 34$$

$$109 = 3 \times 34 + 7$$

$$34 = 4 \times 7 + 6$$

$$7 = 1 \times 6 + 1$$

$$6 = 1 \times 6 + 0$$

$$\text{So } \gcd(143, 252) = 1$$

$$1 = 7 - 6$$

$$= 7 - (34 - 4(7))$$

$$= 5(7) - 34$$

$$= 5(109 - 3(34)) - 34$$

$$= 5(109) - 16(34)$$

$$= 5(109) - 16(143 - 109)$$

$$= 21(109) - 16(143)$$

$$= 21(252 - 143) - 16(143)$$

$$= -37(143) + 21 \times 252$$

$$\text{Hence } x = -37 \text{ and } y = 21.$$

Apply the Euclidean algorithm.

The only positive integer that divides both 143 and 252 is 1.

Work backwards through the steps in the Euclidean algorithm.

In the previous example, the only positive integer which divided both 252 and 143 was 1. Pairs of numbers with this property are said to be **relatively prime** or **coprime**.

- **Two integers a and b are relatively prime if $\gcd(a, b) = 1$.**
- **The integers a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$.**

Notation

If and only if, or **iff**, mean that two statements are equivalent. It can also be represented by the symbol $\Leftrightarrow$.

In this case,

- if $ax + by = 1$, then a and b are relatively prime
- if a and b are relatively prime, then $ax + by = 1$.

Example 11

Find:

- a Use the Euclidean algorithm to show that 49 and 60 are relatively prime.
- b Find integers x and y such that $49x + 60y = 1$
- c Hence find integers p and q such that $49p + 60q = 5$

$$\text{a } 60 = 49 \times 1 + 11$$

$$49 = 4 \times 11 + 5$$

$$11 = 2 \times 5 + 1$$

$$\text{So } \gcd(49, 60) = 1$$

Apply the Euclidean algorithm to 49 and 60.

This confirms that 49 and 60 are coprime.

$$\begin{aligned}
 \text{b } 1 &= 11 - 2(5) \\
 &= 11 - 2(49 - 4(11)) \\
 &= 9(11) - 2(49) \\
 &= 9(60 - 49) - 2(49) \\
 &= 9(60) - 11(49) \\
 &= -11(49) + 9(60)
 \end{aligned}$$

Hence $x = -11$ and $y = 9$

$$\begin{aligned}
 \text{c } -11(49) + 9(60) &= 1 \\
 \Rightarrow -55(49) + 45(60) &= 5 \\
 \text{Therefore } p &= -55 \text{ and } q = 45
 \end{aligned}$$

Use back substitution within the Euclidean algorithm to find x and y .

Multiply by 5.

Exercise 1B

1 Find:

a $\gcd(7, 7)$

b $\gcd(100, 20)$

c $\gcd(15, 18)$

(P) 2 If $\gcd(p, 42) = 6$ where $p \in \mathbb{Z}^+$, write down three different possible values of p .

3 Use the Euclidean algorithm to find the greatest common divisor of each pair of integers. Show each step of the algorithm.

a $a = 32, b = 78$

b $a = 91, b = 104$

c $a = 172, b = 64$

d $a = 167, b = 117$

e $a = -323, b = 221$

f $a = 1292, b = 884$

(E) 4 Use the Euclidean algorithm to find the highest common factor of 143 and 910. (3 marks)

Hint 'Highest common factor' means the same thing as 'greatest common divisor'.

(E) 5 a Use the Euclidean algorithm to find the greatest common divisor of 222 and 1050. (3 marks)

b Hence write the fraction $\frac{222}{1050}$ in its simplest form. (1 mark)

6 For each pair of numbers, find integers x and y such that $ax + by = \gcd(a, b)$.

a $a = 32, b = 78$

b $a = 91, b = 104$

c $a = 12\,378, b = 3054$

d $a = -119, b = 272$

e $a = 2378, b = 1769$

f $a = -2059, b = 2581$

(E) 7 a Use the Euclidean algorithm to show that 39 and 16 are relatively prime. (3 marks)

b Hence find integers, p and q such that $39p + 16q = 1$. (2 marks)

(E) 8 Use the Euclidean algorithm to find integers a and b such that $170a + 21b = 1$. (4 marks)

(E) 9 a Find integers x and y such that $172x + 20y = \gcd(172, 20)$, (4 marks)

b Hence, find a solution to the equation $172x + 20y = 100$, $x, y \in \mathbb{Z}$. (2 marks)

- E/P** 10 Find a solution to the equation $99a + 345b = 300$, $a, b \in \mathbb{Z}$. (5 marks)
- E/P** 11 The functions f and g are defined as $f(n) = 8n + 3$ and $g(n) = 5n + 2$, $n \in \mathbb{Z}^+$.
- a Find $\gcd(f(1), g(1))$. (2 marks)
- b Show that $f(n)$ and $g(n)$ are relatively prime for all $n \in \mathbb{Z}^+$. (4 marks)
- E/P** 12 a Show that $\gcd(a, a+x) \mid x$, where a and x are any two integers. (3 marks)
- b Hence or otherwise show that any two consecutive integers are relatively prime. (2 marks)
- E/P** 13 a Use the Euclidean algorithm to find the highest common factor of 63 and -23 . (3 marks)
- b Hence, find x_0 and y_0 such that $x = x_0$, $y = y_0$ is a solution to $63x - 23y = -7$. (1 mark)
- c Show that $x = x_0 - 23t$, $y = y_0 - 63t$, $t \in \mathbb{Z}$, is also a solution to $63x - 23y = -7$. (2 marks)
- d Find t such that $xy \leq 0$, or otherwise argue that it is not possible. (2 marks)

Challenge

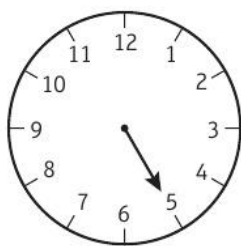
- 1 Prove that $\gcd(a, b) = \gcd(a + bc, b)$ for all $a, b, c \in \mathbb{Z}$.
- 2 Given that $\gcd(a, b) = d$, and $ax + by = z$, where $a, b, x, y, z \in \mathbb{Z}$ and $z > 0$, prove that $z \geq d$.

Problem-solving

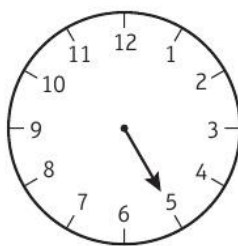
Show that if d is a common divisor of a and b then it is also a common divisor of $a + bc$ and b , and vice versa.

1.3 Modular arithmetic

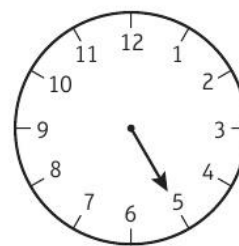
Modular arithmetic is a system of arithmetic that is restricted to the remainders when integers are divided by a given integer, called the modulus. You can visualise the case when the modulus is 12 by looking at the hour hand on a standard clock face:



5 hours after noon, the hour hand points at 5 o'clock.



After a further 12 hours, the hour hand points at 5 o'clock again. 17 hours have passed in total. In arithmetic **modulo 12** the numbers 5 and 17 are **congruent**. You write $5 \equiv 17 \pmod{12}$.



After 29 hours have passed, the hour hand points at 5 o'clock again. 29 is congruent to both 17 and 5 modulo 12.

This relationship is called **modular congruence**. You can define it for any modulus using divisibility.

- Let m be a positive integer. If a and b are integers, then a is congruent to b modulo m if $m \mid (a - b)$.

Notation

If a is congruent to b modulo m , then you write $a \equiv b \pmod{m}$. If a is not congruent to b modulo m , then you write $a \not\equiv b \pmod{m}$.

In the example of the clock face, $29 - 5 = 24$ and $12 \mid 24$, so $29 \equiv 5 \pmod{12}$. You can think of integers that are congruent modulo m as having the **same remainder** when divided by m .

$a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when they are divided by m .

Watch out Neither a nor b is necessarily the remainder.

Example 12

Decide whether the following statements are true or false.

a $24 \equiv 9 \pmod{5}$

b $5 \equiv -11 \pmod{8}$

c $4 \equiv 17 \pmod{2}$

- a** $24 - 9 = 15$ and $5 \mid 15$ so true
b $5 - (-11) = 16$ and $8 \mid 16$ so true
c $4 - 17 = -13$ and $2 \nmid -13$ so false

24 and 9 both leave a remainder of 4 when divided by 5.

Adding or subtracting integer multiples of the modulus produces congruent numbers.

■ **If $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{m}$ for some positive integer m if and only if there exists an integer k such that $a = b + km$.**

You can use this fact to find numbers that are congruent to a given number.

Example 13

Given that $n \equiv 10 \pmod{3}$, write down:

a three different possible values of n

b the greatest negative value of n

c the value of n contained in the set $\{0, 1, 2\}$

- a** 10, 13, 16
b -2
c 1

$$10 - 4 \times 3 = -2$$

You need to know the following properties of congruences:

- **$a \equiv 0 \pmod{m}$ if and only if $m \mid a$** $28 \equiv 0 \pmod{4}$ and $4 \mid 28$
- **$a \equiv a \pmod{m}$** $3 \equiv 3 \pmod{5}$
- **If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$** $7 \equiv 4 \pmod{3}$ and $4 \equiv 7 \pmod{3}$
- **If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$** $11 \equiv 8 \pmod{3}$ and $8 \equiv 2 \pmod{3}$, then $11 \equiv 2 \pmod{3}$

Example 14

Given that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, prove that $a \equiv c \pmod{m}$.

$$a \equiv b \pmod{m} \Rightarrow m \mid (a - b)$$

$$\text{So there exists an integer } k \text{ such that } km = a - b \quad (1)$$

$$b \equiv c \pmod{m} \Rightarrow m \mid (b - c)$$

$$\text{So there exists an integer } j \text{ such that } jm = b - c \quad (2)$$

Add together (1) and (2):

$$(k + j)m = a - c$$

Since k and j are integers, $k + j$ must be an integer.

$$\text{So } m \mid (a - c) \Rightarrow a \equiv c \pmod{m}$$

Use the definition of modular congruence and the definition of divisibility.

You also need to know the following **rules of arithmetic** for modular congruences.

▪ Let $a, b, c, d, m, n \in \mathbb{Z}$ and $m, n > 0$, with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

- $a \pm c \equiv b \pm d \pmod{m}$
- $ac \equiv bd \pmod{m}$
- $ka \equiv kb \pmod{m}$
- $a^n \equiv b^n \pmod{m}$

Example 15

Show that $23^{753} \equiv 1 \pmod{11}$.

$$23 \equiv 1 \pmod{11} \Rightarrow 23^{753} \equiv 1^{753} \equiv 1 \pmod{11}$$

Example 16

Find the remainder when 343^5 is divided by 11.

$$343 = 31 \times 11 + 2, \text{ so } 343 \equiv 2 \pmod{11}$$

$$\text{So } 343^5 \equiv 2^5 \equiv 32 \pmod{11}$$

$$32 = 2 \times 11 + 10, \text{ so } 32 \equiv 10 \pmod{11}$$

$$\text{So } 343^5 \equiv 10 \pmod{11}$$

So the remainder when 343^5 is divided by 11 is 10.

Find the remainder when 343 is divided by 11.

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

Example 17

Work out the final digit in the number 513^{50} .

$$\begin{aligned} 513 &\equiv 3 \pmod{10} \\ \text{So } 513^{50} &\equiv 3^{50} \pmod{10} \\ 3^2 &\equiv 9 \equiv -1 \pmod{10} \\ (3^2)^{25} &\equiv (-1)^{25} \equiv -1 \equiv 9 \pmod{10} \\ \text{So the last digit of } 513^{50} &\text{ is } 9. \end{aligned}$$

Finding the last digit of a number is the same as finding its remainder when you divide by 10.

Problem-solving

3^{50} is still too large to work out on your calculator. Look for ways of simplifying the power. You can write 3^{50} as $(3^2)^{25} = 9^{25}$. Because $9 \equiv -1 \pmod{10}$ it is easy to work out large powers of 9 (mod 10).

Example 18

Find the remainder when 19^{273} is divided by 12.

$$\begin{aligned} 19 &\equiv 7 \pmod{12} \\ 19^2 &\equiv 49 \pmod{12}, \text{ but } 49 \equiv 1 \pmod{12} \Rightarrow \\ 19^2 &\equiv 1 \pmod{12} \\ 19^{273} &= 19^{272} \times 19 = (19^2)^{136} \times 19 \\ (19^2)^{136} &\equiv 1^{136} \equiv 1 \pmod{12} \\ \text{So } 19^{273} &\equiv 1 \times 7 \equiv 7 \pmod{12} \\ \text{So the remainder when } 19^{273} &\text{ is divided by 12 is } 7. \end{aligned}$$

7^{273} is still much too large to calculate. But if there is some small power of 7 for which $7^n \equiv 1 \pmod{12}$ then you can use powers of powers to simplify your working.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$

Example 19

Find the remainder when $1! + 2! + \dots + 100!$ is divided by 15

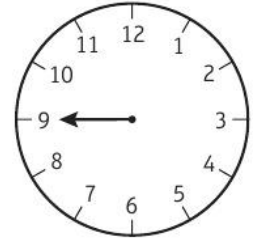
$$\begin{aligned} \text{When } n \geq 5, n! &\equiv 0 \pmod{15} \\ 1! + 2! + \dots + 100! &\equiv 1! + 2! + 3! + 4! + 0 \\ &\quad + \dots + 0 \pmod{15} \\ &\equiv 1 + 2 + 6 + 24 \pmod{15} \\ &\equiv 3 \pmod{15} \\ \text{So the remainder is } &3. \end{aligned}$$

For all $n \geq 5$, $n!$ contains factors of both 3 and 5, and hence contains a factor of 15.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$

Exercise 1C

- 1 The diagram shows a clock face 9 hours after noon.
Determine the number that the hour hand is pointing to:
- a 13 hours after noon b 20 hours after noon
c 100 hours after noon d 999 hours after noon.



- 2 Decide whether the following statements are true or false.
- a $15 \equiv 3 \pmod{6}$ b $19 \equiv -6 \pmod{5}$ c $102 \equiv 245 \pmod{2}$
d $431 \equiv 277 \pmod{11}$ e $2146 \equiv 0 \pmod{4}$ f $-50 \equiv 118 \pmod{12}$
- 3 Given that $n \equiv 8 \pmod{7}$, write down:
- a three different possible positive values of n
b three different possible negative values of n
c a value of n such that $0 \leq n < 7$.

Problem-solving

Use the definition of modular congruence and the definition of divisibility.

- (P)** 4 Given that $a \equiv b \pmod{m}$, prove that $b \equiv a \pmod{m}$

- (E/P)** 5 Amy writes down the following rule for modular arithmetic:

$$a \equiv -a \pmod{m}$$

- a Give a counter-example to show that Amy's rule is not generally true. **(2 marks)**
b Explain the conditions under which Amy's rule will be true. **(3 marks)**
- 6 The serial number of a certain currency is 11 digits long. The first 10 digits of the serial number are followed by a security check digit. If the note is genuine, then the 10-digit number will be congruent to the check digit (mod 9).
Check whether the following two serial numbers are genuine:
a serial number 51177875501 b serial number 88100245327

- 7 Show that:
- a $21^{201} \equiv 1 \pmod{5}$ b $99^{99} \equiv -1 \pmod{10}$
c $217^{1000} \equiv 0 \pmod{7}$ d $23^{75} \equiv 7 \pmod{8}$

- (E)** 8 Find the remainder when 218^6 is divided by 9. **(2 marks)**
- (E)** 9 a Find the remainder when 7^{50} is divided by 50. **(3 marks)**
b Hence find the remainder when 7^{51} is divided by 50. **(1 mark)**

- (E)** 10 Find the final digit in the number 1004^{200} . (3 marks)
- (E/P)** 11 Find the remainder when $1! + 2! + 3! + \dots + 50!$ is divided by 21. (3 marks)
- (E/P)** 12 Show that $2^{100} + 3^{100} + 4^{100} + 5^{100} \equiv 0 \pmod{3}$ (4 marks)
- (P)** 13 **a** Given that $a \equiv b \pmod{m}$ prove by induction that $a^k \equiv b^k \pmod{m}$, where $k \in \mathbb{Z}^+$
b By means of a counter example, show that the converse of this rule is not true.
- (E)** 14 Prove that $5^{22} + 17^{22} \equiv 6 \pmod{11}$ (4 marks)
- (E/P)** 15 **a** Find the units digit in 2018^9 (2 marks)
b Find the units digit in 9^{2018} (3 marks)
c Hence, find the units digit in $2018^9 + 9^{2018}$ (1 mark)
- (E/P)** 16 Find the remainder when 129^{123} is divided by 127 (4 marks)
- (E/P)** 17 The number $n = \sum_{r=1}^{100} r!$. Find:
a the final digit in n (2 marks)
b the final two digits in n (3 marks)

Problem-solving

For part **b** you need to find values of a, b, k and m such that $a^k \equiv b^k \pmod{m}$ but $a \not\equiv b \pmod{m}$.

Challenge

Find the last two digits of:

- a** 19^{198} **b** $11^{12^{13}}$ **c** 7^{7^7}

1.4 Divisibility tests

You have probably used some simple mental rules to determine whether numbers are divisible by 2, 5 or 10:

- **An integer is divisible by:**
 - **2 if and only if its last digit is even**
 - **5 if and only if its last digit is 5 or 0**
 - **10 if and only if its last digit is 0**

You can prove that these results work using modular arithmetic. In order to do this you need to write the number as a sum of its digits multiplied by powers of 10:

- A number N with decimal digits $a_n a_{n-1} a_{n-2} \dots a_1 a_0$ can be written as $10^n a_n + 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots + 10 a_1 + a_0$

For example, you can write the 4-digit number 7835 as $1000 \times 7 + 100 \times 8 + 10 \times 3 + 5$.

Note Because each of the a_i are decimal digits they are integers between 0 and 9.

Example 20

Prove that a positive integer N is divisible by 10 if and only if its last digit is 0.

Let N be the number with decimal digits

$a_n a_{n-1} a_{n-2} \dots a_1 a_0$

$$\text{So } N = 10^n a_n + 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots + 10 a_1 + a_0$$

$$\text{So } N \equiv 0 + 0 + 0 + \dots + 0 + a_0 \pmod{10}$$

$$\text{So } N \equiv a_0 \pmod{10}$$

$$\text{So } a_0 = 0 \Rightarrow N \equiv 0 \pmod{10} \Rightarrow 10 \mid N$$

$$\text{Conversely, } 10 \mid N \Rightarrow N \equiv 0 \pmod{10}$$

$$\Rightarrow a_0 \equiv 0 \pmod{10} \Rightarrow a_0 = 0$$

Write the decimal expansion of N and consider it modulo 10. Any term containing a positive power of 10 will be congruent to 0 (mod 10).

a_0 is the last digit of N .

Watch out This is an 'if or only if' proof so you need to prove both directions:
Last digit 0 $\Rightarrow 10 \mid N$ **and** $10 \mid N \Rightarrow$ last digit 0

a_0 is an integer between 0 and 9, so $a_0 \equiv 0 \pmod{10} \Rightarrow a_0 = 0$

You need to know and understand similar rules for divisibility by 3, 4, 6, 9 and 11:

- An integer is divisible by:
- 3 if and only if the sum of its digits is divisible by 3
 - 4 if and only if its last two digits are divisible by 4
 - 6 if and only if it is divisible by both 2 and 3
 - 9 if and only if the sum of its digits is divisible by 9
 - 11 if and only if the difference between the sum of its digits with even position and the sum of its digits with odd position is divisible by 11

This is the **alternating sum** of the digits. If a number has digits $abcde\dots$ then it is divisible by 11 if and only if $a - b + c - d + e - \dots$ is divisible by 11.

Example 21

N is a 3-digit number abc , so that $N = 100a + 10b + c$, where $a, b, c \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $a \neq 0$.

Prove that $11 \mid N$ if and only if $11 \mid (a - b + c)$.

Let $N = 100a + 10b + c$

$100 \equiv 1 \pmod{11}$

$10 \equiv -1 \pmod{11}$

So $N \equiv a - b + c \pmod{11}$

So $N \equiv 0 \pmod{11}$ if and only if $a - b + c \equiv 0 \pmod{11}$

So $11 \mid N$ if and only if $11 \mid (a - b + c)$

Use the addition and multiplication rules for modular arithmetic.

Example 22

Use the divisibility rules to determine whether:

a 7146 is divisible by 9

b 5838 is divisible by 6

c 2261914 is divisible by 4

d 813747 is divisible by 11

a $7 + 1 + 4 + 6 = 18$ and $9 \mid 18$ so $9 \mid 7146$

b $2 \mid 8$ so $2 \mid 5838$

$5 + 8 + 3 + 8 = 24$ and $3 \mid 24$ so $3 \mid 5838$

Hence $6 \mid 5838$

c $14 = 3 \times 4 + 2$ so $4 \nmid 14$.

So $4 \nmid 2261914$

d $8 - 1 + 3 - 7 + 4 - 7 = 0$

$11 \mid 0$ so $11 \mid 813747$

The sum of the digits must be divisible by 9.

To be divisible by 6 the number must be divisible by both 2 and 3.

Check to see if the final two digits are divisible by 4.

The sum of the digits with even position (from the right) is $4 + 3 + 8 = 15$

The sum of the digits with odd position (from the right) is $7 + 7 + 1 = 15$

Remember that 0 is divisible by any integer.

You can apply these rules for divisibility to find numbers with given properties.

Example 23

N is a 3-digit number abc , so that $N = 100a + 10b + c$, where a , b and c are integers between 0 and 9, with $a \neq 0$. N has the following properties:

- N is divisible by 9
- The sum of the digits of N is even
- $N \equiv 3 \pmod{11}$

Find all possible values for N , showing your working clearly.

Fact 1: $9 \mid a + b + c$, so $a + b + c = 9p$ for some $p \in \mathbb{Z}$

Fact 2: $a + b + c = 2q$ for some $q \in \mathbb{Z}$

Since $a, b, c \leq 9$, $a + b + c \leq 27$

So $a + b + c = 9$ or 18 or 27

Since $a + b + c$ is even, $a + b + c = 18$ (1)

Fact 3: $100a + 10b + c \equiv 3 \pmod{11}$

$100 \equiv 1 \pmod{11}$ and $10 \equiv -1 \pmod{11}$

so $a - b + c \equiv 3 \pmod{11}$

Since $0 \leq a, b, c \leq 9$

$a - b + c = -8$ or 3 or 14

(2)

From (1) and (2),

$18 - 2b = -8$ or 3 or 14

So $2b = 26$ or 15 or 4

Since b is an integer between 0 and 9,

$2b = 4$ and $b = 2$

Hence from (1), $a + 2 + c = 18$, so $a + c = 16$.

Possibilities are:

$a = 8, c = 8$

$a = 7, c = 9$

$a = 9, c = 7$

So the possible values of N are 828, 729 and 927.

Write out the properties mathematically.

Problem-solving

Remember that a , b and c represent decimal digits. You will need to use the fact that they must be integers between 0 and 9 to make deductions. Make sure you write down all of your reasoning.

So far you have only used the first two facts. Write out fact 3, then use modular arithmetic to simplify.

Use the restrictions on a , b and c again to write down possible values of $a - b + c$. The least possible value of $a - b + c$ is -9 and the greatest possible value is 18, so write down any integers in this range that are congruent to 3 (mod 11).

$$a - b + c = a + b + c - 2b$$

Use the condition on b to choose the only possible value of b .

Exercise 1D

1 Showing all of your working, use the divisibility rules to determine whether:

- | | |
|-----------------------------|------------------------------|
| a 2502 is divisible by 9 | b 5931 is divisible by 3 |
| c 101795 is divisible by 11 | d 2000560 is divisible by 4 |
| e 51792 is divisible by 6 | f 1326094 is divisible by 11 |

- (P)** 2 Prove that a positive integer N is divisible by 2 if and only if its last digit is divisible by 2.
- (P)** 3 Prove that a positive integer N is divisible by 5 if and only if its last digit is 5 or 0.
- (P)** 4 N is a 3-digit number abc , so that $N = 100a + 10b + c$, where $a, b, c \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $a \neq 0$.
Prove that $9 \mid N$ if and only if $9 \mid (a + b + c)$.
- (P)** 5 N is a 5-digit number $abcde$, so that $N = 10000a + 1000b + 100c + 10d + e$, where $a, b, c, d, e \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $a \neq 0$.
Prove that $11 \mid N$ if and only if $11 \mid (a - b + c - d + e)$.
- (E/P)** 6 N is a positive integer, the sum of whose digits is divisible by 3. Prove that N is divisible by 3. **(4 marks)**
- Problem-solving**

You need to prove this for a general integer with any number of digits.
- (E/P)** 7 Prove that any positive integer is divisible by 4 if and only if its final two digits are divisible by 4. **(4 marks)**
- (E)** 8 Use divisibility tests to show that 6 159 285 is divisible by both 9 and 11, showing your working clearly. **(2 marks)**
- (E)** 9 The following 8-digit number has a missing digit.
102 x 5761
Given that the number is divisible by 11, find the value of the missing digit. **(2 marks)**
- (E/P)** 10 The following 8-digit number has two missing digits.
2 a 8455 b 8
Given that the number is divisible by both 11 and 9, find the values of the missing digits. **(3 marks)**
- (P)** 11 Find all possible three-digit numbers which are divisible by both 9 and 11.
- 12 m is a 2-digit number that can be written as ab , so that $m = 10a + b$, where a, b and c are integers between 0 and 9, with $a \neq 0$.
Given that m is divisible by 9 and that $m \equiv 5 \pmod{11}$,
- explain why $a + b$ must equal 9 or 18
 - show that $b - a$ must equal either -6 or 5 .
 - Hence, or otherwise, show that there is exactly one possible value of m and find that value.

- E/P** 13 N is a 2-digit number that can be written as ab , so that $N = 10a + b$, where a, b and c are integers between 0 and 9, with $a \neq 0$.
Given that the sum of the digits of N is divisible by 4 and that $N \equiv 7 \pmod{8}$, find all the possible values of N . **(4 marks)**

- E/P** 14 x is a 3-digit positive integer which has the following properties:
- x is divisible by 11
 - The sum of the digits of x is odd
 - $x \equiv 8 \pmod{9}$
- Find all possible values of x , showing your working clearly. **(6 marks)**

- E/P** 15 Q is a 4-digit number satisfying $1000 \leq Q \leq 9999$.
 Q can be written $abcd$, so that $Q = 1000a + 100b + 10c + d$, where a, b, c and d are integers between 0 and 9, with $a \neq 0$. Q has the following properties:
- Q is divisible by 11 and 3
 - $Q \equiv 5 \pmod{9}$ and $Q \equiv 4 \pmod{11}$
 - The sum of the digits of Q is even.
 - The digits of Q are strictly increasing, so that $a < b < c < d$.
- Find all the possible values for Q , showing your working clearly. **(8 marks)**

Challenge

In **base m** , the number with digits $a_n a_{n-1} a_{n-2} \dots a_1 a_0$ is equal to

$$m^n a_n + m^{n-1} a_{n-1} + m^{n-2} a_{n-2} + \dots + m a_1 + a_0$$

So for example, the base 8 number 357 can be written as a decimal number as

$$8^2 \times 3 + 8 \times 5 + 7 = 239$$

- Prove that a number written in base 8 is divisible by 7 if the sum of its digits is divisible by 7.
- Write down rules for divisibility by 2, 4 and 8 in base 8.
- Find rules for divisibility by 2, 3 and 6 in base 7.

1.5 Solving congruence equations

A You can find solutions to equations written using modular arithmetic. Equations involving modular congruences are called **congruence equations**. Their solutions are usually given in terms of **least residues**.

- The set $\{0, 1, 2, 3, \dots, n-1\}$ is called the **set of least residues modulo n** .

Solving a congruence equation means finding the least residues which satisfy that equation.

Notation A solution in the form $x \equiv n \pmod{m}$ where $0 \leq n \leq m-1$ represents an infinite number of solutions congruent to $n \pmod{m}$. This solution could also be written as $\{n + km : k \in \mathbb{Z}\}$.

Example 24

A

Solve the equation $x \equiv 86 \pmod{7}$.

$$x \equiv 2 \pmod{7}$$

$86 = 12 \times 7 + 2$. Write the solution as a least residue modulo 7.

Notation

You can say that 2 is the least residue of 86 modulo 7.

You can use inverse operations to solve congruence operations involving + and −.

Example 25Solve the equation $x + 15 \equiv 3 \pmod{10}$.

$$x \equiv -12 \pmod{10}$$

$$x \equiv 8 \pmod{10}$$

Subtract 15 from both sides, and then write the solution as a least residue.

You need to be more careful when solving congruence equations of the form $ax \equiv b \pmod{m}$. In some cases this equation has **no solution**, and in some cases it has **multiple solutions** within the set of least residues modulo m .

- Let $a, b, m \in \mathbb{Z}$, with $m > 0$ and $\gcd(a, m) = d$.
 - If $d \nmid b$, then the equation $ax \equiv b \pmod{m}$ has **no solutions**.
 - If $d \mid b$ then the equation $ax \equiv b \pmod{m}$ has d solutions in the set of least residues modulo m .

Problem-solving

If $d \mid b$, then $ax \equiv b \pmod{m}$ will have a unique solution in the set of least residues modulo $\frac{m}{d}$. → **Example 28**

If $\gcd(a, m) = 1$ (a and m are relatively prime) then $ax \equiv b \pmod{m}$ will have a unique solution in the set of least residues modulo m .

→ **Example 29**

Example 26Explain why the equation $14x \equiv 7 \pmod{22}$ has no solutions.

$$\gcd(14, 22) = 2$$

$2 \nmid 7$, so the equation has no solutions.

If a and b have a common factor you can simplify the equation by dividing. The rules for **dividing** (or **cancelling**) in modular arithmetic depend on whether the divisor and the modulus are relatively prime.

- If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod{m}$.
- If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = d$, then $a \equiv b \pmod{\frac{m}{d}}$.

Example 27

A Solve the equation $2n \equiv 26 \pmod{14}$.

$$\begin{aligned}\gcd(2, 14) &= 2 \\ 2 \times n &\equiv 2 \times 13 \pmod{14} \\ n &\equiv 13 \pmod{7} \\ n &\equiv 6 \pmod{7}\end{aligned}$$

You can cancel 2 on both sides of the congruence. But 2 and 14 are not relatively prime, so you need to divide the modulus by $\gcd(2, 14) = 2$ when you cancel.

Problem-solving

$\gcd(2, 14) = 2$, so $2n \equiv 26 \pmod{14}$ will have **two solutions** in the set of least residues modulo 14, or a unique solution in the set of least residues modulo $\frac{14}{2} = 7$.

You could write the solution as $n \equiv 6$ or $13 \pmod{14}$.

Example 28

Solve the equation $42y \equiv 168 \pmod{35}$.

$$\begin{aligned}42y &= 14 \times 3y \text{ and } 168 = 14 \times 12 \\ \text{So } 14 \times 3y &\equiv 14 \times 12 \pmod{35} \\ 3y &\equiv 12 \pmod{5} \\ y &\equiv 4 \pmod{5}\end{aligned}$$

$$\gcd(14, 35) = 7, \text{ so } 3y \equiv 12 \pmod{\frac{35}{7}}.$$

$\gcd(3, 5) = 1$ so you can cancel a factor of 3 on both sides of the congruence without changing the modulus.

$42y \equiv 168 \pmod{35}$ would have $\gcd(42, 35) = 7$ solutions in the set of least residues modulo 35. You could write the answer as $y = 4, 9, 14, 19, 24, 29$ or $34 \pmod{35}$.

If you know that $ax \equiv b \pmod{m}$ has a solution, and you have reduced the equation as much as possible by cancelling, then you need to find a **multiplicative inverse** of a .

- **A multiplicative inverse of a modulo m is an integer p that satisfies $ap \equiv 1 \pmod{m}$. The multiplicative inverse exists if and only if $\gcd(a, m) = 1$.**

You can find multiplicative inverses using Bezout's identity:

If a and m are relatively prime, there exist integers p and q which satisfy

$$ap + mq = 1 \quad \text{---} \quad ap + mq = \gcd(a, m) = 1$$

$$ap = 1 - mq$$

$$\Rightarrow ap \equiv 1 \pmod{m}$$

Any number that can be written as $1 \pm$ an integer multiple of m is congruent to 1 (mod m).

So p is a multiplicative inverse of a modulo m .

Problem-solving

If the equation has a solution then $\gcd(a, m) \mid b$, so you can use the laws of division to reduce the equation to one in which a and m are relatively prime.

Example 29**A**

- a Find a multiplicative inverse of 10 modulo 63.
 b Hence solve the equation $10x \equiv 4 \pmod{63}$.

a $63 = 6 \times 10 + 3$
 $10 = 3 \times 3 + 1$
 $3 = 3 \times 1 + 0$
 $\Rightarrow \gcd(10, 63) = 1$, so the equation has a unique solution modulo 63.
 $1 = 10 - 3(3)$
 $= 10 - 3(63 - 6(10))$
 $= 19(10) - 3(63)$
 So $19(10) = 1 + 3(63)$
 So 19 is a multiplicative inverse of 10 modulo 63.

b $10x \equiv 4 \pmod{63}$
 $19 \times 10x \equiv 76 \pmod{63}$
 $x \equiv 13 \pmod{63}$

You need to find Bezout's identity for 10 and 63. Apply the Euclidean algorithm.

Work backwards through the steps in the Euclidean algorithm.

Multiply both sides by the multiplicative inverse of 10.

$19 \times 10 \equiv 1 \pmod{63}$ so $19 \times 10x \equiv x \pmod{63}$.
 And $76 = 63 + 13$, so $76 \equiv 13 \pmod{63}$.

You know there is only one solution modulo 63, so you are finished.

Example 30

Solve $75x \equiv 12 \pmod{237}$.

$237 = 3 \times 75 + 12$
 $75 = 6 \times 12 + 3$
 $12 = 4 \times 3 + 0$
 $\Rightarrow \gcd(75, 237) = 3$, so the equation has three solutions modulo 237.

Method 1

$3 = 75 - 6(12)$
 $= 75 - 6(237 - 3(75))$
 $= 19(75) - 6(237)$
 So $19(75) = 3 + 6(237)$
 $19(75) \equiv 3 \pmod{237}$
 $76(75) \equiv 12 \pmod{237}$

So 76 is one solution.

$$\frac{237}{3} = 79$$

Other solutions are $76 + 79 = 155$ and
 $76 + 2(79) = 234$
 $x \equiv 76, 155 \text{ or } 234 \pmod{237}$

If you can't spot the gcd of 75 and 237, you can start by using the Euclidean algorithm.

Problem-solving

When $\gcd(a, m) \neq 1$ there are two possible methods:

Method 1

- Use back substitution to find p and q such that $ap + mq = \gcd(a, m)$
- Multiply everything by $\frac{b}{\gcd(a, m)}$ to find k such that $ka \equiv b \pmod{m}$.
- k is one solution.
- Add multiples of $\frac{m}{\gcd(a, m)}$ to find $\gcd(a, m)$ distinct solutions modulo m .

A

Method 2

$$75x \equiv 12 \pmod{237}$$

$$25x \equiv 4 \pmod{79}$$

Euclidean algorithm on 25 and 79:

$$79 = 3 \times 25 + 4$$

$$25 = 6 \times 4 + 1$$

$$4 = 4 \times 1 + 0$$

$$\gcd(25, 79) = 1$$

$$1 = 25 - 6(4)$$

$$= 25 - 6(79 - 3(25))$$

$$= 19(25) - 6(79)$$

$$\text{So } 19(25) = 1 + 6(79)$$

$$19 \times 25 \equiv 1 \pmod{79}$$

So 19 is a multiplicative inverse of 25 modulo 79.

$$25x \equiv 4 \pmod{79}$$

$$x \equiv 76 \pmod{79}$$

Problem-solving**Method 2**

- Divide everything by $\gcd(a, m)$, including the modulus, to simplify the equation.
- You will now have an equation of the form $px \equiv q \pmod{r}$ with p and r relatively prime.
- Find a multiplicative inverse for p modulo r and multiply through by this inverse.

Notice that the coefficients in Bezout's identity are the same for the reduced equation.

Multiply both sides of the congruence by 19. The 25 disappears because 19 is the multiplicative inverse of 25.

Exercise 1E

1 Write down the least residue of:

a 20 modulo 9

b 7 modulo 2

c 120 modulo 15

d 91 modulo 20

2 Solve:

a $x \equiv 30 \pmod{7}$

b $x \equiv 69 \pmod{9}$

c $x \equiv -60 \pmod{6}$

d $x \equiv -63 \pmod{11}$

e $x \equiv -38 \pmod{17}$

f $2 + x \equiv 3 \pmod{9}$

g $x + 5 \equiv 21 \pmod{9}$

h $x - 3 \equiv 50 \pmod{11}$

3 Given that $27n \equiv 81 \pmod{15}$, show that $n \equiv 3 \pmod{5}$.

4 a Use the Euclidean algorithm to show that 91 and 20 are relatively prime.

b Hence solve $91n \equiv 455 \pmod{20}$.

5 Solve:

a $10x \equiv 20 \pmod{7}$

b $3x \equiv 9 \pmod{8}$

c $5x \equiv 15 \pmod{3}$

d $3x \equiv 12 \pmod{9}$

e $6x \equiv 18 \pmod{15}$

f $20x \equiv 200 \pmod{30}$

Hint You can solve these congruence equations using the division (cancelling) laws. Make sure your solution represents all possible solutions.

- A** **6 a** Write down the set of least residues modulo 12.

P **b** Find all the members of this set that satisfy $4x \equiv 8 \pmod{12}$.

E **7 a** Use the Euclidean algorithm to find integers a and b such that $120a + 733b = 1$. (4 marks)

b Hence solve the equation $120x \equiv 1 \pmod{733}$. (1 mark)

E **8 a** Use the Euclidean algorithm to find integers a and b such that $571a + 50b = 1$. (4 marks)

b Hence write down the multiplicative inverse of 50 modulo 571. (1 mark)

c Solve the equation $50x \equiv 3 \pmod{571}$ (2 marks)

9 Find the multiplicative inverse of:

a 7 modulo 10 **b** 3 modulo 4

c 12 modulo 37 **d** 70 modulo 99

10 Solve each of the following congruence equations.

a $5x \equiv 2 \pmod{7}$ **b** $5x \equiv 9 \pmod{49}$ **c** $3x \equiv 2 \pmod{78}$

d $8x \equiv 7 \pmod{13}$ **e** $15x \equiv 7 \pmod{91}$ **f** $10x \equiv 9 \pmod{27}$

11 Solve each of the following congruence equations, or state, with a reason, if no solutions exist.

a $9x \equiv 15 \pmod{21}$ **b** $14x \equiv 13 \pmod{21}$ **c** $9x \equiv 12 \pmod{15}$

d $490x \equiv 750 \pmod{800}$ **e** $12x \equiv 9 \pmod{18}$ **f** $15x \equiv 9 \pmod{25}$

E/P **12** Given that $\gcd(a, m)$ is the smallest integer that can be written as a linear combination of a and m , prove that the equation $ax \equiv b \pmod{m}$, where $a, b, m \in \mathbb{Z}$, has no solutions if $\gcd(a, m) \nmid b$. (4 marks)

E/P **13 a** Use the Euclidean algorithm to find the highest common factor of 80 and 702. (3 marks)

b Hence state the number of distinct solutions to the equation $80x \equiv 20 \pmod{702}$ in the set of least residues modulo 702. (1 mark)

c Find all of these possible solutions. (4 marks)

E/P **14 a** Show that the equation $39x \equiv 10 \pmod{216}$ has no solutions. (4 marks)

b Solve the equation $39x \equiv 9 \pmod{216}$. (4 marks)

E/P **15** Find all possible integers in the range $0 \leq n < 29$ that satisfy $21n \equiv 12 \pmod{30}$. (5 marks)

E/P **16** Solve the congruence equation $25x \equiv 6 \pmod{277}$. (5 marks)

E/P **17** Find all possible positive integers, x , less than 100 that satisfy $28x \equiv 20 \pmod{100}$. (5 marks)

E/P **18** Solve the congruence equation $70x \equiv 20 \pmod{925}$. (5 marks)

1.6 Fermat's little theorem

A You can use Fermat's little theorem to find least residues of powers quickly, and to solve some congruence equations involving powers.

■ **Fermat's little theorem states that, if p is a prime number and a is any number not divisible by p , then**

- $a^{p-1} \equiv 1 \pmod{p}$
- $a^p \equiv a \pmod{p}$

Problem-solving

You can prove this theorem by considering the product of the least positive residues of p . You do not need to know the proof for your examination. → **Mixed exercise, Challenge**

The two statements of the theorem given above are equivalent. You can use them to state without any calculation that, for example

$$3^{22} \equiv 1 \pmod{23} \quad \text{— 23 is a prime number.}$$

$$500^{101} \equiv 500 \pmod{101}$$

$$\equiv 96 \pmod{101} \quad \text{— 101 is a prime number and } 101 \nmid 500.$$

Example 31

Find the least residue of 3^{202} modulo 11.

By Fermat's little theorem, $3^{10} \equiv 1 \pmod{11}$
 $\Rightarrow 3^{202} = 3^{200} \times 3^2 = (3^{10})^{20} \times 3^2 \equiv 1 \times 9 \pmod{11}$
 So $3^{202} \equiv 9 \pmod{11}$

State that you are using Fermat's little theorem.

If you have to solve a congruence equation with a prime modulus, you might be able to use Fermat's little theorem.

If p is prime and $p \nmid a$, then $\gcd(a, p) = 1$, so $ax \equiv b \pmod{p}$ has exactly one solution in the set of least residues modulo p .

$$ax \equiv b \pmod{p}$$

$$a^{p-2} ax \equiv a^{p-2} b \pmod{p} \quad \text{— Multiply both sides by } a^{p-2}.$$

$$x \equiv a^{p-2} b \pmod{p} \quad \text{— } a^{p-2} a = a^{p-1} \equiv 1 \pmod{p}, \text{ by Fermat's little theorem.}$$

■ **If a and b are positive integers and p is a prime number with $p \nmid a$, then**

- a^{p-2} is a multiplicative inverse of a modulo p
- the solution to the equation $ax \equiv b \pmod{p}$ is given by $x \equiv a^{p-2} b \pmod{p}$.

Example 32**A**Find the solution to the linear congruence $7x \equiv 10 \pmod{11}$.

By Fermat's little theorem,

$$7^9 \times 7x \equiv 7^9 \times 10 \pmod{11}$$

$$x \equiv 7^9 \times 10 \pmod{11}$$

$$7^2 = 49 \equiv 5 \pmod{11} \Rightarrow 7^3 \equiv 2 \pmod{11}$$

$$\Rightarrow 7^6 \equiv 4 \pmod{11} \Rightarrow 7^9 \equiv 4 \times 2 \pmod{11}$$

$$\text{So } x \equiv 8 \times 10 \pmod{11}$$

$$x \equiv 3 \pmod{11}$$

7^9 is a multiplicative inverse of 7 modulo 11.

$$x \equiv a^{p-2}b \pmod{p}$$

Use multiplication modulo 11 to find the least residue of 7^9 .

Example 33Find the remainder when 2^{1000} is divided by 13.

$$2^{12} \equiv 1 \pmod{13} \Rightarrow 2^{996} = (2^{12})^{83}$$

$$\equiv 1 \pmod{13} \Rightarrow 2^{1000} = 2^{996} \times 2^4$$

$$\equiv 2^4 \equiv 16 \equiv 3 \pmod{13}$$

So the remainder is 3.

Example 34Find the solution to the congruence equation $x^{103} \equiv 4 \pmod{11}$.

$$x^{11} \equiv x \pmod{11}$$

$$x^{103} = (x^{11})^9 \cdot x^4 \equiv x^9 \cdot x^4 \equiv x^{13} \equiv x^{11} \cdot x^2$$

$$\equiv x \cdot x^2 \equiv x^3 \pmod{11}$$

Now we only need to solve $x^3 \equiv 4 \pmod{11}$

By inspection, the perfect cube that leaves a remainder of 4 when divided by 11 is 5^3 .

Therefore $x = 5$. In general, the solution would be $5 + 11k$ for any integer k .

Use Fermat's little theorem in the form $a^p \equiv a \pmod{p}$.

Exercise 1F

1 Find the least residue of:

a 3^{31} modulo 7

b 5^{33} modulo 17

c 128^{129} modulo 17

d 9^{794} modulo 11

- A** 2 Find the least residue of 8^{50} modulo 13. (3 marks)
- E**
- E/P** 3 Solve the congruence equation $4x^{11} \equiv 3 \pmod{11}$. (5 marks)
- E/P** 4 Show that $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ is divisible by 7. (5 marks)
- E** 5 a State Fermat's little theorem. (2 marks)
 b Hence, or otherwise, show that $2^{2018} \equiv 4 \pmod{5}$. (2 marks)
- P** 6 a Using Fermat's little theorem, show that the congruence equation $x^{103} \equiv 4 \pmod{11}$ can be reduced to $x^3 \equiv 4 \pmod{11}$.
 b Hence, by inspection, find a value of x between 0 and 10 that satisfies this equation.
 c Given that x satisfies $x^3 \equiv 4 \pmod{11}$, explain why $x + 11k$ also satisfies the equation for any $k \in \mathbb{Z}$.
- E/P** 7 Prove that $5^{22} + 17^{22} \equiv 6 \pmod{11}$. (4 marks)
- E/P** 8 By means of a counterexample, disprove the following statement.

For any integers a and p , $a^{p-1} \equiv 1 \pmod{p}$

(2 marks)

1.7 Combinatorics

Combinatorics is the branch of mathematics that deals with counting. In GCSE you used the **product rule of counting** to work out numbers of possible combinations. For example, if you have 7 different t-shirts and 3 different pairs of jeans, then there are $7 \times 3 = 21$ different ways of choosing a t-shirt and a pair of jeans.



- If you can choose one item in m different ways, and a second item in n different ways, then the total number of ways of choosing both items is $m \times n$.

You can extend this rule to situations when you have to choose more than two items.

- If you need to choose k items, and the k th item can be chosen in n_k different ways, then the total number of ways of choosing all k items is $n_1 \times n_2 \times \dots \times n_k$.

Notation You could also say that $n_1 \times n_2 \times \dots \times n_k$ is the total number of possible **combinations** of these k items.

Example 35**A**

A number plate consists of two letters, followed by two digits, followed by three more letters. The letters can be chosen from the entire alphabet except the letters I, O, Q or Z, and the digits can be chosen from 0 up to 9.



a Find the total number of different number plates that can be generated in this way.

All number plates registered in one particular region must start with the letter combinations CW or CX.

b Find the total number of different number plates that can be generated in this way.

$$\begin{aligned} \text{a } & 22 \times 22 \times 10 \times 10 \times 22 \times 22 \times 22 \\ & = 515\,363\,200 \end{aligned}$$

$$\text{b } 2 \times 10 \times 10 \times 22 \times 22 \times 22 = 2\,129\,600$$

You could not list all the possible number plates systematically. Use the product rule of counting.

The first two letters can be chosen in one of two ways.

Example 36

Find the total number of 3-digit even numbers.

The first digit can be chosen in 9 different ways.

The second digit can be chosen in 10 different ways.

The third digit can be chosen in 5 different ways.

$$\begin{aligned} \text{Total number of possibilities} &= 9 \times 10 \times 5 \\ &= 450 \end{aligned}$$

The first digit cannot be 0, but the second digit can.

The number is even so the third digit must be 0, 2, 4, 6 or 8.

You can find the number of combinations in more complicated situations by adding or subtracting possibilities.

Example 37

A Find the total number of positive integers less than 1000 that contain the digit 5

a exactly once

b at least once

- a** 1-digit numbers: 1 possibility
 2-digit numbers: $1 \times 9 + 8 \times 1 = 9 + 8$
 $= 17$ possibilities
 3-digit numbers: $1 \times 9 \times 9 + 8 \times 1$
 $\times 9 + 8 \times 9 \times 1 = 81 + 72 + 72$
 $= 225$ possibilities
 In total, there are $1 + 17 + 225 = 243$ possibilities

- b** Number of positive integers less than 1000 that do not contain the digit 5:
 1-digit numbers: 8 possibilities
 2-digit numbers: $8 \times 9 = 72$ possibilities
 3-digit numbers: $8 \times 9 \times 9 = 648$ possibilities
 In total, there are $8 + 72 + 648 = 728$
 So there are $999 - 728 = 271$ positive integers less than 1000 that contain the digit 5 at least once.

Consider each possible position for the 5 separately. If the 3-digit number is $5\square\square$, then the second two digits can each be chosen in 9 ways (any digit except 5).

If the number is $\square 5\square$, then the first digit cannot be 0 so there are $8 \times 1 \times 9$ possibilities.

Problem-solving

You could consider 1-, 2- and 3-digit numbers simultaneously by allowing 0 in the first or second digit: $1 \times 9 \times 9 + 9 \times 1 \times 9 + 1 \times 9 \times 9 = 243$

Problem-solving

There are 999 positive integers less than 1000. Work out the number that do not contain the digit 5, then subtract this from 999.

You could also work this out by allowing 0 in the first or second digit as $9 \times 9 \times 9 - 1$. The -1 is needed because you have counted 000 which is not a positive integer.

Example 38

A set $S = \{1, 2, 3, 4, 5, 6\}$. Find the total number of possible subsets of S .

S contains 6 elements.
 Each element can be either selected for the subset or not selected.
 So the total number of possible subsets is given by:
 $2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6 = 64$

Notation

A subset of S is a set whose elements are all contained in S . Example of subsets of S are $\{2, 4, 6\}$ and $\{3\}$. S is a subset of itself, and the **empty set**, $\{\}$, is also a subset of S .

■ If a set S contains n elements, then the total number of possible subsets of S is 2^n .

Example 39**A**

A group of 10 students are being selected to clean up a local park. Given that at least one student must be selected, how many different groups of students could be selected to clean up the park?

There are 10 students.

So there are $2^{10} = 1024$ possible subsets of the group of students.

At least one student must be selected, so the total number of possible groups is $2^{10} - 1 = 1021$

Each subset represents a different possible group of students.

Watch out Subtract 1 as you can't have the empty set (no students) in this case.

You can use the product rule of counting to determine the number of ways n items can be **arranged**.

Notation This is called the number of **permutations** of n items.

Suppose you have 5 different textbooks that you want to arrange on a shelf:

Maths (M), Physics (P), English (E), Biology (B), and History (H).

Each book can be placed in one of five positions:

$\underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad}$
1 2 3 4 5

You can put any book in position 1, so you have five choices. Once you have placed the first book (your maths book, for example), you have four different choices for the book you can place in position 2:

$\underline{M} \underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{P} \underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{E} \underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{B} \underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{H} \underline{\quad} \underline{\quad} \underline{\quad} \underline{\quad}$
1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5

Once you have placed books in positions 1 and 2, you have three different choices for the book you can place in position 3:

$\underline{M} \underline{P} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{M} \underline{E} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{M} \underline{B} \underline{\quad} \underline{\quad} \underline{\quad}$ $\underline{M} \underline{H} \underline{\quad} \underline{\quad} \underline{\quad}$
1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5

Once you have placed the first three books, there are two books available position 4, and only one book available for position 5. So, the number of ways of arranging all 4 books is

$$5 \times 4 \times 3 \times 2 \times 1 = 120 = 5!$$

■ **There are $n!$ different ways of placing n items in order.**

Notation This is also called the number of **permutations** of n items.

Example 40

- A** Consider the letters $ABCDEF$.
- Find the number of different strings of length 6 that can be written using these letters exactly once each.
 - Find the number of these strings that contain:
 - the substring DEF
 - the letters DEF together in any order.

a $6! = 720$

This is the number of permutations of 6 distinct items.

- b i** Consider 4 items: A , B , C , and DEF

The number of possible permutations of these four items is $4! = 24$.

There are 24 strings containing the substring DEF .

DEF must appear in this order. Consider them as a single block. The remaining letters, A , B , and C can be placed arbitrarily.

- ii** There are $4! = 24$ permutations containing the string DEF in order. The string DEF can be arranged in $3! = 6$ different ways.

So there will be $4! \times 3! = 144$ ways of arranging them.

There are 144 strings containing DEF together in any order.

Use the multiplication principle. If there are m ways an event can occur followed by n ways a second event can occur, then there are a total of $m \times n$ ways that the two events can occur.

In the above example you were arranging **all 6** of the items you were given. In many cases, you may want to arrange a **subset** of the whole collection rather than the entire collection. For example, suppose you want to shelve 3 of 5 books rather than all 5.

You now only have three positions. In the first position you can select any of the 5 books (your maths book, say). In the second position you can choose from the four remaining books, as shown here:

$$\begin{array}{cccc} \underline{M} & \underline{P} & \underline{} & \underline{} \\ 1 & 2 & 3 & \end{array} \quad \begin{array}{cccc} \underline{M} & \underline{E} & \underline{} & \underline{} \\ 1 & 2 & 3 & \end{array} \quad \begin{array}{cccc} \underline{M} & \underline{B} & \underline{} & \underline{} \\ 1 & 2 & 3 & \end{array} \quad \begin{array}{cccc} \underline{M} & \underline{H} & \underline{} & \underline{} \\ 1 & 2 & 3 & \end{array}$$

In the third and final position, you only have three books remaining to choose from:

$$\begin{array}{cccc} \underline{M} & \underline{P} & \underline{E} & \underline{} \\ 1 & 2 & 3 & \end{array} \quad \begin{array}{cccc} \underline{M} & \underline{P} & \underline{B} & \underline{} \\ 1 & 2 & 3 & \end{array} \quad \begin{array}{cccc} \underline{M} & \underline{P} & \underline{H} & \underline{} \\ 1 & 2 & 3 & \end{array}$$

In total, there are $5 \times 4 \times 3 = 60$ ways of shelving the books.

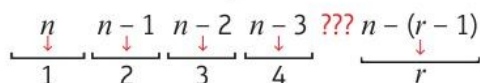
You can write $5 \times 4 \times 3$ in factorial notation as $\frac{5 \times 4 \times 3 \times \cancel{2} \times \cancel{1}}{\cancel{2} \times \cancel{1}} = \frac{5!}{2!}$

- The number of possible permutations of r items taken from a set of n items, where $n \geq r$, is given by

$${}^n P_r = \frac{n!}{(n-r)!}$$

Notation ${}^n P_r$, or ' n permute r ' is sometimes written as ${}_n P_r$, P_r^n or $P(n, r)$. Your calculator might have a key marked $[nPr]$.

- A** You can see why this result is true by imagining that you are arranging r books on a shelf, chosen from a collection of n books. The book in the first position can be chosen in n ways. The book in the second position can be chosen in $(n - 1)$ ways, and so on up to the book in the r th position, which can be chosen in $n - (r - 1)$ ways.



NOTE: Do not know what goes in where ??? is shown (x2) – Tech-Set.

The total number of arrangements is

$${}^n P_r = n \times (n - 1) \times (n - 2) \times ??? \times (n - r + 1) = \frac{n!}{(n - r)!}$$

Example 41

15 runners compete in a cross-country race.

Find the number of different ways the top 6 positions can be filled.

$${}^{15} P_6 = \frac{15!}{(15 - 6)!} = 3\,603\,600$$

Since the runners are all different, this is a permutation of 6 items taken from a set of 15 items.

If some of the objects are **identical**, this reduces the total number of possible unique permutations. Suppose you wanted to permute the letters in the word CARRIER. This word contains the letter R three times. If you counted the number of possible permutations using the rule above you would count $7! = 5040$ arrangements. But you would have counted some identical arrangements twice. For example, if Rs are denoted as R_1 , R_2 and R_3 then you have counted $R_1 C E R_2 A R_3 I$ and $R_3 C E R_1 A R_2 I$ separately, even though they represent identical strings of letters.

In any string, the three Rs can be arranged in $3! = 6$ different ways, so you have counted incorrectly by a multiple of 6. The correct number of permutations is $\frac{7!}{3!} = 840$.

- The number of permutations of n items, of which r are identical is given by $\frac{n!}{r!}$
- The number of permutations of n items, of which r_1 are identical, r_2 are identical, and so on, is given by $\frac{n!}{r_1! \times r_2! \times \dots}$

Example 42

Find the number of possible different permutations of the letters in the word WINNINGS.

This is a set of 8 items in which:

2 are identical (I)

3 are identical (N)

So the total number of permutations is

$$\frac{8!}{3! \times 2!} = 3360$$

$n = 8$, $r_1 = 2$, $r_2 = 3$. There are no other repeated letters.

- A** When you were calculating permutations of objects, the **order** of the objects was important. For example, when you were shelving 3 books from a set of 5 different books you wanted to count *MPE* separately from *EPM*.

Suppose now that you are interested in the number of ways of **choosing** 3 books from a set of 5 books if **order is not important**.

You already know that there are $\frac{5!}{2!} = 60$ ways of choosing the books in order. This includes, for example, all possible permutations of the set $\{M, P, E\}$:

MPE, MEP, PME, PEM, EPM, EMP

In this instance, you only want to count 1 for all of these possible options, so you need to divide the total number of permutations by the number of ways of permuting 3 items, or 3!

The number of ways of choosing 3 items (in any order) from a set of 5 items is $\frac{5!}{3!2!} = 10$.

- **The number of possible combinations of r items (in any order) taken from a set of n items, where $n \geq r$, is given by**

$${}^nC_r = \frac{n!}{r!(n-r)!}$$

Notation nC_r or “ n choose r ” is sometimes written as ${}_nC_r$, C_r^n or $C(n, r)$. Your calculator might have a key marked $\left[\frac{nCr}{} \right]$. You have encountered it before in your work on the binomial theorem. ← Pure Year 1, Chapter 8

This is the number of ways of choosing r items in order divided by the number of possible orderings of those r items:

$${}^nC_r \frac{{}^nP_r}{r!} = \frac{n!}{r!(n-r)!} = \frac{n!}{r!(n-r)!}$$

Example 43

In a lottery game you choose 6 numbers from a choice of 45 by shading in a grid.

6 numbers are selected at random and if you match all six you win a jackpot prize.

Find the probability of winning a jackpot prize.



$$\binom{45}{6} = 8\,145\,060$$

$$P(\text{Jackpot}) = \frac{1}{8\,145\,060}$$

Order is not important, and you need to have the exact combination to win.

Example 44**A**

In poker, a deck of 52 different cards is used. There are 13 cards in each of four suits.

A hand is made up of five cards, arranged in any order.

a Work out the total number of different hands that are possible.

A **flush** is a hand containing five cards of the same suit.

b Work out the number of hands containing five cards of the same suit.

Four-of-a-kind is a hand containing four cards of the same value, such as four 7s, or four queens.

c Work out the number of four-of-a-kind hands.

$$\text{a } \binom{52}{5} = 2\,598\,960$$

The player can arrange their cards in any order, so work out ${}^{52}C_5$.

$$\text{b } \binom{13}{5} \times 4 = 5148$$

There are $\binom{13}{5}$ ways to get a flush in each suit, and four suits.

$$\text{c } 13 \times 48 = 624$$

The four-of-a-kind can be one of 13 values, and the remaining card can be chosen in $52 - 4 = 48$ different ways. Use the product rule of counting.

Example 45

The set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Find:

a the number of subsets of S containing exactly 4 elements

b the number of different 4-digit numbers that can be made using the elements of S . (Each element can be used only once.)

$$\text{a } \binom{8}{4} = 70$$

Order is not important in a subset, so use 8C_4 .

$$\text{b } {}^8P_4 = 1680$$

Each element in S is distinct and you need to choose 4 of them **in order**.

Exercise 1G

1 Evaluate:

a 5P_5

b 5C_2

c ${}^{20}P_1$

d 8P_3

e ${}^{20}C_7$

f ${}^{100}C_3$

2 You are buying a computer and have the following choices:

- three types of hard drive
- two memory capacities
- four types of graphics cards.

Find the total number of possible configurations for this computer.

- A** 3 A set menu in a restaurant has a choice of 3 starters, 4 main courses, and 3 desserts. Find the total number of possible combinations of courses.
- 4 A multiple choice test consists of 12 questions, each with four possible options. Find the total number of possible ways of answering these 12 questions.
- E/P** 5 The lock on a briefcase has three dials. The first dial can be any letter and the last two dials can be any digit from 0 to 9. Here is one possible combination:
- Z03
- a** How many different ways are there of setting the code? **(2 marks)**
- A different suitcase has four dials. The first two dials can be any letter from A to E, and the last two dials can be any **even** digit greater than 0. Here is one possible combination.
- CC24
- b** How many different ways are there of setting this code? **(2 marks)**
- E/P** 6 A password uses the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. The password must consist of 3 distinct odd digits followed by any other three distinct digits. No digits are repeated. Find the total number of passwords that can be generated in this way. **(2 marks)**
- E/P** 7 Find the total number of 5-digit odd numbers that do not contain the digit 0. **(3 marks)**
- E/P** 8 Find the number of three-digit numbers that contain the digit 7
- a** exactly once **(2 marks)**
- b** at least once **(3 marks)**
- 9 Alison has 7 different textbooks. Find the number of different ways of shelving:
- a** all 7 textbooks **b** 2 textbooks **c** 5 textbooks
- E** 10 The 11 members of a football team are each assigned a number from 1 to 11. Work out the total number of possible assignments of numbers to players. **(2 marks)**
- E/P** 11 Jonjo has the number cards 73156
- a** Find the number of different:
- i** 5-digit numbers **ii** 3-digit numbers
- he can make with these number cards. **(4 marks)**
- Jonjo adds an extra number card showing 7.
- b** Find the number of different 6-digit numbers Jonjo can now make. **(2 marks)**
- E/P** 12 Find the number of possible different arrangements of the letters in the word REDEEMED. **(3 marks)**

- A** 13 Four couples are sitting in a row of eight seats at a cinema.
Find the number of possible seating arrangements if:
- a** there are no restrictions on who sits where (2 marks)
 - b** the two members of each couple must sit next to each other. (4 marks)
- E** 14 A lottery game at a fete requires players to choose four different numbers from 1 to 10.
At the end of the day, four balls are chosen at random from 10 balls numbered from 1 to 10.
A player who matches all four numbers wins a star prize.
Find the probability of winning a star prize. (2 marks)
- E/P** 15 A photography club has 17 members. The club has to elect three officers: president, deputy, and treasurer.
- a** Find the total number of ways that the three officers can be elected from the members. (1 mark)
- The 17 members of the club consist of 10 females and 7 males.
- b** Find the total number of ways that the three officers can be elected such that:
 - i** the president is female
 - ii** the president and deputy are of the same gender
 - iii** the three officers are not all of the same gender. (4 marks)
- The club decides to elect three officers of any gender, and not to assign specific roles to each of them.
- c** Find the number of ways in which this could be done. (2 marks)
- E/P** 16 The digits 1, 2, 3, 4, 5, 6, 7, 8, 9 are to be used to generate a four-digit number. Each digit can be used more than once.
Find the total number of possible numbers with:
- a** no repeated digits, such as 6519 (2 marks)
 - b** one repeated digit, and two distinct digits, such as 2717 (2 marks)
 - c** two repeated distinct digits, such as 3993. (2 marks)
- E** 17 The set $S = \{1, 2, 3, 4, 5\}$.
- a** Find the total number of possible subsets of S . (2 marks)
 - b** Find the number of subsets of S which contain 3 elements. (2 marks)
- E/P** 18 The set $S = \{n \in \mathbb{Z}^+ : n < 1000 \text{ and } n \text{ is divisible by } 9\}$
- a** Find the number of elements in S . (2 marks)
 - b** Find the number of subsets of S which contain 3 elements or fewer. (3 marks)
- E/P** 19 A school chess club consists of 9 boys and 12 girls. A team of four members is needed for an upcoming competition.
- a** Find the total number of teams that can be formed. (2 marks)
 - b** How many of these teams have the same number of boys and girls? (2 marks)
 - c** How many of these teams have more boys than girls? (3 marks)

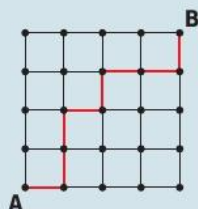
- A** 20 A shipment of 100 hard disks contains 4 defective disks. A sample of 6 disks is chosen for inspection.
- E/P**
- Find the total number of possible samples. (2 marks)
 - Find the probability that this sample contains at least 1 defective disk. (3 marks)
- E/P** 21 The England football world cup squad consists of 23 players. A starting team of 11 players is to be chosen for the first match in the group stage. Calculate the total number of different possible teams in each of the following circumstances.
- Any player can play in any position, and positions are not assigned. (2 marks)
 - Any player can play in any position, and each player is assigned to a unique position. (2 marks)
 - Players must be chosen from the following specialisms, but positions are not assigned within each specialism.

Specialism	Goalkeeper	Defender	Midfielder	Forward
Number of players available	3	10	5	5
Number of players to be chosen	1	5	3	2

(3 marks)

Challenge

The diagram shows a 4×4 grid with a route from the bottom left (**A**) to the top right (**B**) shown.



- Given that routes may only travel along grid lines to the right, or up, find the number of different possible routes from **A** to **B** on this grid.
- Find an expression for the number of such routes on an $n \times n$ grid.

Mixed exercise 1

- E** 1 Use the Euclidean algorithm to find the greatest common divisor of 60 and 444. (2 marks)
- 2 **a** Use the Euclidean algorithm to show that 150 and 721 are relatively prime. (3 marks)
- b** Hence find integers a and b such that $150a + 721b = 1$. (4 marks)
- c** Use your answer to part **b** to find integers p and q such that $150a + 721b = 5$. (1 mark)
- E/P** 3 **a** Use the Euclidean algorithm to show that 21 and 362 are relatively prime. (3 marks)
- b** Hence find a solution to the equation $21x + 362y = 10$, $x, y \in \mathbb{Z}$. (5 marks)

- (E/P)** 4 a Use the Euclidean algorithm to find the highest common factor of 99 and 507. **(3 marks)**
 b Find integers a and b such that $99a + 507b = 24$. **(5 marks)**

- (P)** 5 International Standard Book Numbers (ISBNs) are used to identify books. 10-digit ISBNs contain a final ‘check’ digit, which is chosen so that the sum of each digit multiplied by its position (starting from the right) is equal to 0 (mod 11). If a final digit of 10 is needed then the character X is used.

For example, this book has 10-digit ISBN 1292183365.

ISBN digit	1	2	9	2	1	8	3	3	6	5
Position multiplier	10	9	8	7	6	5	4	3	2	1
Product	10	18	72	14	6	40	12	9	12	5

The sum of the products is $198 \equiv 0 \pmod{11}$, so this is a valid ISBN.

- a Show that 0521735254 is a valid ISBN.
 b The first 9 digits of some ISBNs are given below. In each case determine the final ‘check’ digit:
 i 014143976 ii 046502656

- 6 Find the remainder when 23^{999} is divided by 7. **(4 marks)**

- (E/P)** 7 Show that $99^{51} + 51^{99} \equiv 50 \pmod{100}$. **(3 marks)**

- (E)** 8 Show that $50^{50} \equiv 1 \pmod{7}$. **(2 marks)**

- (E)** 9 Find the units digit in 3^{100} . **(3 marks)**

- (E)** 10 Find the remainder when 13^{99} is divided by 170. **(3 marks)**

- (E)** 11 Use divisibility tests to show that the number 335049 is divisible by both 3 and 11. Show your working clearly. **(2 marks)**

- (E/P)** 12 N is a 3-digit number abc , so that $N = 100a + 10b + c$, where $a, b, c \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $a \neq 0$.
 Prove that $3 \mid N$ if and only if $3 \mid (a + b + c)$. **(4 marks)**

- (E/P)** 13 The following 7-digit number has two missing digits.

$$61 \boxed{a} 116 \boxed{b}$$

Given that the number is divisible by both 9 and 11, find the value of the sum of the missing digits. **(3 marks)**

- (E/P)** 14 A 5-digit number N has two missing digits.

$$N = 7 \boxed{a} 28 \boxed{b}$$

Given that N is divisible by both 4 and 11, find all the possible values of N . **(4 marks)**

- E/P** 15 N is a 3-digit number satisfying $100 \leq N \leq 999$.
 N can be written abc , so that $N = 100a + 10b + c$, where a, b and c are integers between 0 and 9, with $a \neq 0$. N has the following properties:
- N is divisible by 9
 - $N \equiv 10 \pmod{11}$
 - The sum of the digits of N is odd.
- Find all possible values of N , showing your working clearly. **(6 marks)**
- A** 16 **a** Use the Euclidean algorithm to find integers a and b such that $75a + 299b = 1$. **(4 marks)**
- E** **b** Hence solve the equation $75x \equiv 5 \pmod{299}$ **(2 marks)**
- E/P** 17 **a** Use the Euclidean algorithm to find the highest common factor of 60 and 741. **(3 marks)**
- b** Hence state the number of distinct solutions to the equation $60x \equiv 30 \pmod{741}$ in the set of least residues modulo 741. **(1 mark)**
- c** Find all of these possible solutions. **(4 marks)**
- E/P** 18 Find all possible integers in the range $0 \leq n < 19$ that satisfy $14n \equiv 6 \pmod{20}$. **(5 marks)**
- E/P** 19 Solve the congruence equation $31x \equiv 2 \pmod{500}$. **(5 marks)**
- E/P** 20 **a** Explain why the congruence equation $39x \equiv 5 \pmod{600}$ has no solutions. **(4 marks)**
- b** Solve the congruence equation $39x \equiv 6 \pmod{600}$. **(3 marks)**
- E** 21 **a** State Fermat's little theorem. **(2 marks)**
- b** Hence, or otherwise, find the least residue of 7^{25} modulo 13. **(2 marks)**
- E/P** 22 Solve the congruence equation $10x^{11} \equiv 3 \pmod{11}$. **(3 marks)**
- E/P** 23 Find the total number of positive integers less than 5000 that contain the digit 9
- a** at least once **(4 marks)**
- b** at least twice **(2 marks)**
- E/P** 24 Paulo has the five letter cards $\boxed{M} \boxed{A} \boxed{T} \boxed{H} \boxed{S}$
- a** Find the number of ways these letters can be arranged. **(2 marks)**
- b** Find the number of these arrangements that contain
- i** the word $\boxed{H} \boxed{A} \boxed{T}$
- ii** the letters in the word $\boxed{H} \boxed{A} \boxed{T}$ arranged in any order. **(4 marks)**
- E/P** 25 Find the number of possible different arrangements of the letters in the word MUSKETEER. **(3 marks)**

- A** 26 Five adults and five children take it in turns to serve themselves from a buffet. Find the number of possible orders of people if:
- E/P**
- a** there are no restrictions on order (2 marks)
 - b** all the adults must serve themselves first. (3 marks)
- E** 27 To play the EuroMillions lottery, you must select 5 different numbers from 1 to 50, and 2 different Lucky Stars from 1 to 12. Find the total number of different ways of selecting these 7 numbers. (4 marks)
- E/P** 28 An artist has n different colours available. She can mix colours in any combination to create new colours. Assume that any unique combination of colours produces a unique colour. Given that the artist can create more than 500 different colours, find the least possible number of different colours she has available. (3 marks)
- E/P** 29 A set S contains n distinct elements.
- a** Write an expression for the number of different subsets of S containing 3 elements. (1 mark)
 - b** Write an expression for the total number of different subsets of S . (1 mark)
 - c** By considering subsets, or otherwise, show that $\sum_{r=0}^n \binom{n}{r} = 2^n$. (3 marks)

Challenge

In this question you may assume Bezout's identity and the division (cancellation) laws for modular congruences.

Euclid's lemma states that if p is a prime number and $p \mid ab$, where $a, b \in \mathbb{Z}$, then either $p \mid a$ or $p \mid b$ (or both).

a Using Bezout's identity, prove Euclid's lemma.

Fermat's little theorem states that if p is a prime number and a is an integer not divisible by p , then $a^p \equiv a \pmod{p}$.

Let a be a positive integer not divisible by p .

- b** Prove that when the numbers $\{a, 2a, 3a, 4a, \dots, (p-1)a\}$ are reduced to least residues modulo p , that they are exactly the members of the set $\{1, 2, 3, 4, \dots, p-1\}$, in some order.
- c** By considering the product of all the numbers in each set, prove that $a^p \equiv a \pmod{p}$

Summary of key points

- 1 If a and b are integers with $a \neq 0$, then b is divisible by a if there exists an integer k such that $b = ka$. In this case, we say that a divides b and denote this by $a \mid b$. If a does not divide b then we write $a \nmid b$.
- 2 For any $a, b, c \in \mathbb{Z}$, with $a \neq 0$:
 - $a \mid a$ (every integer divides itself)
 - $a \mid 0$ (0 is divisible by any integer)
 - $a \mid b$ and $b \mid c \Rightarrow a \mid c$
 - $a \mid b$ and $a \mid c \Rightarrow a \mid bn + cm$ for all $m, n \in \mathbb{Z}$
 - $a \mid b \Leftrightarrow an \mid bn$ for all $n \in \mathbb{Z}, n \neq 0$
 - If a and b are positive integers and $a \mid b$ then $a \leq b$
- 3 The **division algorithm**: If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.
 - 1 Begin with values of a and b .
 - 2 Set q equal to the greatest integer that is less than or equal to $\frac{a}{b}$
 - 3 Set $r = a - bq$.
- 4 If a, b , and c are integers and $c \neq 0$, then c is called a common divisor of a and b if $c \mid a$ and $c \mid b$.
- 5 The **greatest common divisor** of two integers a and b is a positive integer d that satisfies the two conditions:
 - $d \mid a$ and $d \mid b$
 - if c is a common divisor of a and b , then $c \leq d$
- 6 The **Euclidean algorithm**: Given positive integers a and b with $a \geq b$:
 - 1 Apply the division algorithm to a and b to find integers q_1 and r_1 such that $a = q_1 b + r_1$, where $0 \leq r_1 < b$. If $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$.
 - 2 If $r_1 \neq 0$, apply the division algorithm to b and r_1 to find integers q_2 and r_2 such that $b = q_2 r_1 + r_2$ where $0 \leq r_2 < r_1$. If $r_2 = 0$, then $\gcd(a, b) = r_1$.
 - 3 If $r_2 \neq 0$, continue the process. This results in the system of equations:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

The last non-zero remainder in this process, r_n , is the greatest common divisor of a and b : $\gcd(a, b) = r_n$.

- 7** Bezout's identity states that if a and b are non-zero integers, then there exist integers x and y such that $\gcd(a, b) = ax + by$.
- 8** • Two integers a and b are relatively prime if $\gcd(a, b) = 1$.
 • The integers a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$.
- 9** Let m be a positive integer. If a and b are integers, then a is congruent to b modulo m if $m \mid (a - b)$.
- 10** $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when they are divided by m .
- 11** If $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{m}$ for some positive integer m if and only if there exists an integer k such that $a = b + km$.
- 12** Properties of congruences:
 • $a \equiv 0 \pmod{m}$ if and only if $m \mid a$
 • $a \equiv a \pmod{m}$
 • If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$
 • If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$
- 13** Let $a, b, c, d, m, n \in \mathbb{Z}$ and $m, n > 0$, with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:
 • $a \pm c \equiv b \pm d \pmod{m}$
 • $ac \equiv bd \pmod{m}$
 • $ka \equiv kb \pmod{m}$
 • $a^n \equiv b^n \pmod{m}$
- 14** An integer is divisible by:
 • 2 if and only if its last digit is even
 • 5 if and only if its last digit is 5 or 0
 • 10 if and only if its last digit is 0
- 15** A number N with decimal digits $a_n a_{n-1} a_{n-2} \dots a_1 a_0$ can be written as

$$10^n a_n + 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots + 10 a_1 + a_0$$
- 16** An integer is divisible by:
 • 3 if and only if the sum of its digits is divisible by 3
 • 4 if and only if its last two digits are divisible by 4
 • 6 if and only if it is divisible by both 2 and 3
 • 9 if and only if the sum of its digits is divisible by 9
 • 11 if and only if the difference between the sum of its digits with even position and the sum of its digits with odd position is divisible by 11.

- 17** The set $\{0, 1, 2, 3, \dots, n-1\}$ is called the set of least residues modulo n .
- 18** Let $a, b, m \in \mathbb{Z}$, with $m > 0$ and $\gcd(a, m) = d$
- If $d \nmid b$ then the equation $ax \equiv b \pmod{m}$ has no solutions
 - If $d \mid b$ then the equation $ax \equiv b \pmod{m}$ has d solutions in the set of least residues modulo m
- 19**
- If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod{m}$.
 - If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = d$, then $a \equiv b \pmod{\frac{m}{d}}$.
- 20** A multiplicative inverse of a modulo m is an integer p that satisfies $ap \equiv 1 \pmod{m}$. The multiplicative inverse exists if and only if $\gcd(a, m) = 1$.
- 21** **Fermat's little theorem** states that, if p is a prime number and a is any number not divisible by p , then
- $a^p - 1 \equiv 1 \pmod{p}$
 - $a^p \equiv a \pmod{p}$
- 22** If a and b are positive integers and p is a prime number with $p \nmid a$, then
- a^{p-2} is a multiplicative inverse of a modulo p
 - the solution to the equation $ax \equiv b \pmod{p}$ is given by $x \equiv a^{p-2}b \pmod{p}$
- 23**
- If you can choose one item in m different ways, and a second item in n different ways, then the total number of ways of choosing both items is $m \times n$.
 - If you need to choose k items, and the k th item can be chosen in n_k different ways, then the total number of ways of choosing all k items is $n_1 \times n_2 \times \dots \times n_k$.
- 24** If a set S contains n elements, then the total number of possible subsets of S is 2^n .
- 25** There are $n!$ different ways of placing n items in order.
- 26** The number of possible permutations of r items taken from a set of n items, where $n \geq r$, is given by ${}^nP_r = \frac{n!}{(n-r)!}$
- 27** The number of permutations of n items, of which r are identical is given by $\frac{n!}{r!}$
- 28** The number of permutations of n items, of which r_1 are identical, r_2 are identical, and so on, is given by $\frac{n!}{r_1! \times r_2! \times \dots}$
- 29** The number of possible combinations of r items (in any order) taken from a set of n items, where $n \geq r$, is given by ${}^nC_r = \binom{n}{r} = \frac{n!}{(n-r)!r!}$

Groups

2

Objectives

After completing this chapter you should be able to:

- know and be able to use the axioms for a group → pages 00–00
- be able to use Cayley tables and describe properties of cyclic groups → pages 000–00
- be able to identify the order of an element and that of a group → pages 000–000
- be able to identify subgroups of a group → pages 00–00
- be able to use Lagrange's theorem → pages 00–00
- Be able to recognise and describe isomorphism between two groups → pages 00–00

Analysis of the symmetry groups of molecules has led to the discovery of new molecular structures such as carbon nanotubes, the strongest and stiffest material known to man.

Prior knowledge check

- 1 The functions f and g are defined as

$$f(x) = x^2 + 1, x \in \mathbb{R}$$

$$g(x) = |x - 3|, x \in \mathbb{R}$$

Find: **a** $fg(2)$ **b** $gf(2)$

← Pure Year 2, Chapter 2

- 2 Find $n \in \{0, 1, 2, 3, 4, 5, 6\}$ such that:

a $12 \equiv n \pmod{7}$

b $3^3 \equiv n \pmod{7}$

c $2n \equiv 1 \pmod{7}$

d $6^{99} \equiv n \pmod{7}$

← Section 1.3

- 3 $\mathbf{M} = \begin{pmatrix} 4 & 1 \\ -1 & 3 \end{pmatrix}$ and $\mathbf{N} = \begin{pmatrix} 5 & 0 \\ 2 & 1 \end{pmatrix}$. Find:

a $\mathbf{MN}$

b $\det \mathbf{N}$

c $\mathbf{N}^{-1}$

← Core Pure Book 1, Chapter 6

- 4 Write down the 2×2 matrix corresponding to:

a a reflection in the x -axis

b a rotation through 90° anticlockwise about the origin.

← Core Pure Book 1, Chapter 7

2.1 The axioms for a group

You have encountered sets of numbers previously in your course, but a set can be any collection of distinct objects.

- **A binary operation on a set is a calculation that combines two elements of the set to produce another element of the set.**

Some binary operations occur naturally in mathematics. For example, the operation of addition (+) on the set of integers, $\mathbb{Z}$, is a binary operation, as it combines two integers to produce a third integer.

Similarly, matrix multiplication is a binary operation on the set of 2×2 matrices with real elements.

Notation $S = \{a, b, c, \dots\}$ means that the set S contains the elements, $a, b, c, \dots$. You can write $a \in S$ to show that a , for example, is a member of S .

Watch out The **order** in which the elements of the set are combined in a binary operation is important. For example, subtraction ($-$) forms a binary operation on the set of real numbers, but in general $a - b \neq b - a$.

Example 1

$$S = \{x + y\sqrt{3} : x, y \in \mathbb{Z}\}$$

Show that addition is a binary operation on S .

Let $s_1 = a + b\sqrt{3}$, $s_2 = c + d\sqrt{3}$ where $a, b, c, d \in \mathbb{Z}$.
 $s_1 + s_2 = a + b\sqrt{3} + c + d\sqrt{3} = (a + c) + (b + d)\sqrt{3}$
 As $a, b, c, d \in \mathbb{Z}$, $a + c \in \mathbb{Z}$ and $b + d \in \mathbb{Z}$.
 So $s_1 + s_2 \in S$, and therefore addition is a binary operation on S .

Define two elements of the set.

Add the elements.

Use properties of integers to show that the sum is also a member of S .

Notation You can say that the set S is **closed** under addition.

Example 2

Show that the set of natural numbers, $\mathbb{N} = \{1, 2, 3, 4, \dots\}$, is not closed under subtraction.

For example, $4, 5 \in \mathbb{N}$, but $4 - 5 = -1 \notin \mathbb{N}$.

You only need to find one counter-example to show that $\mathbb{N}$ is **not** closed under subtraction.

For the set of integers, $\mathbb{Z}$, and the binary operation of addition, the number 0 has the property that for any integer $a \in \mathbb{Z}$, $a + 0 = a$. You say that 0 is an **identity element** of $\mathbb{Z}$ under addition.

- **An identity element of a set S under a binary operation $*$ is an element $e \in S$ such that, for any element $a \in S$, $a * e = e * a = a$.**

Notation Binary operations do not always have to correspond to familiar operations such as $+$, $-$, $\times$ or $\div$. You sometimes use the symbols $*$ or $\circ$ to denote an unfamiliar or general binary operation.

An identity element depends on both the set and the binary operation, and does not necessarily exist. For example, the set of natural numbers $\mathbb{N}$ does not contain 0, so does not have an identity element under addition. However, the number $1 \in \mathbb{N}$ satisfies $a \times 1 = 1 \times a = a$, so $\mathbb{N}$ does have an identity element under multiplication.

Example 3

Prove that an identity element of a set S under a binary operation must be unique.

Let $*$ denote the binary operation on S .

Assume that there are two distinct identity elements,

$e, f \in S$

$$e * f = f$$

$$e * f = e$$

So $e = f$, which contradicts the fact that e and f are distinct.

So it is impossible for a set to contain two distinct identity elements, and the identity element is unique.

Use proof by contradiction.

← Pure Year 2, Section 1.1

e is an identity element and $f \in S$ so $e * f = f$.

Similarly, because f is an identity element, $e * f = e$.

The set of integers $\mathbb{Z}$ under the binary operation of addition has identity element 0. The integers 4 and -4 , for example, are such that $-4 + 4 = 4 + (-4) = 0$. You say that 4 and -4 are **inverse** elements of each other.

- Let S be a set and $*$ be a binary operation on S . If an identity element e exists, and there exist elements $a, b \in S$ such that $a * b = b * a = e$, then a is the inverse of b and b is the inverse of a .

Notation

You can write $b = a^{-1}$ and $a = b^{-1}$.

Example 4

The binary operation $*$ on the set of real numbers is defined as $a * b = a + b + ab$.

- a Find a real number e that satisfies the property $a * e = a$.

The real number m has inverse m^{-1} that satisfies the property $m * m^{-1} = e$.

- b Express m^{-1} in terms of m .

a $a * e = a$

$$\Rightarrow a + e + ae = a$$

$$\Rightarrow e + ae = 0$$

$$\Rightarrow e(1 + a) = 0$$

$$\Rightarrow e = 0$$

b $m * m^{-1} = 0$

$$\Rightarrow m + m^{-1} + mm^{-1} = 0$$

$$\Rightarrow m + (1 + m)m^{-1} = 0$$

$$\text{So } m^{-1} = -\frac{m}{m+1}, m \neq -1$$

Set up and solve an equation.

0 is the identity element for this binary operation on $\mathbb{R}$.

The real number -1 has no inverse under this binary operation.

Consider three elements of $\mathbb{Z}$ under the binary operation of addition. For example, $6, 3, 99 \in \mathbb{Z}$:

$$6 + (3 + 99) = 6 + 102 = 108$$

$$(6 + 3) + 99 = 9 + 99 = 108$$

So $6 + (3 + 99) = (6 + 3) + 99$. This is an example of the **associative** property of addition.

■ A binary operation $*$ on a set S is associative if, for any $a, b, c \in S$,

$$a * (b * c) = (a * b) * c$$

Example 5

A binary operation on $\mathbb{R}$ is defined by $a \circ b = ab + 1$.

Show that $\circ$ is not associative.

Consider the elements $2, 3, 4 \in \mathbb{R}$.

$$2 \circ (3 \circ 4) = 2 \circ (3 \times 4 + 1)$$

$$= 2 \circ 13$$

$$= 2 \times 13 + 1 = 27$$

$$(2 \circ 3) \circ 4 = (2 \times 3 + 1) \circ 4$$

$$= 7 \circ 4$$

$$= 7 \times 4 + 1 = 29$$

So $2 \circ (3 \circ 4) \neq (2 \circ 3) \circ 4$, so the operation $\circ$ is not associative.

Problem-solving

In order for the operation $\circ$ to be associative, it must satisfy $a \circ (b \circ c) = (a \circ b) \circ c$ for **any** $a, b, c \in \mathbb{R}$. If you can find three real numbers which do not satisfy this condition, then you have shown that $\circ$ is not associative.

Write a conclusion.

You can use the properties of binary operations to define a **group**.

■ If G is a set and $*$ is a binary operation defined on G , then $(G, *)$ is a group if the following four axioms hold:

- **Closure:** for all $a, b \in G$, $a * b \in G$
- **Identity:** there exists an identity element $e \in G$, such that for all $a \in G$, $a * e = e * a = a$
- **Inverses:** for each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$
- **Associativity:** for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$

Watch out A group is a set **together with** a binary operation that satisfies these four axioms. A set on its own is not a group.

Example 6

Show that:

- the set of integers forms a group under addition
- the set of integers does not form a group under multiplication.

- a Closure:** The sum of two integers is an integer, so the set is closed under addition.
Identity: For all $n \in \mathbb{Z}$, $n + 0 = n = 0 + n$. $0 \in \mathbb{Z}$ so there is an identity element.
Inverses: For all $n \in \mathbb{Z}$, $n + (-n) = (-n) + n = 0$. $-n \in \mathbb{Z}$ so $-n$ is the inverse of n .
Associativity: $a + (b + c) = a + b + c = (a + b) + c$ for all $a, b, c \in \mathbb{Z}$.
 Hence the set of integers forms a group under addition.
- b** For all $n \in \mathbb{Z}$, $n \times 1 = 1 \times n = n$.
 So the identity element is 1.
 0 is an integer, but there is not an integer n such that $0 \times n = 1$.
 The inverse axiom fails, so the set of integers does not form a group under multiplication.

Notation You can write this group as $(\mathbb{Z}, +)$.

List each axiom and explain why it holds for integers under addition.

Watch out Check that inverse elements are members of the set. If the question was about 'positive integers', then the negative of each integer would not be a member of the set.

It is possible to prove associativity more formally. In your exam, you will be told if you can assume that the associativity axiom holds. **→ Exercise 2A, Challenge**

Problem-solving

You only need to show that one of the four axioms fails. For the inverse axiom to hold, **every** element in the set must have an inverse. You could also say that there is no integer n such that $2 \times n = 1$.

Example 7

The operation $*$ is defined by $a * b = a + b - 1$, where a and b are real numbers. Determine whether the set of real numbers under the operation $*$ forms a group.

Closure: The real numbers are closed under addition and subtraction, so $a + b - 1$ is a real number.
Identity: $a * 1 = a + 1 - 1 = a$
 $1 * a = 1 + a - 1 = a$
 1 is a real number.
 So the identity element is 1.
Inverses: $a * (2 - a) = a + (2 - a) - 1 = 1$
 $(2 - a) * a = (2 - a) + a - 1 = 1$
 If a is a real number, then $2 - a$ is a real number.
 The inverse of each element a is $2 - a$.
Associativity:
 $(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1$
 $= a + b + c - 2$
 $a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1$
 $= a + b + c - 2$
 Therefore $*$ is associative.
 Hence the set of real numbers form a group under $*$.

Watch out You must check that the identity works when applied in either direction, so that $a * e = e * a = a$

Remember to show inverses in both directions.

Show that the associativity axiom holds.

All four group axioms hold, so $(\mathbb{R}, *)$ is a group.

Example 8

Prove that, for all elements a, b in a group $(G, *)$, there exists a unique element c such that $a * c = b$.

Existence: Let $c = a^{-1} * b$.
 $a^{-1} \in G$ (by inverse axiom) and $a^{-1} * b \in G$ (by closure axiom)
 Then $a * c = a * (a^{-1} * b) = (a * a^{-1}) * b$ (by associativity axiom)
 $= e * b = b$

Uniqueness: Assume there is a distinct element $d \in G$ which also satisfies $a * d = b$.

Then $d = e * d = (a^{-1} * a) * d = a^{-1} * (a * d)$ (by associativity axiom)
 $= a^{-1} * b$
 $= a^{-1} * (a * c)$
 $= (a^{-1} * a) * c$
 $= e * c = c$

So $d = c$, which is a contradiction, so c must be unique.

Start by proving that such an element exists, and then prove that it must be unique.

$$b = a * c$$

Notation

Similarly, there is a unique element $f \in G$ which satisfies $f * a = b$. These two properties are called the **latin square** property, and are important when constructing Cayley tables. → **Section 2.2**

Exercise 2A

1 $S = \{x + y\sqrt{3} : x, y \in \mathbb{Z}\}$

Determine whether each of the following is a binary operation on S .

- a subtraction b multiplication
 c division

Hint You need to determine whether S is closed under each operation.

2 Determine whether each set is closed under the operation $*$.

- a positive integers, $x * y = \frac{x!y!}{xy}$ b real numbers, $x * y = \sqrt{x + y}$
 c odd numbers, $x * y = x^2y$ d complex numbers, $x * y = |x| + |y|$

3 For the set $\mathbb{C}$ of complex numbers under the binary operation of multiplication,

- a state the identity element
 b find the inverse of $1 + i$, giving your answer in the form $a + ib$.

4 For the set of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $a \in \mathbb{R}$, $a \neq 0$, under matrix multiplication,

- a state the identity element b find the inverse of $\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$

5 Determine whether each of the following operations is associative over the real numbers.

- a $x * y = xy^2$ b $x * y = 3^{xy}$
 c $x * y = |x| + |y|$ d $x * y = xy + x + y$

- 6 Determine whether each of the following pairs of sets and operations form a group. You may assume that the real numbers are associative over addition and multiplication.

- | | |
|-----------------------------------|-------------------------------------|
| a positive real numbers, $\times$ | b integers, $\div$ |
| c odd integers, $+$ | d even integers, $\times$ |
| e real numbers, $-$ | f positive rational numbers, $\div$ |

Hint Positive means that 0 is excluded.

- (P) 7 The operation $*$ on the set of rational numbers, $\mathbb{Q}$, is defined by $a * b = \frac{ab}{a+b}$

- a Prove that $\mathbb{Q}$ is closed under $*$.
b Show that this binary operation does not have an identity element.

- (E/P) 8 The operation $*$ on the set of positive integers $\mathbb{Z}^+$ is defined by $a * b = a + b - 2$.

- a Determine whether or not $*$ is:
i closed ii associative.

(3 marks)

- b i Find the identity element for $*$.
ii Hence show that $\mathbb{Z}^+$ does not form a group under $*$.

(4 marks)

Problem-solving Find an element of $\mathbb{Z}^+$ that does not have an inverse.

- (E/P) 9 The operation $*$ is defined by $a * b = ab + a$, where a and b are real numbers. Show that $\mathbb{R}$ does not form a group under $*$.

(4 marks)

- (E/P) 10 Show that the set of integer-valued 2×2 matrices forms a group under addition. You may assume that addition of integers is associative.

(5 marks)

- (E/P) 11 Show that the set of 2×2 diagonal matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \neq 0$, forms a group under matrix multiplication.

(4 marks)

- (E/P) 12 Let M be the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$, and $a \neq 0$ and $c \neq 0$. Prove that M is a group under matrix multiplication.

(6 marks)

- (E/P) 13 Show that the set of functions of the form $f(x) = ax + b$, where $a, b \in \mathbb{R}$ and $a \neq 0$, forms a group under function composition.

(6 marks)

- (E/P) 14 Prove that for any element a in a group, the inverse of a is unique.

(2 marks)

- (P) 15 Prove that for all elements a, b in a group $(G, *)$,

a $(a^{-1})^{-1} = a$

b $(a * b)^{-1} = b^{-1} * a^{-1}$

- (E/P) 16 A set G forms a group under the operation of multiplication. For $a, b \in G$, prove that

$a^2b^2 = (ab)^2 \Rightarrow ab = ba$

(3 marks)

Problem-solving Multiply by a^{-1} on the left and b^{-1} on the right.

- E/P** 17 A group $(G, \circ)$ contains elements a and b such that a and b are self-inverse. Given that $a \circ b = b \circ a$, prove that $a \circ b$ is also self-inverse. (4 marks)

Problem-solving An element of a group x is **self-inverse** if $x = x^{-1}$.

Challenge

The set $\mathbb{N}^0$ is the natural numbers including 0. The **Peano axioms** for defining this set are:

- 1 $0 \in \mathbb{N}^0$
- 2 For any $a \in \mathbb{N}^0$ there exists a **successor** $S(a) \in \mathbb{N}^0$.
- 3 0 is not the successor of any number.
- 4 For $m, n \in \mathbb{N}^0$, $m = n \Leftrightarrow S(m) = S(n)$
- 5 If a set N contains 0, and $a \in N \Rightarrow S(a) \in N$, then $N = \mathbb{N}^0$.
- a Prove that $\mathbb{N}^0$ must contain an infinite number of elements.

You can define **addition** (+) on the set $\mathbb{N}^0$ as follows.

For any $a, b \in \mathbb{N}^0$,

- 6 $a + 0 = a$
- 7 $a + S(b) = S(a + b)$
- b Using this definition of addition, prove by induction that, for any $a, b, c \in \mathbb{N}^0$, $(a + b) + c = a + (b + c)$

Problem-solving

The Peano axioms are a formal way of defining natural numbers:

$1 = S(0)$
 $2 = S(1) = S(S(0))$
 $3 = S(2) = S(S(S(0)))$
 and so on.

2.2 Cayley tables and finite groups

In the previous section, all the groups you considered contained an infinite number of elements. A **finite group** contains only a finite number of elements in its underlying set.

You can represent a finite group in a **Cayley table**.

- A Cayley table fully describes the structure of a finite group by showing all possible products of elements of the group.

Here is part of a Cayley table for a group with underlying set $\{a, b, c, \dots\}$ and operation $*$.

$*$	a	b	c	$\dots$
a				
b				
c	$\rightarrow$	d		
$\vdots$				

All the elements of the underlying set are written as row and column headings (in the same order).
 The element corresponding to $c * b$ is at the intersection of the row containing c with the column containing b . In this case, $c * b = d$.

Watch out The row heading is always the first element in the operation, and the column heading is the second element in the operation.

Example 9

The set $\{1, -1, i, -i\}$, where $i^2 = -1$, forms a group under multiplication.

a Draw a Cayley table for this group.

b Write down:

- i the identity element ii the inverse of i iii the inverse of -1

a

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- b
- i 1 is the identity
 - ii $-i$
 - iii -1

$-1 \times (-i) = i$, so the entry at this position is i .

Problem-solving

The entries in the Cayley table are all members of the underlying set $\{1, -1, i, -i\}$. This shows that the set is closed under multiplication.

The entries in the row corresponding to 1 are the same as the corresponding column headings, and similarly for the column corresponding to 1. This shows that $1 \times a = a \times 1 = a$ for all elements a , so 1 is the identity.

Look for the identity in the row corresponding to i , then read off the corresponding column heading.

The properties of groups give rise to corresponding properties of Cayley tables:

■ **When a group's elements are displayed in a Cayley table, then:**

- **all entries must be members of the group** This is a consequence of the latin square
- **every entry appears exactly once in every row and every column** property of groups. ← Example 8
- **the identity element must appear in every row and column** Because every element has an inverse.
- **the identity elements are symmetric across the leading diagonal** Because $a^{-1} * a = a * a^{-1}$ for every element in a group.

Modular arithmetic groups

You can use modular arithmetic to define finite groups on sets of integers. You will need to use the operations of **multiplication modulo n** and **addition modulo n** .

- **The operation $\times_n$ of multiplication modulo n is defined on integers a and b as the remainder when ab is divided by n .**
- **The operation $+_n$ of addition modulo n is defined on integers a and b as the remainder when $a + b$ is divided by n .**

Notation

You can use $\equiv_n$ to show multiplication or addition modulo n . For example,
 $4 \times 3 \equiv_{10} 2$, because $4 \times 3 \equiv 2 \pmod{10}$
 $6 + 5 \equiv_7 4$, because $6 + 5 \equiv 4 \pmod{7}$

← Section 1.3

The Cayley tables below show the set $\{0, 1, 2, 3, 4\}$ under the actions of addition and multiplication modulo 5.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$$2 \times 4 = 8 \text{ and } 8 \equiv 3 \pmod{5}$$

Example 10

The set $S = \{0, 1, 2, 3, 4\}$. Use the Cayley tables above to determine whether S forms a group under:

a addition modulo 5

b multiplication modulo 5

a **Closure:** All elements are members of S , so the set is closed under addition modulo 5.

Identity: The identity element is 0.

Inverses: Since 0 appears in every row and every column, then every element has an inverse.

Associativity: Addition on the integers is associative, so addition modulo 5 is associative. Hence $(S, +_5)$ is a group.

b The identity element is 1.

1 does not appear in the 0 row, or the 0 column. $(S, \times_5)$ is not a group since 0 does not have an inverse.

For example, the inverse of 2 is 3.

Problem-solving

You can see from the Cayley table that the set $\{1, 2, 3, 4\}$ **does** form a group under multiplication modulo 5.

Example 11

$S = \{1, 3, 7, 9\}$. Determine whether each of the following are groups. You may assume that the associative law holds in each case.

a $(S, \times_{10})$

b $(S, \times_{12})$

a Construct a Cayley table

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Closure: From the table, the set is closed under multiplication modulo 10.

Identity: The identity element is 1 since $1 \times a = a \times 1 = a$ for all $a \in S$.

Inverses: 1 and 9 are self-inverse, and 7 is the inverse of 3 and vice versa.

Associativity: Assumed

Hence $(S, \times_{10})$ is a group.

b $1 \times 3 \equiv_{12} 3$

$3 \times 3 \equiv_{12} 9$

$7 \times 3 \equiv_{12} 9$

$9 \times 3 \equiv_{12} 3$

So 3 has no inverse, so S is not a group under $\times_{12}$.

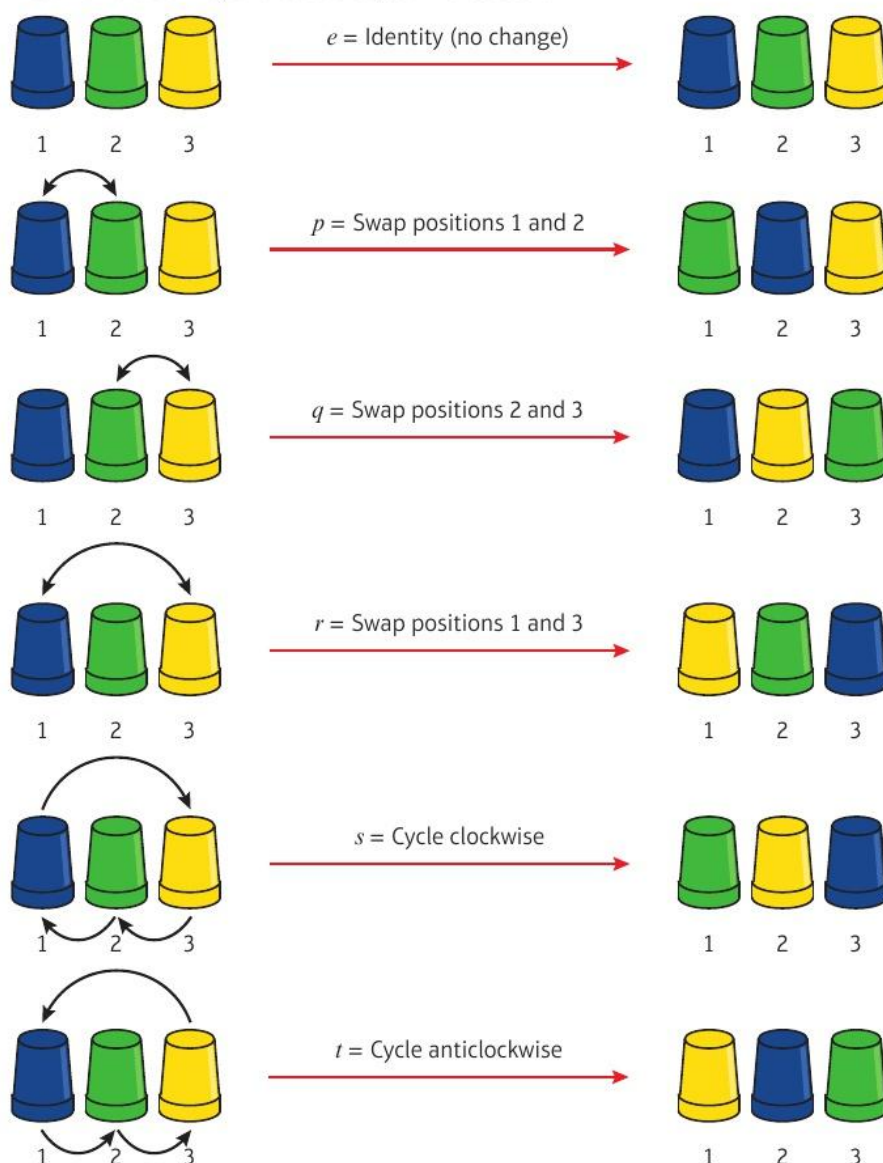
For a small set you can write down all the inverses.

Problem-solving

An element of a set (other than 1) that is a divisor of n cannot have an inverse under multiplication modulo n . Work out $a \times 3 \pmod{12}$ for every element $a \in S$ to show that no inverse exists.

Groups of permutations

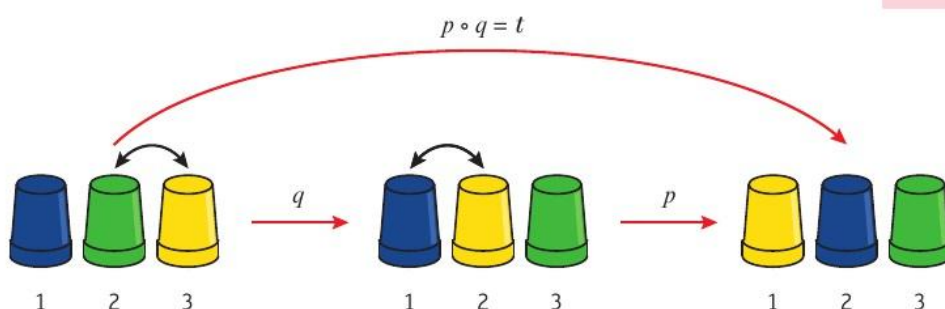
Operations on sets do not need to correspond to familiar arithmetic operations. For example, consider an arrangement of 3 cups. The order in which the cups are arranged can be altered in 6 different ways. Each of these ways is called a **permutation**:



Note The cups move, but the positions (numbered 1, 2 and 3) stay the same. An **identity** permutation (one which does not move any cups) is also included.

You can define a set S of these 6 permutations, and you can define an operation $\circ$ on this set as the **composition** of two permutations. For example, the composition $p \circ q$ would mean 'swap positions 2 and 3 and then swap positions 1 and 2'.

The diagram below shows that this has the same effect as the single permutation t :



Notation Unless you are told otherwise in a question, permutations are composed in the same way as functions, so that $p \circ q$ means do q first and then p .

Example 12

For the set of permutations of 3 cups, $\{e, p, q, r, s, t\}$ as defined above, find:

a $q \circ p$

b $r \circ r$

$$\begin{aligned} \text{a } & BGY \xrightarrow{p} GBY \xrightarrow{q} GYB \\ & \text{So } q \circ p = s \end{aligned}$$

$$\begin{aligned} \text{b } & BGY \xrightarrow{r} YGB \xrightarrow{r} BGY \\ & \text{So } r \circ r = e \end{aligned}$$

Note that $q \circ p \neq p \circ q$

$r \circ r$ is the identity permutation, e , so r is self-inverse.

The construction of the complete Cayley table for this group is left as an exercise. → **Exercise 2B Q12**

This group of all 6 possible permutations of 3 objects, together with the operation of composition, is called the **symmetric group** on 3 elements.

■ **The symmetric group on n elements is defined as the group of all possible permutations that can be performed on n objects, together with the operation of composition.**

Notation This group is often denoted as S_n .

You can use **two-row notation** to write permutations more quickly. Here are the permutations in the example above written using two-row notation.

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & p &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & q &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ r &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & s &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & t &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

The use of two-row notation for permutations makes it easy to find compositions and inverses.

Consider the following two permutations on 5 objects.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

In the **composition** $\alpha \circ \beta$, the element in position 1 moves to position 5 (under β), then to position 3 (under α). So in $\alpha \circ \beta$ the element in position 1 moves to position 3:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

Similarly,

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

The identity permutation on 5 objects is $e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$, so to find the **inverse** of a permutation read from the bottom row to the top row rather than from top to bottom. For example, if 1 appears below 2 in a permutation α then 2 must appear below 1 in α^{-1} .

$$\text{If } \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}, \text{ then } \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$$

Example 13

Show that the permutations

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

form a group under composition. You may assume the associativity axiom is satisfied.

$\times_{10}$	e	p	q	r
e	e	p	q	r
p	p	e	r	q
q	q	r	e	p
r	r	q	p	e

Closure: The elements of the table are all members of the set and hence it is closed.

Identity: e is the identity element.

Inverses: The identity transformation e is included in every row and column, so every element has an inverse.

Associativity: Associativity is assumed in the composition of transformations. Hence the set is a group under composition.

$$\begin{aligned} p \circ q &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = r \end{aligned}$$

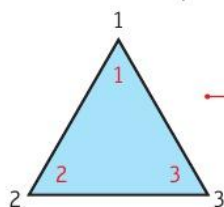
$$e \circ e = e, p \circ p = e, q \circ q = e \text{ and } r \circ r = e.$$

Notation

This group is called the **Klein four-group**, K_4 .

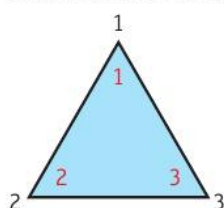
Groups of symmetries

You can construct finite groups by considering the symmetries of shapes. Consider the different ways in which an equilateral triangle can be rigidly transformed onto itself.



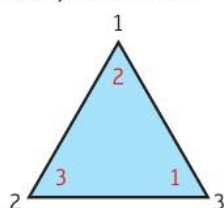
Start by labelling the positions (outside the triangle) and the vertices (inside the triangle). The positions will stay the same, but the vertices will move as the triangle is transformed.

There are three rotational symmetries:



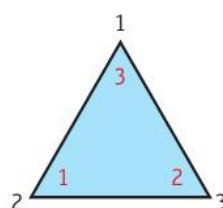
0

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$



Clockwise $\frac{2\pi}{3}$

$$R = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

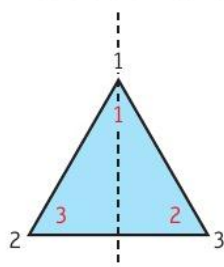


Anticlockwise $\frac{2\pi}{3}$ (or clockwise $\frac{4\pi}{3}$)

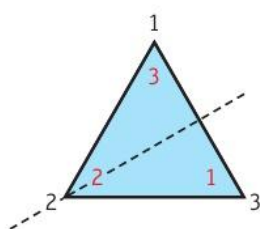
$$S = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Using two-line notation where the second row shows the image of each vertex after the transformation.

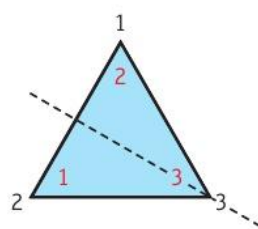
There are three reflections through the three medians:



$$L = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



$$M = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



$$N = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Example 14

Show that $G = \{I, R, S, L, M, N\}$ forms a group under composition of transformations. You may assume that the associative law holds.

$\circ$	I	R	S	L	M	N
I	I	R	S	L	M	N
R	R	S	I	N	L	M
S	S	I	R	M	N	L
L	L	M	N	I	R	S
M	M	N	L	S	I	R
N	N	L	M	R	N	I

Closure: The elements of the table are all members of the set, so the set is closed.

$$\begin{aligned} \text{For example, } R \circ L &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = N \end{aligned}$$

Notation The element S is sometimes called R^2 because $S = R \circ R$

Identity: I is the identity element.

Inverses: The identity transformation I is included in every row and column, so every element has an inverse.

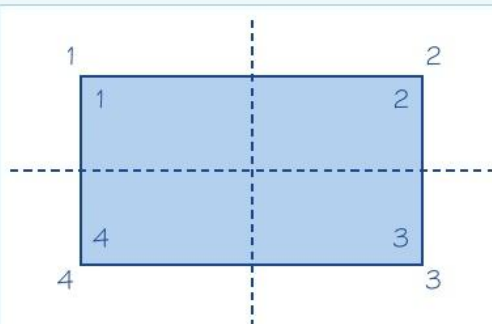
Associativity: Associativity is assumed in the composition of transformations.
So the set of symmetries of the equilateral triangle forms a group under composition.

Use the Cayley table to show that the four group axioms hold.

Notation The group of symmetries of an n -sided regular polyhedron is sometimes called a **dihedral group**, and is denoted as D_{2n} (as it contains $2n$ elements).

Example 15

Show that the symmetries of a rectangle form a group under composition of transformations. You may assume that the associativity axiom holds.



Identity transformation: $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Rotation π about the centre: $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

Reflection about horizontal axis of symmetry:

$q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Reflection about vertical axis of symmetry:

$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

From the working shown in Example 13, these permutations form a group under composition.

Problem-solving

Label the positions of the vertices, and the vertices themselves, with integers. You could use a piece of cardboard to help you visualize the possible transformations. Make sure you label both sides of the cardboard.

Use two-line notation to define the image of each transformation.

These are the same permutations shown in Example 13. This group is also the **Klein four-group**. It is not a dihedral group because the rectangle is not a regular polygon.

→ Section 2.4

Cyclic Groups

Some of the groups you have already considered have the property that all of the elements of the group can be obtained by repeatedly applying the group operation to a particular single group element.

■ **A cyclic group is a group in which every element can be written in the form a^k , where a is the group generator and k is a positive integer.**

- $(\mathbb{Z}, +)$ is cyclic, as applying repeated addition to 1 generates every element of the group.
- $\{0, 1, 2, 3, \dots, n-1\}$ is a cyclic group under addition modulo n .
1 and $n-1$ are both generators of this group.

Notation a^k means applying the group operation k times. For example, $a^3 = a \circ a \circ a$.

Notation This group is sometimes denoted as $\mathbb{Z}_n$.

Example 16

The set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is a group under addition modulo 8. Show that 3 is a generator of this group and write each element in terms of this generator.

$$\begin{aligned} 3 &\equiv_8 3 \\ 3^2 &\equiv_8 6 \\ 3^3 &\equiv_8 1 \\ 3^4 &\equiv_8 4 \\ 3^5 &\equiv_8 7 \\ 3^6 &\equiv_8 2 \\ 3^7 &\equiv_8 5 \\ 3^8 &\equiv_8 0 \end{aligned}$$

All the elements of S can be written in the form 3^k for some positive integer k , so 3 generates the group.

Watch out In this notation, 3^2 means 'apply the group operation twice', so $3^2 = 3 + 3 \equiv_8 6$.

This group also has generators 1, 7 and 5.

Example 17

The set $\{1, 3, 5, 7\}$ forms a group under multiplication modulo 8. Show that this group is not cyclic.

1 can only generate 1.
 $3^2 \equiv_8 1$, $3^3 \equiv_8 3$, ...
 so 3 can only generate 1 and 3.
 $5^2 \equiv_8 1$, $5^3 \equiv_8 5$, ...
 so 5 can only generate 1 and 5.
 $7^2 \equiv_8 1$, $7^3 \equiv_8 7$, ...
 so 7 can only generate 1 and 7.

There is no element that can generate every element of the group, so the group is not cyclic.

Under multiplication, 1 is the identity.

Check each element to see whether it can generate the group. If the pattern repeats without having generated every element then you know that element cannot be a generator.

Links This is another example of the **Klein four-group**. This is the smallest non-cyclic group.
 → Section 2.4

Exercise 2B

- The set $S = \{1, -1\}$ forms a group under multiplication. Construct a Cayley table for $(S, \times)$.
- Construct a Cayley table for each set under the given operation. Determine, with reasons, whether the set and operation form a group.
 - $\{-1, 0, 1\}$ with addition
 - $\{1, 5, 7, 11\}$ with multiplication modulo 12

- (E)** 3 The set $G = \{1, 2, 3, 4, 5, 6\}$ forms a group under multiplication modulo 7. Complete the following Cayley table for this group.

$\times_7$	1	2	3	4	5	6
1				4		
2						
3			2			
4						
5		3				
6						1

(3 marks)

- (E)** 4 The set $S = \{1, 2, 4, 8\}$ is a group under multiplication modulo 15.
- a ii Construct a Cayley table for $(S, \times_{15})$
- ii Show that S forms a group under multiplication modulo 15. You may assume that the associative axiom is satisfied. (6 marks)
- b Show that S does not form a group under multiplication modulo 12. (3 marks)

- (E)** 5 The set $G = \{a, 2, 4, 6\}$ forms a group under the operation of addition modulo 8.
- a Write down the value of a . (1 mark)
- b Complete the following Cayley table for $(G, +_8)$.

$+_8$		2	4	6
2		4		
4				2
6				

(3 marks)

- c Find an element which generates $(G, +_8)$ and write each element in terms of this generator. (2 marks)

- (E/P)** 6 The operation $\circ$ is defined on the set $S = \{0, 1, 2, 3\}$ by $a \circ b = ab + a + b \pmod{5}$
- a Complete the following Cayley table for $(S, \circ)$.

$\circ$	0	1	2	3
0				
1				
2				1
3	3			

(3 marks)

- b Show that S is a group. You may assume that the associative law is satisfied. (3 marks)

Hint $a \circ b$ is equal to the remainder when $ab + a + b$ is divided by 5.

- (P)** 7 Consider a set $A = \{a, b\}$. Let $M = \{q, r, s, t\}$ be the set containing mappings on the elements of A defined by:

$$q(a) = a, q(b) = a; r(a) = a, r(b) = b; s(a) = b, s(b) = a; t(a) = b, t(b) = b$$

- a Construct a Cayley table for composition of mappings, $\circ$, as an operation on M .
- b Write down the identity element for $\circ$.
- c State, with reasons, whether $(M, \circ)$ forms a group.

Hint So the element $q \in M$ maps both a and b onto a .

- P** 8 The operation $*$ is defined on the set $A = \{10, 20, 30, 40, 50\}$ by the Cayley table below.

$*$	10	20	30	40	50
10	10	10	20	30	40
20	10	20	10	20	30
30	20	10	30	10	20
40	30	20	10	40	10
50	40	30	20	10	50

Determine whether each of the following statements is true or false, giving reasons for your answers.

- a A is closed under the operation $*$.
- b There is an identity element.
- c $*$ is associative.
- d $(S, *)$ is a group.

- E/P** 9 The binary operation $*$ is defined on the set $G = \{0, 1, 2, 3\}$ by

$$a * b = a + 2b + ab \pmod{4}$$

- a Construct a Cayley table for $(G, *)$. (3 marks)
- b Determine whether $*$ is associative, justifying your answer. (3 marks)
- c Find all solutions to the equation $x * 1 = 2 * x$, for $x \in G$ (3 marks)

- E/P** 10 A student writes the following:

$S = \{1, 9, 16, 22, 53, 74, 79, 81\}$ forms a group under multiplication modulo 91.

- a Show that the student is not correct. (2 marks)
- b Write down one additional element the student can include in S to make the statement correct. (1 mark)

- E/P** 11 Let S be the set of non-negative integers less than n . Given that S contains an element $a \neq 1$ such that $a \mid n$, prove that S does not form a group under multiplication modulo n . (4 marks)

- P** 12 The group S_3 consists of the set of all possible permutations of 3 objects, together with composition. The underlying set has 6 elements:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad q = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

- a Construct a Cayley table for S_3 .
- b Verify that S_3 satisfies the closure, identity and inverse axioms.

Hint These are the possible permutations of 3 cups given on page 12.

- 13 Consider the permutations $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

Compute each of the following, where $\circ$ is the composition of permutations.

Give your answers in two-row notation.

- | | | | |
|--------------------------------|--------------------------------|-----------------------------|-----------------------------|
| a $b \circ a$ | b $a \circ b$ | c a^{-1} | d b^{-1} |
| e $b^{-1} \circ a^{-1}$ | f $a^{-1} \circ b^{-1}$ | g $(b \circ a)^{-1}$ | h $(a \circ b)^{-1}$ |

- (E/P)** 14 Consider the set $M = \{1, 3, 9, 11\}$ under multiplication modulo 16. For the purposes of this question, denote this multiplication by $\times$.

- a** Show that $3 \times (9 \times 11) = (3 \times 9) \times 11$. **(2 marks)**
b Show that $(M, \times)$ is a group. **(5 marks)**
c Show that this group is cyclic, and write down all possible generators of this group. **(3 marks)**

- 15 Show that the following groups are cyclic and find their generators.

- a** $\{1, 3, 7, 9\}$ under multiplication modulo 10
b $\{4, 8, 12, 16\}$ under multiplication modulo 20
c $\{1, 2, 4, 5, 7, 8\}$ under multiplication modulo 9

- (P)** 16 Explain why 6 cannot generate a group under multiplication modulo 8.

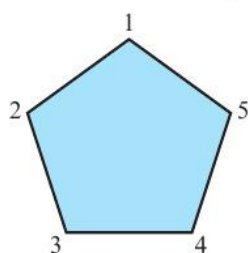
- (E/P)** 17 A group $(G, \times_{21})$ is generated by the number 5.

Find the members of G , and write each one in terms of the generator. **(3 marks)**

- (E/P)** 18 **a** Show that $\omega = \frac{\sqrt{2}}{2}(1 + i)$ generates a group under the operation of complex multiplication. **(5 marks)**

- b** Write down the other generators of this group. **(2 marks)**

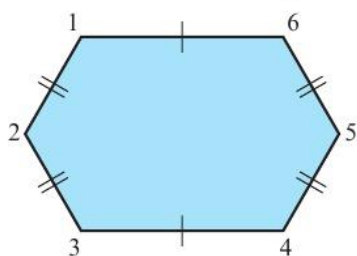
- (E/P)** 19 The vertices of a pentagon are labelled as follows:



The permutations $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$ correspond to clockwise rotations of 0° , 72° and 144° .

- a Write the permutations p_4 and p_5 that correspond to clockwise rotations of 216° and 288° respectively. (2 marks)
- b Complete a Cayley table for $P = \{p_1, p_2, p_3, p_4, p_5\}$ under composition. (4 marks)
- c Prove that the set of rotational symmetries of a pentagon form a group under composition. (5 marks)
- d Show that this group is cyclic, and that it is generated by p_2 . (3 marks)

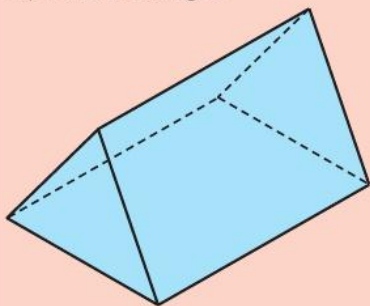
E/P 20 The vertices of a hexagon are labelled as follows:



- a Write down four permutations h_1, h_2, h_3, h_4 that correspond to the four symmetries of the hexagon. (4 marks)
- b Show that the set of symmetries $H = \{h_1, h_2, h_3, h_4\}$ form a group under composition. (6 marks)
- c Explain why H is not a cyclic group. (2 marks)

Challenge

The solid shown is a right triangular prism whose cross-section is an equilateral triangle.



Construct a Cayley table for the group of symmetries of this solid.

Hint Your group should contain 12 elements.

2.3 Order and subgroups

You can use **order** to describe the size of a finite group.

- If a finite group G has n distinct elements, then the order of G is n .

Notation The order of G is written as $|G|$.
Groups with an infinite number of elements, such as $(\mathbb{Z}, +)$ are said to have infinite order.

You can also consider the order of individual elements within a group. In Example 17, you looked at the group $\{1, 3, 5, 7\}$ under multiplication modulo 8. This group has identity 1, and $3^2 = 1$, $5^2 = 1$ and $7^2 = 1$.

You say that the elements 3, 5 and 7 all have **order 2**.

- The order of an element a in a group $(G, *)$ with identity e is the smallest positive integer k such that $a^k = e$.
- If $(G, *)$ is finite with $a \in G$, then $|a|$ divides $|G|$.
- $(G, *)$ is cyclic if and only if there exists an element a such that $|a| = |G|$. This element will be a generator of the group.

Notation The order of the element a is written as $|a|$.
An element has **finite order** if $a^m = e$ for some $m \in \mathbb{Z}^+$.
An element has **infinite order** if $a^m \neq e$ for every $m \in \mathbb{Z}^+$.

Example 18

Let $(G, \circ)$ be a finite group. Prove that every element in G must have finite order.

$|G| = n$
Let a be any element in G , and consider $a, a^2, a^3, \dots, a^{n+1}$
Since G is closed, these values are $n + 1$ elements of a group with n distinct elements.
So at least two of them must be equal, say $a^j = a^k$, with $j > k$
Then $a^j a^{-k} = a^k a^{-k}$
 $\Rightarrow a^{j-k} = e$
So $|a| \leq j - k$, and must be finite, as required.

G is a finite group, so it must have a finite number of elements.

Notation a^{-k} means $\underbrace{a^{-1} \circ a^{-1} \circ \dots \circ a^{-1}}_{k \text{ times}}$

Example 19

For each of the following groups, write down the order of the group, and the order of each element in the group.

- $\{1, -1, i, -i\}$ under complex multiplication
- $\{1, 3, 7, 9\}$ under multiplication modulo 10

a The group contains 4 elements so it has order 4.

$$|1| = 1$$

$$|-1| = 2$$

$$|i| = 4$$

$$|-i| = 4$$

b The group contains 4 elements so it has order 4.

$$|1| = 1, |3| = 4, |7| = 4 \text{ and } |9| = 2$$

The identity element always has order 1.

$$(-1)^2 = 1$$

Any element of a group with order 2 is self-inverse.

$$i^2 = -1, i^3 = -i, i^4 = 1$$

This is a cyclic group with order 4, and both i and $-i$ generate the group, so they both have order 4.

$$3^4 = 81 \equiv_{10} 1, 7^4 = 2401 \equiv_{10} 1 \text{ and } 9^2 = 81 \equiv_{10} 1$$

Example 20

G has elements $\{e, p, p^2, p^3, q, pq, p^2q, p^3q\}$ under multiplication, where e is the identity.

You can assume the associativity axiom is satisfied.

A partially completed Cayley table is shown below.

$\times$	e	p	p^2	p^3	q	pq	p^2q	p^3q
e	e	p	p^2	p^3	q	pq	p^2q	p^3q
p	p	p^2	p^3	e	pq	p^2q	p^3q	q
p^2	p^2	p^3	e	p	p^2q	p^3q	q	pq
p^3	p^3	e	p	p^2	p^3q			
q	q	p^3q	p^2q	pq	e			
pq	pq	q	p^3q	p^2q	p			
p^2q	p^2q	pq	q	p^3q	p^2			
p^3q	p^3q	p^2q	pq	q	p^3			

a State the order of the group.

b State the order of p and q .

c Complete a Cayley table and verify that G forms a group.

d Find the order of pq , p^2q and p^3q .

Watch out You cannot assume that $pq = qp$.

a The group has 8 elements, so $|G| = 8$.

b p has order 4.

q has order 2.

From the table, $p \times p^3 = e$, so $p^4 = e$.

From the table, $q \times q = e$ so $q^2 = e$.

c

$\times$	e	p	p^2	p^3	q	pq	p^2q	p^3q
e	e	p	p^2	p^3	q	pq	p^2q	p^3q
p	p	p^2	p^3	e	pq	p^2q	p^3q	q
p^2	p^2	p^3	e	p	p^2q	p^3q	q	pq
p^3	p^3	e	p	p^2	p^3q	q	pq	p^2q
q	q	p^3q	p^2q	pq	e	p^3	p^2	p
pq	pq	q	p^3q	p^2q	p	e	p^3	p^2
p^2q	p^2q	pq	q	p^3q	p^2	p	e	p^3
p^3q	p^3q	p^2q	pq	q	p^3	p^2	p	e

Closure: Each element that appears in the table is a member of G , so G is closed.

Identity: e is the identity.

Inverses: e appears in every row and column, so every element has an inverse.

Associativity: Associativity is assumed. Hence, G is a group under multiplication.

- d $(pq)^2 = (pq^2)^2 = (pq^3)^2 = e$
So pq , p^2q and p^3q are of order 2.

Problem-solving

Use the associative law, the orders of p and q and the existing entries in the Cayley table to write each product as an element of the set.

For example,

$$p^3 \times pq = p^4q = q$$

$$q \times pq = qp \times q = p^3q \times q = p^3q^2 = p^3$$

$$pq \times p^3q = p(qp^3)q = p(pq)q = p^2$$

$$p^2q \times p^2q = p^2(qp^2)q = p^4q^2 = e$$

$$p^3q \times p^2q = p^3(qp^2)q = p^5q^2 = p$$

Use the Cayley table to show that the four group axioms hold.

Example 21

The set $\{0, 1, 2, 3, 4\}$ forms a group under addition modulo 5.

Explain why no element of this group, other than the identity, can be self-inverse.

The order of the group is 5.

Any self-inverse element, other than the identity, must have order 2.

But the order of an element must divide the order of the group. Since 2 does not divide 5, there can be no such self-inverse element in the group.

0 is the identity element. If the element a was self-inverse you would have $a + a \equiv_5 0$.

Note The identity element of any group is always self-inverse, since $e \circ e = e$.

Any group with odd order cannot contain a self-inverse element, other than the identity.

■ Let a be an element in a group $(G, *)$, then:

- if a has a finite order n , then $a^m = e$ if and only if $n|m$
- if a has infinite order, then $x \neq y \Rightarrow a^x \neq a^y$
- if $a^x = a^y$ with $x \neq y$, then a must have finite order.

Subgroups

If some subset of the underlying set of a group satisfies the group axioms under the **same operation**, then it is called a **subgroup**. For example, consider the set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of non-negative integers less than 8, which forms a group under addition modulo 8.

The **subset** of S given by $T = \{0, 2, 4, 6\}$ also forms a group under addition modulo 8.

Since T is a subset of S , and because each set forms a group **under the same operation**, you say that $(T, +_8)$ is a subgroup of $(S, +_8)$.

- If a non-empty subset H of a group G is itself a group under the binary operation of G , we call H a subgroup of G .
 - If $H \subset G$, then H is a proper subgroup of G .
 - If $H \subseteq G$, then H is a subgroup of G .

Every group has at least two subgroups, $(\{e\}, *)$ and $(G, *)$ itself. $(\{e\}, *)$ is called the **trivial subgroup**, and any other subgroups are called **non-trivial subgroups**.

Notation $B \subseteq A$ means that the set B is contained in the set A . B is a **subset** of A . $B \subset A$ means that B is contained in, **but not equal to**, A . B is a **proper subset** of A . This notation can be applied either to sets or to groups.

Note $H \subset G \Rightarrow |H| < |G|$
 $H \subseteq G \Rightarrow |H| \leq |G|$

Example 22

- a Show that the set $S = \{5^n : n \in \mathbb{Z}\}$ forms a group under multiplication.
- b Determine, with reasons, whether each of the following subsets of S forms a subgroup of $(S, \times)$.
 - i $T = \{5^{2n} : n \in \mathbb{Z}\}$
 - ii $U = \{5^n : n \in \mathbb{Z}^+\}$

a **Closure:** $5^a \times 5^b = 5^{a+b}$.
 For any $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$, so $5^{a+b} \in S$.
Identity: $5^0 \in S$, and $5^0 \times 5^n = 5^n \times 5^0 = 5^n$ for all $n \in \mathbb{Z}$, so 5^0 is the identity element.
Inverses: $5^{-a} \times 5^a = 5^a \times 5^{-a} = 5^0$.
 For any $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$, so $5^{-a} \in S$.
Associativity:
 $5^a \times (5^b \times 5^c) = 5^a \times 5^{b+c} = 5^{a+b+c}$
 $(5^a \times 5^b) \times 5^c = 5^{a+b} \times 5^c = 5^{a+b+c}$
 So $5^a \times (5^b \times 5^c) = (5^a \times 5^b) \times 5^c$ for all $a, b, c \in \mathbb{Z}$, so associativity holds.
 Hence $(S, \times)$ forms a group.

- b i $5^{2a} \times 5^{2b} = 5^{2(a+b)}$ so T is closed.
 $5^0 = 5^{2(0)}$ so identity element exists.
 $5^{-2a} = 5^{2(-a)}$ so inverses exist in T .
 Associativity holds in S so must hold in T .
 So $(T, \times)$ is a subgroup of $(S, \times)$.
- ii The element 5^0 is not a member of U , so U has no identity element.
 U does not form a subgroup of $(S, \times)$.

$$5^0 = 1$$

Problem-solving

Associativity asserts a relationship between 3 fixed elements in a set. If T is a subset of S , then any 3 elements of T must also be elements of S . So if associativity holds in S , then it must also hold in T .

You can use the following rule to find subgroups of **finite groups** quickly.

- Let G be a group and H a finite non-empty subset of G . Then, H is a subgroup of G if H is closed under the operation of G .

Watch out Part **b ii** in Example 22 illustrates that this result does not necessarily hold for infinite subsets.

Example 23

The set $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ forms a group under addition modulo 8.

Find two nontrivial proper subgroups of $(S, +_8)$.

+	0	2	4	6	1	3	5	7
0	0	2	4	6	1	3	5	7
2	2	4	6	0	3	5	7	1
4	4	6	0	2	5	7	1	3
6	6	0	2	4	7	1	3	5
1	1	3	5	7	2	4	6	0
3	3	5	7	1	4	6	0	2
5	5	7	1	3	6	0	2	4
7	7	1	3	5	0	2	4	6

There are two possible subgroups:

$A = \{0, 2, 4, 6\}$ and $B = \{0, 4\}$.

Delete rows and columns from the Cayley table. If you can leave a Cayley table which is **closed** (i.e. the entries in your remaining rows and columns are only those elements in the corresponding row and column headings) then it will represent a subgroup.

Problem-solving

Any subgroup must contain the identity element.

Note B is also a subgroup of A .

In the previous example, you can see that the subgroup $\{0, 2, 4, 6\}$ is generated by the element 2, and the subgroup $\{0, 4\}$ is generated by the element 4. This illustrates one method that can be used to find subgroups.

- If G is a finite group, then any element $a \in G$ generates a subgroup of G , written $\langle a \rangle$.

You can also use **Lagrange's theorem** to make deductions about subgroups.

- **Lagrange's theorem states:**
If H is a subgroup of a finite group G , then $|H|$ divides $|G|$.

Watch out The converse of this result is not true: not every subgroup of G can be generated by an element of G . Only **cyclic** subgroups are generated in this way.

Note You can quote this theorem by name in your examination. You do not need to be able to prove it.

Example 24

The set $G = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ forms a group under multiplication modulo 21.

- Find the elements in the subgroup of $(G, \times_{21})$ generated by the element 5, and state its order.
- Explain why $(G, \times_{21})$ has no subgroup of order 5.

a $5^2 \equiv_{21} 4$

$5^3 \equiv_{21} 20$

$5^4 \equiv_{21} 16$

$5^5 \equiv_{21} 17$

$5^6 \equiv_{21} 1$

So the subgroup $\langle 5 \rangle \subset (G, \times_{21})$ consists of the set $\{1, 4, 5, 16, 17, 20\}$.

The order of $\langle 5 \rangle$ is 6.

- b** The order of the group is 12, and 5 does not divide 12, so by Lagrange's theorem there can be no subgroup of order 5.

$5 \times 5 = 25 \equiv 4 \pmod{21}$

$5^4 = 5^3 \times 5 = 100 \equiv 16 \pmod{21}$

You can write the subgroup as the set of elements $\{1, 4, 5, 16, 17, 20\}$ or in terms of its generator, as $\langle 5 \rangle$.

There are 6 elements in the underlying set.

Exercise 2C

- The set $\{1, 2, 4, 5, 7, 8\}$ forms a group under multiplication modulo 9. Find:

- the order of the group
- the order of each element in the group

- The Cayley table for the Klein four-group is given below

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- Write down the order of each element.
- Hence state, with a reason, whether the group is cyclic.

- (E)** 3 The set $\{0, 1, 2, 3, 4, 5\}$ forms a group under addition modulo 6. Find:

- the order of the group (1 mark)
- the order of each element in the group (3 marks)
- a subgroup of order 3. (1 mark)

- E/P** 4 The operation $\circ$ is defined on the set H , where $H = \{0, 1, 2, 4, 5, 6\}$ by $x \circ y = x + y + 2xy \pmod{7}$
- a i Complete the Cayley table shown to the right.
 ii Show that $(H, \circ)$ is a group. You may assume that the associative axiom is satisfied. **(6 marks)**
- b Find:
 i an element that generates $(H, \circ)$
 ii a subgroup of order 3
 iii a subgroup of order 2 **(5 marks)**

$\circ$	0	1	2	4	5	6
0		1				
1		4				
2						
4					0	2
5						
6					1	

- E/P** 5 The set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ forms a group under multiplication modulo 11.
- a State the order of $(U, \times_{11})$, and hence write down the possible orders of its proper subgroups. **(2 marks)**
- b Show that U is cyclic and write down its generators. **(5 marks)**
- c Find all the proper subgroups of $(U, \times_{11})$ **(4 marks)**

- P** 6 The integers together with addition form the group $(\mathbb{Z}, +)$. State, with reasons, which of the following sets form subgroups of $(\mathbb{Z}, +)$ under the operation of addition.
- a $\mathbb{Z}^+$ b $\{2k : k \in \mathbb{Z}\}$ c $\mathbb{R}$ d $\{-1, 1\}$

- E/P** 7 The set $S = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under multiplication modulo 20.
- a Explain why S cannot have a subgroup of order 3. **(1 mark)**
- b Find the order of each element of S . **(3 marks)**
- c Find three different subgroups of S , each of order 4. **(4 marks)**

Watch out One of the three subgroups cannot be generated by a single element of S .

- P** 8 The Cayley table shows the action of a binary operation $*$ on the set $S = \{a, b, c, d, e, f, g\}$.
- a Show that the set $G = \{a, b, c\}$ forms a group under $*$. You may assume that the associative law is satisfied.
- b S contains 7 elements, and the order of g is 3. What can you deduce about S from this information? Give a reason for your answer.

$*$	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	c	a	e	f	g	d
c	c	a	b	f	g	d	e
d	d	e	f	g	a	b	c
e	e	f	g	a	d	c	b
f	f	g	d	b	c	e	a
g	g	d	e	c	b	a	f

- E/P** 9 The set $\mathbb{C}_{\neq 0}$ of non-zero complex numbers forms a group under complex multiplication. Show that the set $S = \{z \in \mathbb{C}_{\neq 0} : |z| = 1\}$ of points formed by the unit circle in the complex plane is a subgroup of $\mathbb{C}_{\neq 0}$. **(5 marks)**

Watch out $\mathbb{C}_{\neq 0}$ is not finite so you must show that S is closed, and that it contains inverses and an identity element. You can assume associativity as you are told that $\mathbb{C}_{\neq 0}$ is a group.

- E/P** 10 A finite group contains distinct elements x and y . Given that $x^5 = y^2$ and $|x| = 10$, find:
- a** $|x^2|$ **(1 mark)**
 - b** $|y^2|$ **(1 mark)**
 - c** $|y|$ **(1 mark)**
 - d** $|y^3|$ **(1 mark)**

- P** 11 Let G be a group with $|G| = p$, where p is a prime number. Explain why:

- a** G must be cyclic
- b** every element of G except the identity must generate G .

- P** 12 Let G be a finite group, and x be an element of the group of order 4. State, with reasons, whether each of the following statements is true or false.

- | | |
|---|--|
| a x is the identity element | b x is self-inverse |
| c x^2 is self-inverse | d x^3 is self-inverse |
| e $ G = 4k, k \in \mathbb{Z}^+$ | f x generates a subgroup of order 4 |
| g G cannot be a cyclic group | h $x^8 = e$ |
| i $x = x^5$ | j x^3 has order 4 |
| k x^2 has order 4 | |

- E/P** 13 A group H has order 8.
- a** State the possible orders of subgroups of H . **(2 marks)**

Given that H is the group formed by the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$ under addition modulo 8,

- b** find subgroups of each of the orders given in your answer to part **a**. **(4 marks)**

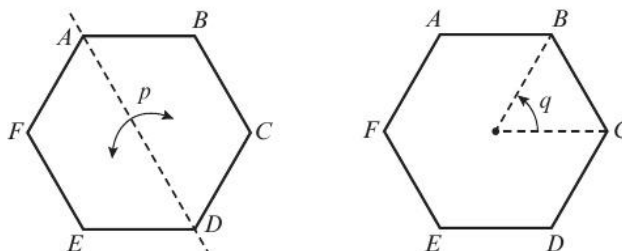
- P** 14 Prove that if G is a group with $|G| = p^2$, where p is a prime number, then G must have a subgroup of order p .

- P** 15 $\mathbb{Q}^\times$ is the group formed by the set of non-zero rational numbers under multiplication. State, with reasons, which of the following sets form subgroups of $\mathbb{Q}^\times$.

- | | |
|--|--|
| a $\mathbb{Z}_{\neq 0}$ (the non-zero integers) | b $\{x : x \in \mathbb{Q}, x > 0\}$ |
| c $\{-1, 1\}$ | d $\mathbb{R}_{\neq 0}$ (the non-zero real numbers) |
| e $\{3^k : k \in \mathbb{Z}\}$ | f $\{1\}$ |
| g $\{x : x \in \mathbb{Q}, x < 0\}$ | h $\{x : x \in \mathbb{Q}, x < 0\} \cup \{1\}$ |

- E/P** 16 The set of real-valued non-singular matrices forms a group under matrix multiplication. Show that the matrix $\begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$ generates a finite subgroup of this group, and state the order of this group. **(4 marks)**

- E/P** 17 S_4 is the group of all possible permutations of 4 elements under the operation of composition.
- Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ generates a subgroup of S_4 of order 3. (3 marks)
 - Find a subgroup of S_4 of order 2. (2 marks)
- P** 18 The rigid symmetries of a regular hexagon $ABCDEF$ form a group under the operation of composition. This group contains the element p representing a reflection in the line through A and D , and the element q representing a rotation through 60° anticlockwise about the centre of the hexagon.



- Write down the order of p and the order of q .
- Construct a Cayley table for the subgroup generated by p
- Describe the effect of the transformation q^2 , and write down the elements of the subgroup generated by q^2 in terms of q .

Challenge

- Let G be a group and H be a finite non-empty subset of G . Given that H is closed under the group operation of G , prove that H is a subgroup of G .
- Consider a group $(G, \circ)$ with an identity element e .
 - Given that $x \in G$ has order n , state the order of x^{-1} . Justify your answer.
 - For $x, y, z \in (G, \circ)$, prove that $y = z^{-1}xz \Rightarrow y^n = z^{-1}x^n z$ for $n \in \mathbb{Z}^+$.

Hint Look at Example 18 for a clue about how to begin.

Hint In part **b**, use mathematical induction.

2.4 Isomorphism

A Sometimes groups defined differently can behave in the same way. If two groups contain exactly the same number of elements, and if those elements combine under the group operation in exactly the same way, then the two groups are **isomorphic**. Consider the following two groups:

- $i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ under composition of permutations
- $\{0, 1, 2\}$ under addition modulo 3

The Cayley tables for these two groups are:

$\circ$	i	α	β	$+$	0	1	2
i	i	α	β	0	0	1	2
α	α	β	i	1	1	2	0
β	β	i	α	2	2	0	1

A You can show that the elements of the two groups behave the same under the group operation by setting up a **one-to-one function** that maps elements of one group onto elements of the other:

$$f(i) = 0, f(\alpha) = 1 \text{ and } f(\beta) = 2$$

You can see from the Cayley tables that this function preserves group operations. For example,

$$\alpha \circ \beta = i \text{ and } 1 + 2 = 0$$

$$\text{So } f(\alpha) + f(\beta) = f(\alpha \circ \beta) \quad \text{Because } f(i) = 0$$

This technique allows you to formally define group isomorphism:

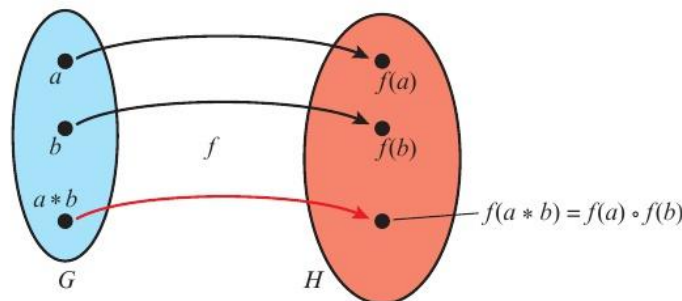
■ **Two groups $(G, *)$ and $(H, \circ)$ are isomorphic if there exists a mapping $f: G \rightarrow H$ such that:**

- **f maps all of the elements of G onto all of the elements of H**
- **f is one-to-one**
- **f preserves structure: $f(a * b) = f(a) \circ f(b)$**

Note If two groups are isomorphic then they are considered to be **exactly the same** for the purposes of group theory.

Notation If $(G, \circ)$ and $(H, *)$ are isomorphic you write $G \cong H$. The function f is called an **isomorphism** from G to H . Its inverse f^{-1} would be an isomorphism from H to G .

Because the group operation is preserved, it makes no difference whether you apply the function before or after combining elements:



Example 25

Let $(G, *)$ and $(H, \circ)$ be isomorphic groups with identity elements e_G and e_H respectively, and let $f: G \rightarrow H$ be an isomorphism from G to H .

Prove that $f(e_G) = e_H$.

$$f(e_G * e_G) = f(e_G) \circ f(e_G)$$

By the definition of an isomorphism

$$\Rightarrow f(e_G) = f(e_G) \circ f(e_G)$$

$$e_G * e_G = e_G$$

$$\Rightarrow f(e_G) \circ e_H = f(e_G) \circ f(e_G)$$

$$f(e_G) \in H$$

$$\Rightarrow (f(e_G))^{-1} \circ f(e_G) \circ e_H = (f(e_G))^{-1} \circ f(e_G) \circ f(e_G)$$

$$\Rightarrow e_H = f(e_G)$$

Cancel by left-multiplying by the inverse of $f(e_G)$.

A ■ If $(G, *)$ and $(H, \circ)$ are isomorphic groups with identity elements e_G and e_H respectively, and $f: G \rightarrow H$ is an isomorphism from G to H then, for all $a \in G$ and $n \in \mathbb{Z}$,

- $f(e_G) = e_H$
- $f(a^{-1}) = (f(a))^{-1}$
- $f(a^n) = (f(a))^n$

Note Group isomorphisms preserve **identities**, **inverses**, and the **order** of elements.

→ Exercise 2D, Q2

■ Group isomorphisms also preserve order and subgroups:

- $|G| = |H|$
- If G has k elements of order n , then H has k elements of order n .
- If G has k subgroups of order n , then H has k subgroups of order n .
- If J is a subgroup of G , then H has a subgroup isomorphic to J .

Problem-solving

If G has an element of order $|G|$ then H has an element of order $|H|$. In other words, if G is cyclic, then H is cyclic.

Example 26

The Cayley tables for two isomorphic groups G and H are shown to the right.

- State the identity element of each group.
- Describe an isomorphism from G onto H .

$(G, *)$	a	b	c	d	$(H, \circ)$	1	3	5	7
a	b	a	d	c	1	1	3	5	7
b	a	b	c	d	3	3	1	7	5
c	d	c	b	a	5	5	7	1	3
d	c	d	a	b	7	7	5	3	1

- a** In group G , b is the identity.
In group H , 1 is the identity.

- b** $f(b) = 1$
 $f(a) = 3$
 $f(c) = 7$
 $f(d) = 5$

The row corresponding to the identity matches the top row.

You know that the identity element in G must map to the identity element in H , so $f(b) = 1$. Try other mappings until you find one that preserves the structure of the Cayley table.

Example 27

G and H are cyclic groups with $|G| = |H|$. Prove that $G \cong H$.

G and H are both cyclic, so they both contain generators, g and h respectively.
Define a mapping $f: G \rightarrow H$ as $f(g^r) = h^r$ for $r \in \mathbb{Z}$.
 f maps all elements of G to all elements of H
 g is a generator of G so $\{g^r : r \in \mathbb{Z}\}$ is exactly the elements of G .
 h is a generator of H so $\{h^r : r \in \mathbb{Z}\}$ is exactly the elements of H .

You can use the generators of each group to define an isomorphism between the two groups. Once you have defined the mapping, you need to show that it is an isomorphism.

A

f is one-to-oneIf $h^j = h^k$ then $j \equiv k \pmod{n} \Rightarrow g^j = g^k$ So $f(g^j) = f(g^k) \Rightarrow g^j = g^k$ f preserves structure $f(g^j \circ g^k) = f(g^{j+k}) = h^{j+k} = h^j \circ h^k = f(g^j) \circ f(g^k)$ So f is an isomorphism from G onto H .

If you need to show that a mapping is one-to-one, it is sufficient to show that $f(a) = f(b) \Rightarrow a = b$.

Problem-solving

The result proved in Example 27 means that there is only one cyclic group of any given order. If you need to specify an isomorphism between cyclic groups you should find generators for each group and map corresponding powers of each generator onto each other:

$$\begin{array}{ccccccc} \{e, g, g^2, g^3, \dots, g^{n-1}\} \\ \downarrow \downarrow \downarrow \downarrow \downarrow \\ \{e, h, h^2, h^3, \dots, h^{n-1}\} \end{array}$$

In Example 26, the elements in G were written in the Cayley table in a different order to the elements in H . This can make it hard to spot group isomorphisms from Cayley tables, especially with larger groups.

You can find isomorphisms between finite groups by classifying **all possible groups** of a given order, and considering their properties. In your examination you will only need to consider isomorphisms of finite groups of order 8 or less.

Notation

Some of these groups have special names, which can be useful to learn. ← Section 2.2

Order	Name	Examples	Properties
1	$\mathbb{Z}_1$	Trivial group	Only group of order 1
2	$\mathbb{Z}_2$	$\{0, 1\}$ under $+_2$	Only group of order 2
3	$\mathbb{Z}_3$	$\{0, 1, 2\}$ under $+_3$	Only group of order 3
4	$\mathbb{Z}_4$	$\{0, 1, 2, 3\}$ under $+_4$	Cyclic group of order 4
	Klein four-group (K_4)	Symmetry group of a rectangle	Only non-cyclic group of order 4 Every element (except the identity) has order 2.
5	$\mathbb{Z}_5$	$\{0, 1, 2, 3, 4\}$ under $+_5$	Cyclic group of order 5
6	$\mathbb{Z}_6$	$\{0, 1, 2, 3, 4, 5\}$ under $+_6$	Cyclic group of order 6
	S_3, D_6	Set of all possible permutations of 3 elements, symmetry group of an equilateral triangle.	No element of order 6
7	$\mathbb{Z}_7$	$\{0, 1, 2, 3, 4, 5, 6\}$ under $+_7$	Cyclic group of order 7
8	$\mathbb{Z}_8$	$\{0, 1, 2, 3, 4, 5, 6, 7\}$ under $+_8$	Cyclic group of order 8
	D_8	Symmetry group of a square	No element of order 8 Exactly 2 elements of order 4
	$\mathbb{Z}_4 \times \mathbb{Z}_2$		No element of order 8 Exactly 4 elements of order 4
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$		No element of order 8 Every element (except the identity) has order 2.
	Quaternion group		No element of order 8 Exactly 6 elements of order 4

- A** From the table above, there are two different groups of order 4, two different groups of order 6, and five different groups of order 8. In each case, the orders of the elements of each group are different.

■ **Groups of order 8 or less can be classified entirely by the orders of their elements.**

Example 28

The group G consists of the elements $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ under the operation of matrix multiplication.

The set $H = \{1, 3, 5, 7, 9, 11, 13, 15\}$ forms a group under multiplication modulo 16.

- a** Show that H contains a subgroup that is isomorphic to G .
b Determine whether H is isomorphic to the symmetry group of a square, giving reasons for your answer.

a Orders of elements in G

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element so has order 1.

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

each have order 2.

So G is the Klein four-group.

Orders of elements in H

1 is the identity so has order 1.

$3^2 \equiv_{16} 5^2 \equiv_{16} 11^2 \equiv_{16} 13^2 \equiv_{16} 9$ so none of these elements have order 2.

However, $3^4 \equiv_{16} 5^4 \equiv_{16} 11^4 \equiv_{16} 13^4 \equiv_{16} 1$

So 3, 5, 11, 13 all have order 4.

$7^2 \equiv_{16} 9^2 \equiv_{16} 15^2 \equiv_{16} 1$

So 7, 9 and 15 all have order 2.

If H has a subgroup isomorphic to G then it must be $K = \{1, 7, 9, 15\}$.

Check that $K = \{1, 7, 9, 15\}$ is a subgroup of H :

$$7 \times 9 \equiv_{16} 9 \times 7 \equiv_{16} 15$$

$$7 \times 15 \equiv_{16} 15 \times 7 \equiv_{16} 9$$

$$9 \times 15 \equiv_{16} 15 \times 9 \equiv_{16} 7$$

$$7^2 \equiv_{16} 9^2 \equiv_{16} 15^2 \equiv_{16} 1$$

K is closed under multiplication modulo 16, so it is a subgroup of H .

K is also the Klein four-group, so $K \cong G$ and K is a subgroup of H as required.

Note The names of the groups of order 8 are given here for completeness. You do not need to know these names for your exam.

Note For groups of order 16 or greater, it is possible to find non-isomorphic groups which have exactly the same numbers of elements of each order.

Problem-solving

You will be able to solve many problems about group isomorphisms by finding the orders of the elements in each group.

G has no element of order 4, so it is not cyclic. The only non-cyclic group of order 4 is the Klein four-group.

The order of an element in a subgroup must be the same as its order in the group. Since the Klein four-group does not contain an element of order 4, none of the elements of order 4 could be contained in a subgroup isomorphic to it.

H is a finite group so if K is a subset of H which is closed under the group operation, then K is a subgroup of H .

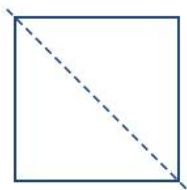
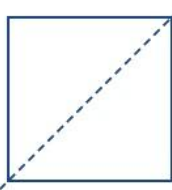
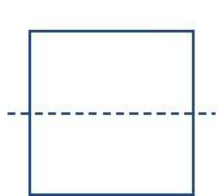
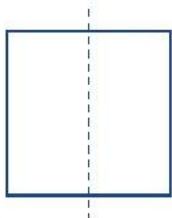
K is a group of order 4 under $\times_{16}$, and has three elements of order 2, so it is the Klein four-group.

A

- b The symmetry group of a square, D_8 , consists of the following elements:



Identity (order 1)

Rotation 90° (order 4)Rotation 180°
(order 2)Rotation 270°
(order 4)

Four different reflections (each of order 2)

So D_8 contains exactly 2 elements of order 4.

H contains 4 elements of order 4,

so H is not isomorphic to D_8 .

Write out the elements of the group, and state the order of each element.

A clockwise rotation of 270° is the same as an anticlockwise rotation of 90° . You would need to perform this operation 4 times to get back to the original square (the identity).

Watch out Make sure you show your working by stating the order of each element, and write a clear conclusion based on your working.

Isomorphic groups must contain exactly the same number of elements of each order.

Exercise 2D

- P** 1 $(G, *)$ and $(H, \circ)$ are isomorphic groups, and $f: G \rightarrow H$ is an isomorphism from G to H . Prove that, for all $a \in G$ and $n \in \mathbb{Z}^+$,

a $f(a^{-1}) = (f(a))^{-1}$

b $f(a^n) = (f(a))^n$

Problem-solving

Use mathematical induction for part b.

- E/P** 2 The set $G = \{1, -1, i, -i\}$ forms a group under complex multiplication. The set $H = \{0, 1, 2, 3\}$ forms a group under addition modulo 4.

a Draw Cayley tables for each group.

(4 marks)

b By defining an isomorphism, show that $G \cong H$.

(4 marks)

- A** 3 The set $G = \{1, 3, 5, 7\}$.
- E/P** a Show that $(G, \times_8)$ is a group. (5 marks)
- b Find all solutions in G to the equation $7 \circ x \circ 3 = y$. Express your answers in the form (x, y) . (3 marks)
- The set $H = \{1, 3, 5, 7, 9\}$.
- c Show that H does not form a group under multiplication modulo 10. (3 marks)
- d Create another set, K , by removing one element from H so that $(K, \times_{10})$ is a group. (1 mark)
- e Determine, with reasons, whether $(G, \times_8)$ and $(K, \times_{10})$ are isomorphic. (2 marks)
- E/P** 4 Consider a group G , of order 4, which has 4 distinct elements e, a, b and c , where e is the identity.
- a Explain why ab cannot equal a or b . (3 marks)
- b Given that c is self-inverse, construct two possible Cayley tables for G . Your Cayley tables should show two groups which are **not** isomorphic. (4 marks)
- The set $H = \{1, -1, i, -i\}$ forms a group under complex multiplication.
- c Determine which one of the groups defined in your answer to part **b** is isomorphic to H , and specify an isomorphism between $\{a, b, c, e\}$ and $\{1, -1, i, -i\}$. (6 marks)
- E/P** 5 The set $G = \{1, 7, 11, 13, 17, 19, 23, 29\}$ forms a group under multiplication modulo 30.
- a Find the order of each element of $(G, \times_{30})$. (3 marks)
- b Find three distinct subgroups of $(G, \times_{30})$, each of order 4. Describe each of these subgroups. (4 marks)
- The group D_8 is the symmetry group of a square.
- c By considering the elements of D_8 corresponding to reflections, or otherwise, show that G is not isomorphic to D_8 . (4 mark)
- E/P** 6 The group $G = \{1, 2, 3, 4, 5, 6\}$ forms a group under multiplication modulo 7.
- a Find the order of each element of $(G, \times_7)$. (4 marks)
- b List all the proper subgroups of $(G, \times_7)$ and describe each group. (3 marks)
- The group $H = \{1, 5, 7, 11, 13, 17\}$ forms a group under multiplication modulo 18.
- c Specify an isomorphism between G and H . (4 marks)
- E/P** 7 a Given that G is a group of order p , where p is a prime number, explain G must be isomorphic to the cyclic group of order p . (3 marks)
- The set $G = \{1, 7, 16, 20, 23, 24, 25\}$ forms a group under multiplication modulo 29.
- The set $H = \{e^{\frac{2k\pi i}{7}} : k \in \{0, 1, 2, 3, 4, 5, 6\}\}$ forms a group under complex multiplication.
- b Specify an isomorphism between G and H . (3 marks)

Problem-solving

To **describe** a group of order 4 you should state whether it is the **cyclic group** or the **Klein four-group**. Alternatively, you should fully specify the orders of each of its elements.

- A** 8 The elements of G are the complex numbers $e^{\frac{k\pi i}{4}}$, where $k = 0, 1, 2, 3, 4, 5, 6, 7$.
E/P G forms a group under complex multiplication.
 The set $H = \{1, 7, 9, 11, 17, 19, 25, 27\}$ forms a group under multiplication modulo 32.
 Specify an isomorphism between $(G, \times)$ and $(H, \times_{32})$. **(4 marks)**
- E/P** 9 The set $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \right\}$ forms a group under matrix multiplication.
 The set $H = \{1, 5, 7, 11\}$ forms a group under the operation of multiplication modulo 12.
 Determine whether G and H are isomorphic, showing your working clearly. **(5 marks)**
- E/P** 10 The set G consists of eight 2×2 matrices:

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\}$$

 G forms a group under matrix multiplication.
a Find the order of each element in this group. **(4 marks)**
b Explain why this group cannot have a subgroup isomorphic to the Klein four-group. **(3 marks)**
 The set $H = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under multiplication modulo 20.
c Determine whether G is isomorphic to H , showing your working clearly. **(3 marks)**

Challenge

The set $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \{0, 1\}, ad - bc \neq 0 \right\}$ consists of all non-singular 2×2 matrices with elements 0 or 1.

- a i** List all the elements of S .

The operation $\times_2$ is defined as matrix multiplication modulo 2. Matrices are multiplied in the normal way, and each element is replaced with its least residue modulo 2.

- ii** Show that S forms a group under $\times_2$. You may assume that the associative law is satisfied.

- iii** Describe one other group which is isomorphic to this group.

The set $T = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \{0, 1, 2\}, ad - bc \not\equiv 0 \pmod{3} \right\}$ forms a group under matrix multiplication modulo 3.

- b i** Find the order of this group.

- ii** Find the inverse of the element $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$.

Mixed exercise 2

- (E/P)** 1 A group G , under the operation of multiplication, contains distinct elements a , b and e , where e is the identity element.
- a Show that $ab^2 \neq a^2b$. (1 mark)
- b Given that $ab^2 = ba$, prove that $ab \neq ba$. (3 marks)
- (E)** 2 The set $G = \{1, 3, 5, 9, 11, 13\}$ forms a group under multiplication modulo 14. Copy and complete the following Cayley table for this group.

$\times_{14}$	1	3	5	9	11	13
1			5			
3		9				
5						
9				11		
11		5				
13						1

(3 marks)

- (E/P)** 3 The set $S = \{1, 3, 5, 7, 9, 11, 13, 15\}$ forms a group under the operation of multiplication modulo 16.
- a List the order of each element in $(S, \times_{16})$. (2 marks)
- b State, with a reason, whether this group is cyclic. (2 marks)
- c Explain why $(S, \times_{16})$ can have no subgroup of order 3. (1 mark)
- d Find a cyclic subgroup of $(S, \times_{16})$ and state a generator of this subgroup. (3 marks)

- (E/P)** 4 a Describe the linear transformation represented by the matrix

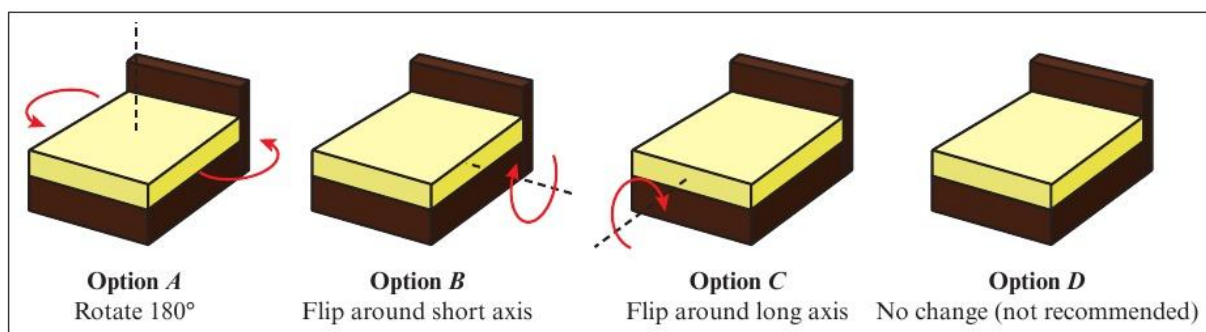
$$M = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix}$$

(2 marks)

A group $(G, \circ)$ is generated by M , where $\circ$ represents matrix multiplication.

- b Write down $|G|$, and write the elements of G in terms of M . (4 marks)
- c Write in the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$
- i M^{-1}
- ii two further generators of G . (2 marks)
- d Find a subgroup of $(G, \circ)$ of order 4, giving each element in terms of M . (2 marks)

- E/P** 5 A mattress manufacturer suggests that customers ‘flip’ their mattress regularly so that it wears out evenly. The following instructions are provided:



The operation $\circ$ is defined on $\{A, B, C, D\}$ as ‘followed by’, so that, for example, $C \circ A$ means ‘flip around long axis then rotate 180°’.

- a Complete the Cayley table for these four options, under the operation of combination of transformations, $\circ$. (3 marks)
- b Assuming associativity, show that these four options form a group under $\circ$. (3 marks)
- c State, with a reason, whether this group is cyclic. (2 marks)

		Second option				
		◦	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
First option	<i>A</i>					
	<i>B</i>					
	<i>C</i>					
	<i>D</i>					

- E/P** 6 The operation $\circ$ is defined on the set $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ by

$$x \circ y = x + y - 2xy \pmod{8}$$

- a i Copy and complete the Cayley table shown. (6 marks)
- ii Show that $(G, \circ)$ is a group. You may assume that the associative axiom is satisfied.
- b Find: (5 marks)
- i an element $a \in G$, other than the identity such that $a = a^{-1}$
 - ii a subgroup of G of order 4.
- c Show that $(G, \circ)$ is not cyclic. (3 marks)

$\circ$	0	1	2	3	4	5	6	7
0		1	2					
1		0						
2								
3							5	0
4								
5						0	7	
6		3						
7		2	5					

- E/P** 7 a Explain why the set of real-valued 2×2 matrices do not form a group under matrix multiplication. (1 mark)
- b Show that the set of non-singular real-valued 2×2 matrices form a group under matrix multiplication. You should state the identity element, and give the inverse of the general 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. You may assume that the associative axiom is satisfied. (5 marks)

- E/P** 8 The binary operator multiplication modulo 18, denoted by $\circ$, is defined on the set $G = \{2, 4, 8, 10, 14, 16\}$

a i Copy and complete the Cayley table below.

$\circ$	2	4	8	10	14	16
2		8		2		
4	8	16	14	4	2	10
8		14		8		
10	2	4	8	10	14	16
14		2		14		
16		10		16		

ii Show that $(G, \circ)$ is a group. You may assume that the associative axiom is satisfied.

(6 marks)

b Show that the element 4 has order 3.

(2 marks)

c Find an element which generates $(G, \circ)$, and write each element in terms of this generator.

(3 marks)

d Set H is defined by $\{x^2 : x \in G\}$. Show that $(H, \circ)$ is a subgroup of $(G, \circ)$.

(2 marks)

- E/P** 9 a Show that the set $S = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6 is a group.

(5 marks)

b Show that the group is cyclic and write down its generators.

(3 marks)

c Explain why $(S, +_6)$ cannot contain a subgroup of order 4.

(1 mark)

d Find the subgroup of $(S, +_6)$ that contains exactly three elements.

(1 mark)

- E/P** 10 Consider the set S of matrices of the form $\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, where $x, y \in \mathbb{R}$.

a Show that S forms a group under matrix multiplication. You may assume that the associative law is satisfied.

(5 marks)

The set R consists of matrices of the form $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ where $x \in \mathbb{R}, x \neq 0$.

b Show that R is a subgroup of S .

(5 marks)

The set T consists of matrices of the form $\begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix}$ where $y \in \mathbb{R}, y \neq 0$.

c Show that T is not a subgroup of S .

(2 marks)

- A** 11 The set $G = \{1, 5, 7, 11, 13, 17, 19, 23\}$ forms a group under multiplication modulo 24.

E/P a Find the order of each element in this group.

(4 marks)

b Explain clearly why this group cannot contain a cyclic subgroup of order 4.

(2 marks)

The elements of H are the complex numbers $e^{\frac{k\pi i}{4}}$, where $k = 0, 1, 2, 3, 4, 5, 6, 7, 8$. H forms a group under complex multiplication.

c Determine, with reasons, whether $G \cong H$.

(3 marks)

A 12 Groups A , B and C are defined as follows.

E/P

A : the set of numbers $\{1, 3, 7, 9\}$ under multiplication modulo 10

B : the set of numbers $\{1, 2, 4, 8\}$ under multiplication modulo 15

C : the set of matrices $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$ under matrix multiplication

a Write down the identity element for each of groups A , B and C . **(2 marks)**

b Determine in each case whether the groups

i A and B **ii** B and C **iii** A and C

are isomorphic. In each case give reasons for your answers. **(5 marks)**

E/P 13 The elements of a group G are the matrices

$$\begin{pmatrix} \cos \frac{k\pi}{3} & \sin \frac{k\pi}{3} \\ -\sin \frac{k\pi}{3} & \cos \frac{k\pi}{3} \end{pmatrix}$$

where $k = 1, 2, 3, 4, 5, 6$.

a State the order of the group and the order of each of its elements. **(4 marks)**

b Determine, with reasons, whether this group is isomorphic to the group of permutations of three elements, S_3 . **(2 marks)**

Challenge

The set S_4 consists of all possible permutations of four objects under composition of permutations.

a Find $|S_4|$.

b Find subgroups $G \subseteq S_4$ with each of the following properties. In each case, list the elements of the subgroup in the form

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}$$

where $a_i, b_i \in \{1, 2, 3, 4\}$.

i G is a cyclic group of order 4

ii G is a cyclic group of order 3

iii $|G| = 6$

A

c Find a subgroup of S_4 that is isomorphic to:

i the Klein four-group

ii the symmetry group of a square, D_8 .

d Explain why S_4 has no subgroups that are isomorphic to:

i the cyclic group of order 6

ii the group $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15.

Summary of key points

- 1 A **binary operation** on a set is a calculation that combines two elements of the set to produce another element of the set.
- 2 An **identity element** of a set S under a binary operation $*$ is an element $e \in S$ such that, for any element $a \in S$, $a * e = e * a = a$.
- 3 Let S be a set and $*$ be a binary operation on S . If an identity element e exists, and there exist elements $a, b \in S$ such that $a * b = b * a = e$, then a is the **inverse** of b and b is the inverse of a .
- 4 A binary operation $*$ on a set S is **associative** if, for any $a, b, c \in S$,

$$a * (b * c) = (a * b) * c$$
- 5 If G is a set and $*$ is a binary operation defined on G , then $(G, *)$ is a **group** if the following four axioms hold:
 - **Closure**: for all $a, b \in G$, $a * b \in G$
 - **Identity**: there exists an identity element $e \in G$, such that for all $a \in G$, $a * e = e * a = a$
 - **Inverses**: for each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$
 - **Associativity**: for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$
- 6 A **Cayley table** fully describes the structure of a finite group by showing all possible products of elements of the group. When a group's elements are displayed in a Cayley table, then:
 - all entries must be members of the group
 - every entry appears exactly once in every row and every column
 - the identity element must appear in every row and column.
 - the identity elements are symmetric across the leading diagonal
- 7 • The operation $\times_n$ of **multiplication modulo n** is defined on integers a and b as the remainder when ab is divided by n .
 • The operation $+_n$ of **addition modulo n** is defined on integers a and b as the remainder when $a + b$ is divided by n .
- 8 The **symmetric group on n elements** is defined as the group of all possible permutations that can be performed on n objects, together with the operation of composition.
- 9 A **cyclic group** is a group in which every element can be written in the form a^k , where a is the **group generator** and k is a positive integer.
- 10 If a finite group G has n distinct elements, then the **order** of G is n .
- 11 • The **order of an element** a in a group $(G, *)$ with identity e is the smallest positive integer k such that $a^k = e$.
 • If $(G, *)$ is finite with $a \in G$, then $|a|$ divides $|G|$
 • $(G, *)$ is cyclic if and only if there exists an element a such that $|a| = |G|$. This element will be a generator of the group.
- 12 Let a be an element in a group $(G, *)$, then:
 - if a has a finite order n , then $a^m = e$ if and only if $n|m$
 - if a has infinite order, then $x \neq y \Rightarrow a^x \neq a^y$
 - if $a^x = a^y$ with $x \neq y$, then a must have finite order.

- 13** If a nonempty subset H of a group G is itself a group under the binary operation of G , we call H a **subgroup** of G .
- If $H \subset G$, then H is a proper subgroup of G .
 - If $H \subseteq G$, then H is a subgroup of G .
- 14** Let G be a group and H a finite non-empty subset of G . Then, H is a subgroup of G if H is closed under the operation of G .
- 15** If G is a finite group, then any element $a \in G$ generates a subgroup of G , written $\langle a \rangle$.
- 16 Lagrange's theorem:** If H is a subgroup of a finite group G , then $|H|$ divides $|G|$.
- 17** Two groups $(G, *)$ and $(H, \circ)$ are **isomorphic** if there exists a mapping $f: G \rightarrow H$ such that:
- f maps all of the elements of G onto all of the elements of H
 - f is one-to-one
 - f preserves structure: $f(a * b) = f(a) \circ f(b)$
- 18** If $(G, *)$ and $(H, \circ)$ are isomorphic groups with identity elements e_G and e_H respectively, and $f: G \rightarrow H$ is an isomorphism from G to H then, for all $a \in G$ and $n \in \mathbb{Z}$,
- $f(e_G) = e_H$
 - $f(a^{-1}) = (f(a))^{-1}$
 - $f(a^n) = (f(a))^n$
- 19** Group isomorphisms also preserve order and subgroups:
- $|G| = |H|$
 - If G has k elements of order n , then H has k elements of order n .
 - If G has k subgroups of order n , then H has k subgroups of order n .
 - If J is a subgroup of G , then H has a subgroup isomorphic to J .
- 20** Groups of order 8 or less can be classified entirely by the orders of their elements.

3

Complex numbers

Objectives

After completing this chapter you should be able to:

- Determine the loci of sets of points, z , in an Argand diagram given in the forms $|z - a| = k|z - b|$ and $\arg\left(\frac{z - a}{z - b}\right) = \beta$, where $k, \beta \in \mathbb{R}$, $k > 0$, $k \neq 1$ and $a, b \in \mathbb{C}$ → pages 00-00
- Represent regions on an Argand diagram, including those of the forms $\alpha \leq \arg(z - z_1) \leq \beta$ and $p \leq \operatorname{Re}(z) \leq q$, where $\alpha, \beta, p, q \in \mathbb{R}$ and $z_1 \in \mathbb{C}$ → pages 00-00
- Apply elementary transformations that map points from the z -plane to the w -plane, including those of the forms $w = z^2$ and $w = \frac{az + b}{cz + d}$, where $a, b, c, d \in \mathbb{C}$. → pages 00-00

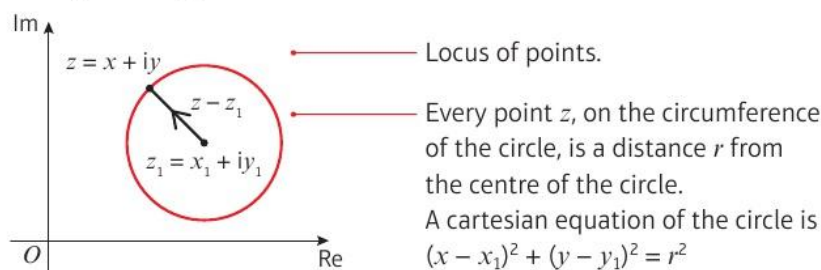
Prior knowledge check

- 1 A complex number z is represented by the point P in the complex plane. Given that $|z + 2 - 4i| = 3$,
 - a sketch the locus of P
 - b find the Cartesian equation of this locus. ← Core Pure Book 1, Chapter 2
- 2 Given that $|z - i| = |z - 4 + 3i|$,
 - a sketch the locus of z
 - b find the Cartesian equation of this locus. ← Core Pure Book 1, Chapter 2
- 3 Sketch the locus of z for $\arg(z + 2i) = \frac{2\pi}{3}$ ← Core Pure Book 1, Chapter 2
- 4 On separate Argand diagrams, shade in the regions represented by:
 - a $|z + 6| \geq |z + 2i|$
 - b $0 \leq \arg(z + 2 + 2i) \leq \frac{\pi}{2}$
 - c $\{|z + 6| \geq |z + 2i|\} \cup \left\{0 \leq \arg(z + 2 + 2i) \leq \frac{\pi}{2}\right\}$ ← Core Pure Book 1, Chapter 2

This is an image of a Julia set. It is a set of points in the complex plane that do not diverge when a given mapping is repeatedly applied to them.

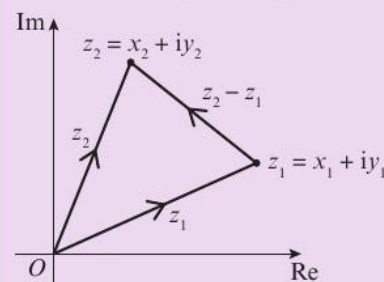
3.1 Loci in an Argand diagram

You can use complex numbers to describe a locus of points on an Argand diagram.



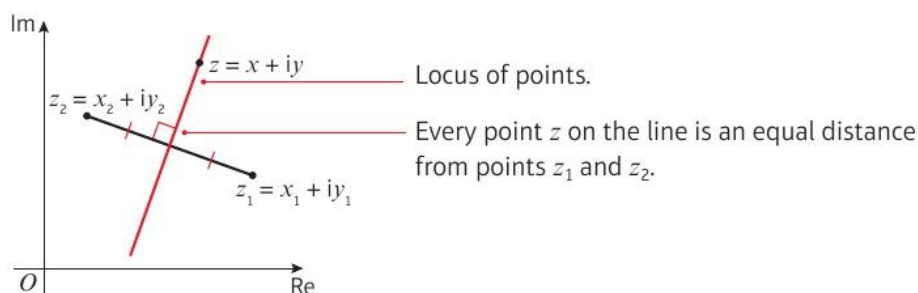
- Given $z_1 = x_1 + iy_1$, the locus of points z on an Argand diagram such that $|z - z_1| = r$, or $|z - (x_1 + iy_1)| = r$, is a circle with centre (x_1, y_1) and radius r .

Links $|z_2 - z_1|$ represents the distance between the points z_2 and z_1 on an Argand diagram:



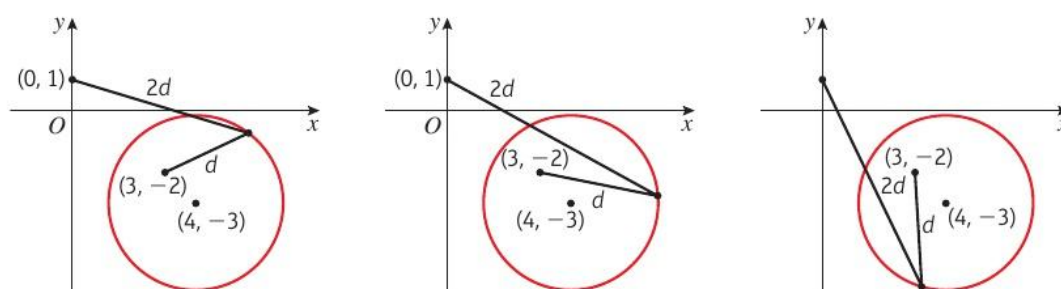
← Core Pure Book 1, Section 2.4

The locus of points that are an equal distance from two different points z_1 and z_2 is the perpendicular bisector of the line segment joining the two points.



- Given $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, the locus of points z on an Argand diagram such that $|z - z_1| = |z - z_2|$ is the perpendicular bisector of the line segment joining z_1 and z_2 .

You need to be able to determine the locus of a set of points whose distances from two fixed points are in a **constant ratio**. For example, the set of points that are exactly twice the distance from $(0, 1)$ as from the point $(3, -2)$. It is not intuitive, but this locus of points is a circle with its centre at $(4, -3)$.



If you replaced the coordinate axes above with an Argand diagram, this would be equivalent to the set of points that were twice as far from i as from $3 - 2i$. You could write this locus as the set of points z that satisfy $|z - i| = 2|z - (3 - 2i)|$.

- The locus of points z that satisfy $|z - a| = k|z - b|$, where $a, b \in \mathbb{C}$ and $k \in \mathbb{R}, k > 0, k \neq 1$ is a circle.

Links When $k = 1$ this locus is the perpendicular bisector of the line segment joining a and b . You can think of a straight line as a circle with an infinite radius. ← Core Pure Book 1, Section 2.4

You can find the centre and radius of the circle by finding its Cartesian equation.

Example 1

Given that $|z - 6| = 2|z + 6 - 9i|$,

- a use algebra to show that the locus of z is a circle, stating its centre and its radius
b sketch the locus of z on an Argand diagram.

a $|z - 6| = 2|z + 6 - 9i|$

$$\Rightarrow |x + iy - 6| = 2|x + iy + 6 - 9i|$$

$$\Rightarrow |(x - 6) + iy| = 2|(x + 6) + i(y - 9)|$$

$$\Rightarrow |(x - 6) + iy|^2 = 2^2|(x + 6) + i(y - 9)|^2$$

$$\Rightarrow (x - 6)^2 + y^2 = 4((x + 6)^2 + (y - 9)^2)$$

$$\Rightarrow x^2 - 12x + 36 + y^2 = 4(x^2 + 12x + 36 + y^2 - 18y + 81)$$

$$\Rightarrow x^2 - 12x + 36 + y^2 = 4x^2 + 48x + 144 + 4y^2 - 72y + 324$$

$$\Rightarrow 3x^2 + 60x + 3y^2 - 72y + 432 = 0$$

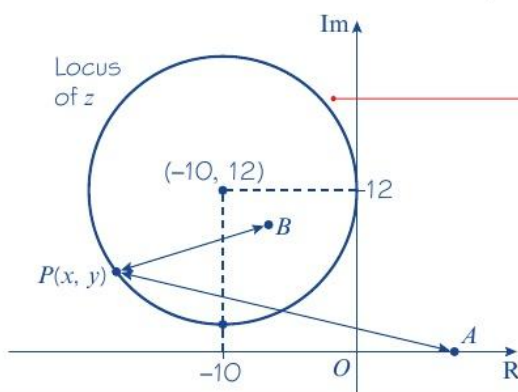
$$\Rightarrow x^2 + 20x + y^2 - 24y + 144 = 0$$

$$\Rightarrow (x + 10)^2 - 100 + (y - 12)^2 - 144 + 144 = 0$$

$$\Rightarrow (x + 10)^2 + (y - 12)^2 = 100$$

So the locus of z is a circle with centre $(-10, 12)$ and radius 10.

b



z can be written as $z = x + iy$.

Group the real and imaginary parts.

Square both sides.

Remove the moduli.

Complete the square twice for x and for y .

Circle $(x - a)^2 + (y - b)^2 = r^2$ with $(a, b) = (-10, 12)$ and $r = 10$.

Locus of z as required.

Problem-solving

$|z - 6|$ represents the distance from the point $A(6, 0)$ to P .

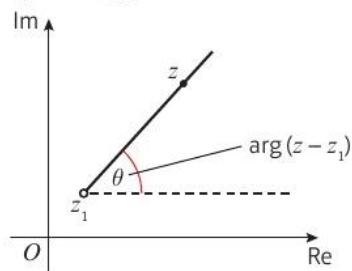
$|z + 6 - 9i| = |z - (-6 + 9i)|$ represents the distance from the point $B(-6, 9)$ to P .

$|z - 6| = 2|z + 6 - 9i|$ gives $AP = 2BP$. This means that P is the locus of points such that the distance AP is twice the distance BP .

One of the points will always be inside the circle and the other will always be outside the circle.

Another previous result for loci in an Argand diagram makes use of the geometric property of the argument of a complex number.

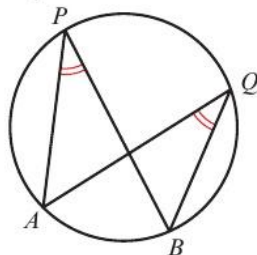
- Given $z_1 = x_1 + iy_1$, the locus of points z on an Argand diagram such that $\arg(z - z_1) = \theta$ is a half-line from, but not including, the fixed point z_1 making an angle θ with a line from the fixed point z_1 parallel to the real axis.



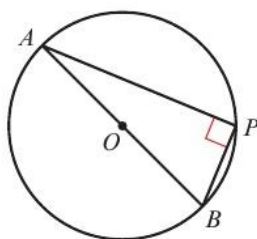
Watch out The endpoint z_1 is **not** included in the locus. You show this by drawing it with an open circle.

You can make use of the following circle properties to determine more complicated loci given in terms of arguments.

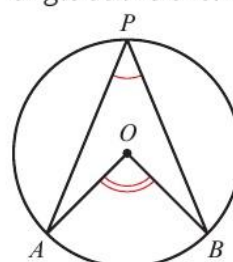
- Angles subtended at an arc in the same segment are equal.
- The angle in a semicircle is a right angle.
- The angle subtended at the centre of the circle is twice the angle at the circumference.



$$\angle APB = \angle AQB$$



$$\angle APB = \frac{\pi}{2}$$

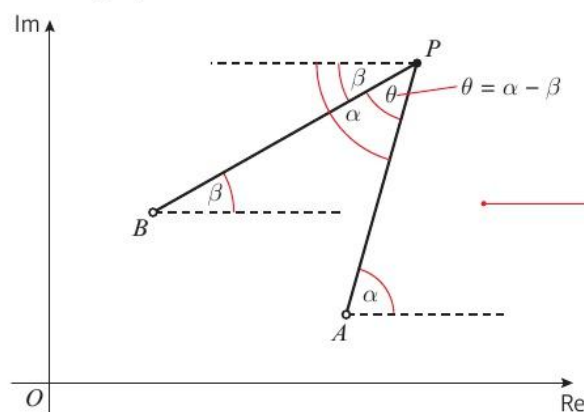


$$\angle AOB = 2\angle APB$$

- The locus of points z that satisfy $\arg\left(\frac{z-a}{z-b}\right) = \theta$, where $\theta \in \mathbb{R}$, $\theta > 0$ and $a, b \in \mathbb{C}$, is an arc of a circle with endpoints A and B representing the complex numbers a and b , respectively.

Watch out The endpoints of the arc, A and B , are **not** included in the locus.

You can see why this locus is the arc of a circle by drawing points A and B on an Argand diagram, and drawing a point P such that $\angle APB = \theta$, where θ is a positive, constant angle.



The solution shown for Example 2 below illustrates the same approach developed here.

From knowing the locus for an equation of the form $\arg(z - z_1) = \theta$, you can conclude that $\arg(z - a) = \alpha$ and $\arg(z - b) = \beta$. It follows that

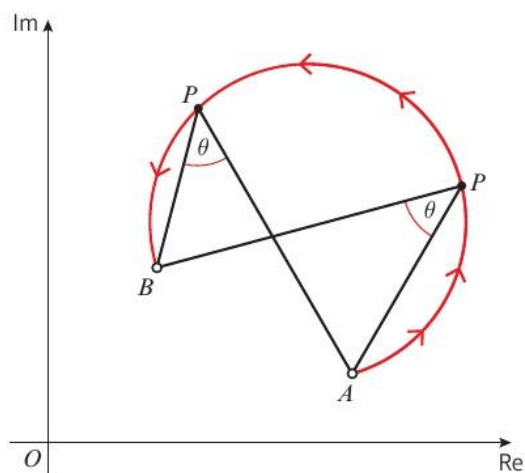
$$\angle APB = \alpha - \beta \quad \text{This is due to the properties of parallel lines.}$$

$$\theta = \alpha - \beta$$

$$= \arg(z - a) - \arg(z - b)$$

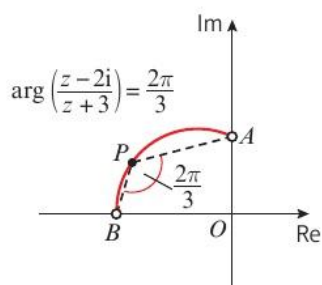
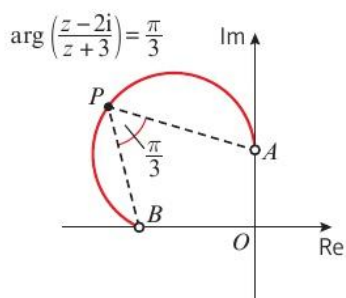
$$= \arg\left(\frac{z - a}{z - b}\right) \quad \arg\left(\frac{z_1}{z_2}\right) = \arg z_1 - \arg z_2 \quad \leftarrow \text{Core Pure Book 1, Section 2.3}$$

As P moves, $\angle APB$ is always equal to the constant θ , and the angle is always subtending the same segment. Thus, from the first circle property given on page XX, point P must lie on a circle. Therefore, the locus of P is the arc of a circle that is drawn **anticlockwise** from A to B .

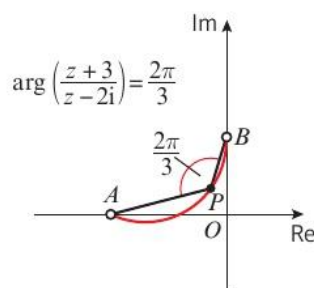
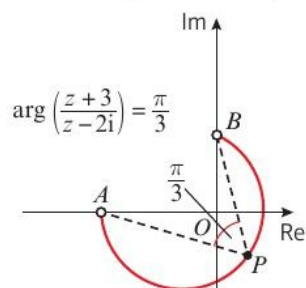


- If $\theta < \frac{\pi}{2}$, then the locus is a major arc of the circle.
- If $\theta > \frac{\pi}{2}$, then the locus is a minor arc of the circle.
- If $\theta = \frac{\pi}{2}$, then the locus is a semicircle.

In these two examples, $a = 2i$ and $b = -3$. The arcs are drawn **anticlockwise** from A to B .



In the following two examples the values of a and b are reversed.



Finding the centre of the circle on which the major or minor arc is located requires algebraic and/or geometric working. This is illustrated in the example below.

Example 2

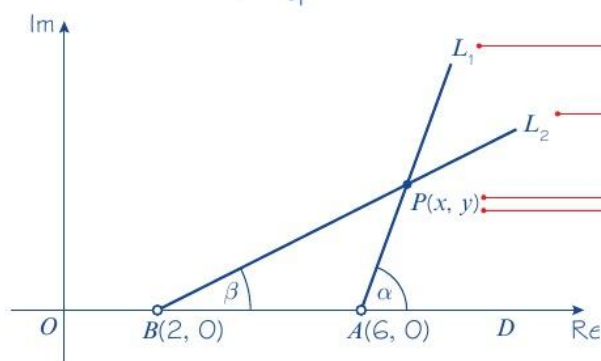
Given that $\arg\left(\frac{z-6}{z-2}\right) = \frac{\pi}{4}$,

- sketch the locus of $P(x, y)$ which is represented by z on an Argand diagram
- find the Cartesian equation of this locus.

a $\arg\left(\frac{z-6}{z-2}\right) = \arg(z-6) - \arg(z-2) = \frac{\pi}{4}$

Let L_1 be the half-line satisfying $\arg(z-6) = \alpha$
and let L_2 be the half-line satisfying $\arg(z-2) = \beta$.

It follows that $\alpha - \beta = \frac{\pi}{4}$ (1)



Use $\arg\left(\frac{z_1}{z_2}\right) = \arg(z_1) - \arg(z_2)$.

Use $\arg(z-6) - \arg(z-2) = \frac{\pi}{4}$

All points on L_1 satisfy $\arg(z-6) = \alpha$.

All points on L_2 satisfy $\arg(z-2) = \beta$.

Therefore the point P is found lying on both L_1 and L_2 where $\alpha - \beta = \frac{\pi}{4}$
As P lies on L_1 and L_2 , it is found where L_1 and L_2 intersect.

From $\triangle ABP$, it follows that

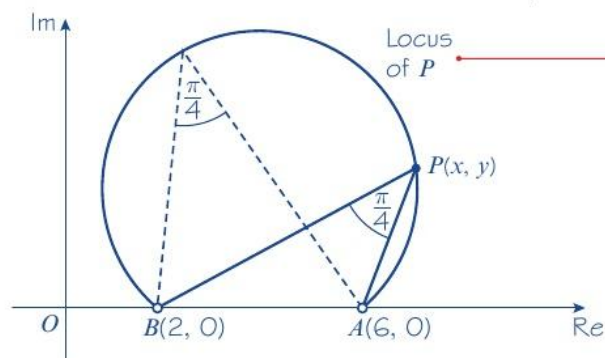
$$\angle BPA + \angle PBA = \angle PAD$$

$$\Rightarrow \angle BPA + \beta = \alpha$$

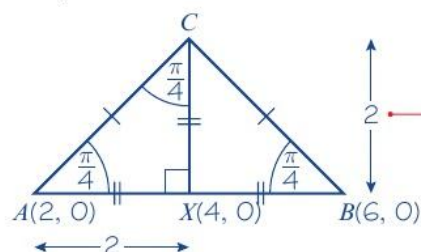
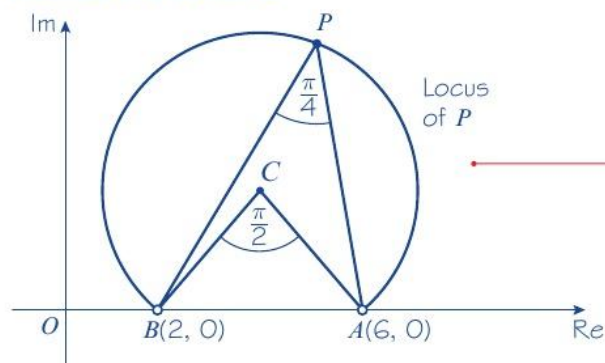
$$\Rightarrow \angle BPA = \alpha - \beta$$

$$\Rightarrow \angle BPA = \frac{\pi}{4}$$

As α and β vary, $\angle BPA$ is constant and is $\frac{\pi}{4}$



b Method 1: Geometric



$AX = CX = 2 \Rightarrow AC = \sqrt{2^2 + 2^2} = 2\sqrt{2}$ and C is the point $(4, 2)$.

So the Cartesian equation of the locus of P is $(x - 4)^2 + (y - 2)^2 = 8$, where $y > 0$.

The exterior angle of a triangle is the sum of the two opposite interior angles.

From the diagram, $\angle PBA = \beta$ and $\angle PAD = \alpha$.

$$\text{Use } \alpha - \beta = \frac{\pi}{4} \quad (1)$$

P can vary but $\angle BPA$ must always be $\frac{\pi}{4}$

From the circle theorems, angles in the same segment of a circle are equal.

Therefore as P varies, $\angle BPA$ will always be equal to $\frac{\pi}{4}$

So, since $\frac{\pi}{4} < \frac{\pi}{2}$ it follows that P must lie on the **major arc** starting at $(6, 0)$ and finishing at $(2, 0)$, but **not** including the points $(6, 0)$ and $(2, 0)$.

$\angle BPA = \frac{\pi}{4} \Rightarrow \angle ACB = \frac{\pi}{2}$, as the angle subtended at the centre of the circle is twice the angle at the circumference.

As CA and CB are both radii, then the radius is $r = CA = CB$.

This implies that $\triangle CAB$ is isosceles and $\angle CAB = \angle CBA = \frac{\pi}{4}$

Let X be the midpoint of AB . Hence

$$\angle CXA = \frac{\pi}{2} \text{ and } \angle XCA = \angle CAX = \frac{\pi}{4}$$

So $\triangle CAX$ is isosceles and $AX = CX = 2$.

Since the locus is the major arc of the circle which lies above the real axis, then the Cartesian equation for the locus must include the condition that $y > 0$.

Watch out The locus is only a part of a circle (an arc), so you need to give a suitable range of values for x and/or y to indicate which part of the circle is included.

Method 2: Algebraic

$$\begin{aligned}
 \frac{z-6}{z-2} &= \frac{x-6+iy}{x-2+iy} \\
 &= \frac{(x-6+iy)(x-2-iy)}{(x-2+iy)(x-2-iy)} \\
 &= \frac{x^2-8x+12+y^2+4iy}{(x-2)^2+y^2} \\
 &= \left(\frac{x^2-8x+12+y^2}{(x-2)^2+y^2} \right) + \left(\frac{4y}{(x-2)^2+y^2} \right)i \\
 \text{So } \arg \left(\left(\frac{x^2-8x+12+y^2}{(x-2)^2+y^2} \right) + \left(\frac{4y}{(x-2)^2+y^2} \right)i \right) &= \frac{\pi}{4} \\
 \Rightarrow \frac{x^2-8x+12+y^2}{(x-2)^2+y^2} &= \frac{4y}{(x-2)^2+y^2} \\
 \Rightarrow x^2-8x+12+y^2 &= 4y \\
 \Rightarrow (x-4)^2 + (y-2)^2 &= 8, \text{ where } y > 0
 \end{aligned}$$

Problem-solving

In order to deal with $\arg\left(\frac{z-6}{z-2}\right)$ algebraically, you need to identify its real and imaginary parts. Write $z = x + iy$ then multiply the numerator and denominator by $(z-2)^*$.

If $\arg w = \theta$, then $\frac{\operatorname{Im}(w)}{\operatorname{Re}(w)} = \tan \theta$. In this case, $\theta = \frac{\pi}{4}$ so the real and imaginary parts are equal.

Watch out

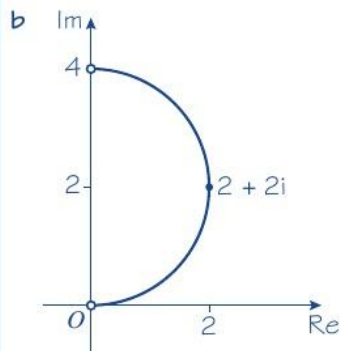
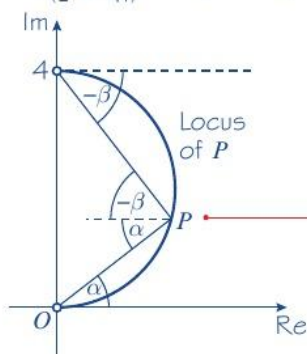
If you use an algebraic method to find the equation of the circle, you still need to use geometric considerations to work out which arc of the circle satisfies the given condition.

Example 3

Given the equation $\arg\left(\frac{z}{z-4i}\right) = \frac{\pi}{2}$,

- sketch the locus of points z that satisfy the equation on an Argand diagram.
- Hence write down the range of possible values of $\operatorname{Re}(z)$.

a $\arg\left(\frac{z}{z-4i}\right) = \arg z - \arg(z-4i) = \alpha - \beta$. So $\alpha - \beta = \frac{\pi}{2}$



The range of possible values for $\operatorname{Re}(z)$ are $0 < \operatorname{Re}(z) \leq 2$.

$\arg z = \alpha$ and $\arg(z-4i) = \beta$

$\arg\left(\frac{z}{z-4i}\right) = \frac{\pi}{2}$

$\alpha - \beta = \frac{\pi}{2}$ and $\alpha < \frac{\pi}{2} \Rightarrow \beta < 0$.

Since the constant angle at P is $\frac{\pi}{2}$, the locus of P is a semicircle from $(0,0)$ anticlockwise to $(0,4)$, not including $(0,0)$ and $(0,4)$.

Problem-solving

The point on the locus furthest to the right is $2 + 2i$, so the largest possible value of $\operatorname{Re}(z)$ is 2. The endpoints of the semicircle are at 0 and $4i$. These points are not included in the locus of z , so use a strict inequality to show the smallest possible value of $\operatorname{Re}(z)$.

Exercise 3A

1 Sketch the locus of z and give the Cartesian equation of the locus of z when:

a $|z + 3| = 3|z - 5|$

b $|z - 3| = 4|z + 1|$

c $|z - i| = 2|z + i|$

d $|z + 2 - 7i| = 2|z - 10 + 2i|$

e $|z + 4 - 2i| = 2|z - 2 - 5i|$

f $|z| = 2|2 - z|$

2 Sketch the locus of z when:

a $\arg\left(\frac{z}{z+3}\right) = \frac{\pi}{4}$

b $\arg\left(\frac{z-3i}{z+4}\right) = \frac{\pi}{6}$

c $\arg\left(\frac{z}{z-2}\right) = \frac{\pi}{3}$

d $\arg\left(\frac{z-3i}{z-5}\right) = \frac{\pi}{4}$

e $\arg z - \arg(z - 2 + 3i) = \frac{\pi}{3}$

f $\arg\left(\frac{z-4i}{z+4}\right) = \frac{\pi}{2}$

(E) 3 The complex number $z = x + iy$ satisfies the equation $|z + 1 + i| = 2|z + 4 - 2i|$. The complex number z is represented by the point P on the Argand diagram.

a Show that the locus of P is a circle with centre $(-5, 3)$

(4 marks)

b Find the exact radius of this circle.

(1 mark)

(E/P) 4 The point P represents a complex number z in an Argand diagram.

Given that $\arg z - \arg(z + 4) = \frac{\pi}{4}$ is a locus of points P lying on an arc of a circle C ,

a sketch the locus of points P

(2 marks)

b find the coordinates of the centre of C

(3 marks)

c find the radius of C

(2 marks)

d find a Cartesian equation for the circle C

(1 mark)

e find the finite area bounded by the locus of P and the x -axis.

(3 marks)

(E/P) 5 A curve F is described by the equation $|z| = |2z + 4|$.

a Show that F is a circle, and find its centre and radius.

(5 marks)

b Sketch F on an Argand diagram.

(2 marks)

c Given that z lies on F , find the range of possible values of $\operatorname{Im}(z)$.

(3 marks)

(E/P) 6 The set of points z lie on the curve defined by $|z - 8| = 2|z - 2 - 6i|$. Find the range of possible values of $\arg(z)$.

(7 marks)

(E/P) 7 A curve S is described by the equation $\arg\left(\frac{w-8i}{w+6}\right) = \frac{\pi}{2}$, $w \in \mathbb{C}$.

a Sketch S on an Argand diagram.

(2 marks)

b Find the Cartesian equation for S .

(3 marks)

c Given that z lies on S , find the largest value of a and the smallest value of b that satisfies $a < \arg(z) < b$

d State the range of possible values of $\operatorname{Re}(z)$.

(1 mark)

- E/P** 8 The point P represents the complex number z that satisfies the equation

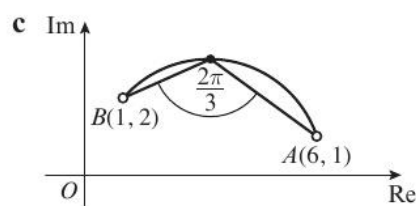
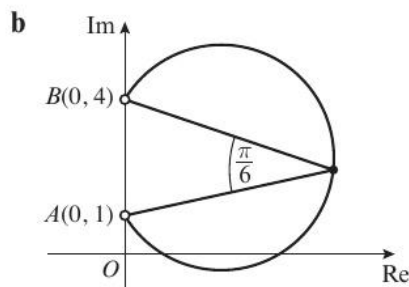
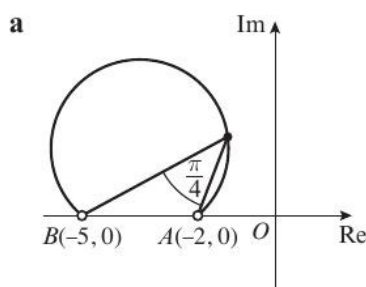
$$\arg(z - 1) - \arg(z + 3) = \frac{3\pi}{4}, z \neq -3$$

Use a geometric approach to find the Cartesian equation of the locus of P .

(5 marks)

- E/P** 9 Each of the three Argand diagrams below shows an arc of a circle drawn from point A to point B that is the locus of a set of complex numbers z . Write down an equation for each locus.

(6 marks)



- E** 10 The curve C has equation $|z + 3| = 3|z - 5|$, $z \in \mathbb{C}$.

(8 marks)

a Show that C is a circle with equation $x^2 + y^2 - 12x + 27 = 0$.

(2 marks)

b Sketch C on an Argand diagram.

(2 marks)

c The point z_1 lies on C such that $\arg(z_1) = \frac{\pi}{6}$. Express z_1 in the form $r(\cos\theta + i\sin\theta)$.

(3 marks)

- E/P** 11 In an Argand diagram, points A and B represent the numbers $6i$ and 3 respectively.

As z varies, the locus of points P satisfying the equation $|z - z_1| = k|z - z_2|$, where $z_1, z_2 \in \mathbb{C}$ and $k \in \mathbb{R}$, is the circle C such that each point P on the circle is twice the distance from point A than it is from point B .

a Write down the complex numbers z_1 and z_2 , and the value of k . **(2 marks)**

Hint $AP = 2BP$

b Show that the Cartesian equation of circle C is $x^2 + y^2 - 8x + 4y = 0$.

(2 marks)

The locus of points w satisfying the equation $\arg(w - 6) = \alpha$ where $\alpha \in \mathbb{R}$ passes through the centre of circle C and intersects it at point Q .

c Find the value of α .

(3 marks)

d Find the exact coordinates of Q .

(3 marks)

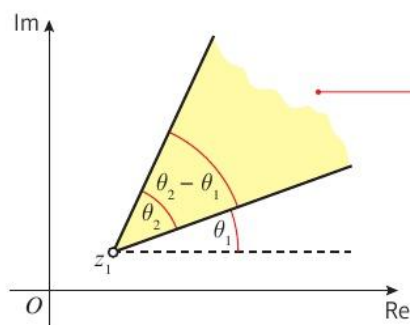
A Challenge

Fully describe the locus of points z that satisfy the equation $|z - a| + |z + a| = b$, where a and b are real constants and $b > 2a$.

3.2 Regions in an Argand diagram

You can use inequalities to represent regions in the Argand diagram.

- The inequality $\theta_1 \leq \arg(z - z_1) \leq \theta_2$ describes a region in an Argand diagram that is enclosed by the two half-lines $\arg(z - z_1) = \theta_1$ and $\arg(z - z_1) = \theta_2$, and also includes the two half-lines.

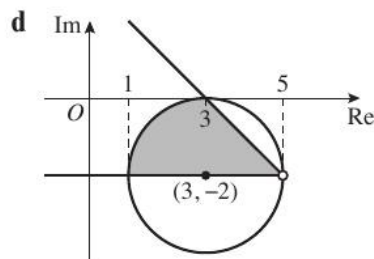
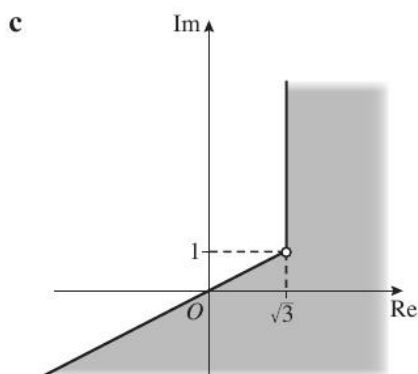
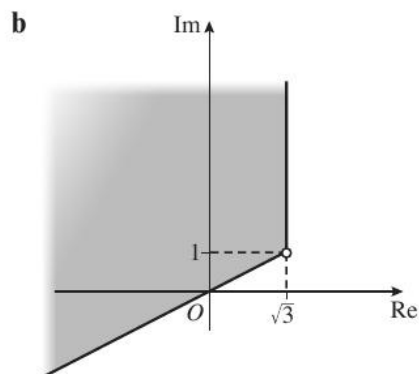
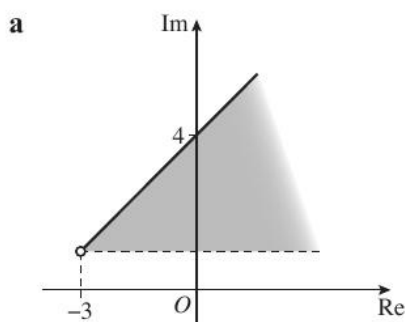


Imagine that the enclosed region in the diagram, represented by $\theta_1 \leq \arg(z - z_1) \leq \theta_2$, is formed by rotating the half-line with argument θ_1 anti-clockwise by the angle $\theta_2 - \theta_1$ about the point z_1 .

Watch out The region described by $\theta_1 < \arg(z - z_1) < \theta_2$ would not include the two half-lines. You would use dotted lines to represent them.

Example 4

Describe algebraically, in terms of z , the region shown in each Argand diagram.



- a The region is enclosed by the two half-lines $\arg(z - (-3 + i)) = 0$ and $\arg(z - (-3 + i)) = \frac{\pi}{4}$.
The region is described by the inequality $0 < \arg(z + 3 - i) \leq \frac{\pi}{4}$.
- b The region is enclosed by the two half-lines $\arg(z - (\sqrt{3} + i)) = \frac{\pi}{2}$ and $\arg(z - (\sqrt{3} + i)) = -\frac{5\pi}{6}$.
The region is described by the inequality $\frac{\pi}{2} \leq \arg(z - \sqrt{3} - i) \leq \frac{7\pi}{6}$.
- c The initial half-line is $\arg(z - \sqrt{3} - i) = -\frac{5\pi}{6}$ and the terminal half-line is $\arg(z - \sqrt{3} - i) = \frac{\pi}{2}$.
The region is described by the inequality $-\frac{5\pi}{6} \leq \arg(z - \sqrt{3} - i) \leq \frac{\pi}{2}$.
- d The shaded region in the diagram is the intersection of a circle and its interior with the region between two half-lines.
The circle and its interior is given by $|z - 3 + 2i| \leq 2$.
The equation for the initial half-line is $\arg(z - 5 + 2i) = \frac{3\pi}{4}$ and the equation for the terminal half-line is $\arg(z - 5 + 2i) = \pi$. So the region between the two half-lines is described by the inequality $\frac{3\pi}{4} \leq \arg(z - 5 + 2i) \leq \pi$.
The shaded region is given by $\{z \in \mathbb{C} : |z - 3 + 2i| \leq 2\} \cap \left\{z \in \mathbb{C} : \frac{3\pi}{4} \leq \arg(z - 5 + 2i) \leq \pi\right\}$.

The initial half-line is horizontal, so $\theta_1 = 0$.
The gradient of the terminal half-line is 1 since it extends from $(-3, 1)$ through $(0, 4)$, so $\theta_2 = \frac{\pi}{4}$.

Since the initial half-line is dashed it is not included ($<$) in the region. The terminal half-line is solid so it is included ($\leq$) in the region.

Watch out The argument θ of any complex number is usually given in the range $-\pi < \theta \leq \pi$. This is called the principal argument. However, you could also give the second half line as $\arg(z - (\sqrt{3} + i)) = \frac{7\pi}{6}$. It makes more sense to use this value in the final inequality so that the second upper value is greater than the lower value.

← CP1, Section 2.2

These are the same half lines as part b. You can consider this region as being formed by rotating the half line $\arg(z - \sqrt{3} - i) = -\frac{5\pi}{6}$ anticlockwise about the point $(\sqrt{3}, 1)$ from an angle of $-\frac{5\pi}{6}$ to an angle of $\frac{\pi}{2}$.

The set of points z satisfying the inequality $|z - z_1| \leq r$ is a circle and its interior with radius r and centre at the point representing z_1 .

The initial half-line extends from $(5, -2)$ through $(3, 0)$, so $\theta_1 = \frac{3\pi}{4}$.
The terminal half-line extends horizontally to the left, so $\theta_2 = \pi$.

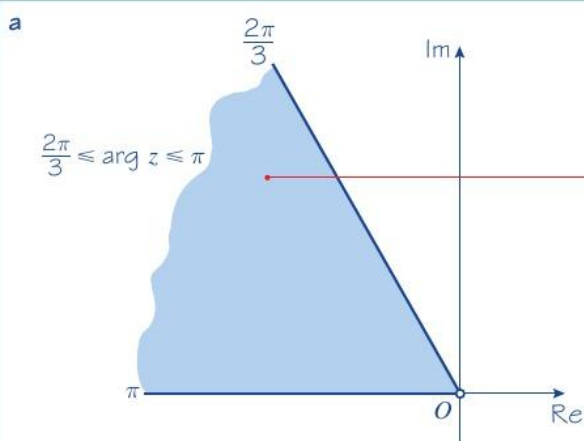
Notation Use set notation, with the symbol $\cap$ denoting the **intersection** of the two sets.

Example 5

On separate Argand diagrams, shade the region satisfied by each set of points:

a $\left\{z \in \mathbb{C} : \frac{2\pi}{3} \leq \arg z \leq \pi\right\} \cap \{z \in \mathbb{C} : |z + 3 - 4i| \leq 5\}$

b $\{z \in \mathbb{C} : 2|z - 4| \leq |z|\} \cap \{z \in \mathbb{C} : 4 \leq \operatorname{Re}(z) \leq 6\}$

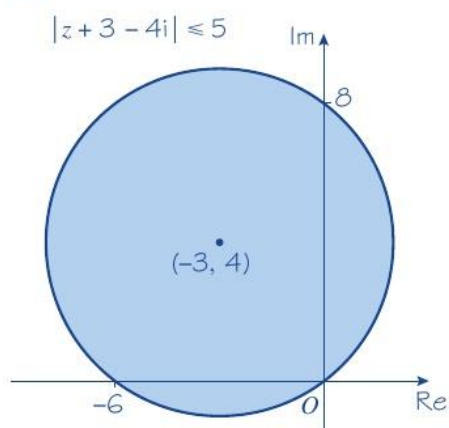


The region described by the inequality $\frac{2\pi}{3} \leq \arg z \leq \pi$ is between the two half-lines $\arg z = \frac{2\pi}{3}$ and $\arg z = \pi$.

Problem-solving

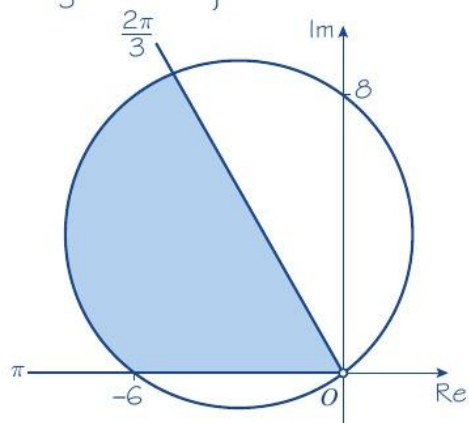
If you have to sketch a union or intersection of regions on an Argand diagram, it is helpful to sketch each region separately first

and



Therefore the intersection is

$$\left\{z \in \mathbb{C} : \frac{2\pi}{3} \leq \arg z \leq \pi\right\} \cap \{z \in \mathbb{C} : |z + 3 - 4i| \leq 5\}$$



b Let $z = x + iy$.

$$\begin{aligned} 2|x - 4 + iy| &\leq |x + iy| \\ 2\sqrt{(x - 4)^2 + y^2} &\leq \sqrt{x^2 + y^2} \\ 4(x^2 - 8x + 16 + y^2) &\leq x^2 + y^2 \\ 3x^2 + 3y^2 - 32x + 64 &\leq 0 \\ x^2 + y^2 - \frac{32}{3}x + \frac{64}{3} &\leq 0 \\ \left(x - \frac{16}{3}\right)^2 + y^2 &\leq \frac{256}{9} - \frac{64}{3} \\ \left(x - \frac{16}{3}\right)^2 + y^2 &\leq \frac{64}{9} \end{aligned}$$

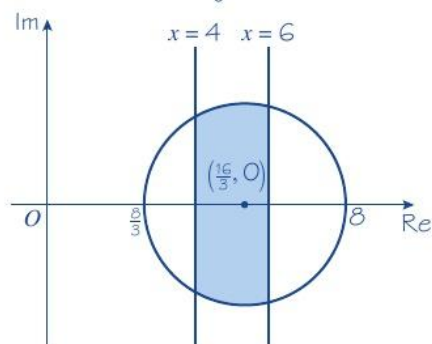
Therefore $2|z - 4| \leq |z|$ describes the region consisting of the circle with centre $(\frac{16}{3}, 0)$ and radius $\frac{8}{3}$ and its interior.

The region described by $4 \leq \operatorname{Re}(z) \leq 6$ is the region between, and including, the vertical lines $x = 4$ and $x = 6$.

So $\{z \in \mathbb{C} : 2|z - 4| \leq |z|\}$

$\cap \{z \in \mathbb{C} : 4 \leq \operatorname{Re}(z) \leq 6\}$

describes the region shaded below.



Problem-solving

The equation $2|z - 4| = |z|$ represents a circle, so the inequality $2|z - 4| \leq |z|$ represents a region consisting of either a circle and its interior, or a circle and the region outside it. You need to use an algebraic approach to find the centre and radius of the circle.

Complete the square.

The locus of points satisfying the equation $\operatorname{Re}(z) = 4$ is the vertical line $x = 4$, and the locus of points satisfying the equation $\operatorname{Re}(z) = 6$ is the vertical line $x = 6$.

Exercise 3B

1 On separate Argand diagrams, shade the regions, R , described by:

a $0 \leq \arg(z - 4 - i) \leq \frac{\pi}{2}$

b $-1 \leq \operatorname{Im}(z) \leq 2$

c $\frac{1}{2} \leq |z| < 1$

d $-\frac{\pi}{3} \leq \arg(z + i) \leq \frac{\pi}{4}$

2 The region R in an Argand diagram is satisfied by the inequalities $|z| \leq 5$ and $|z| \leq |z - 6i|$. Draw an Argand diagram and shade in the region R .

3 Shade on an Argand diagram the region satisfied by the set of points $P(x, y)$, where $|z + 1 - i| \leq 1$ and $0 \leq \arg z < \frac{3\pi}{4}$.

4 Shade on an Argand diagram the region, R , satisfied by the set of points $P(x, y)$, where $|z| < 3$ and $\frac{\pi}{4} \leq \arg(z + 3) \leq \pi$.

5 a Sketch on the same Argand diagram:

- i the locus of points representing $|z - 2| = |z - 6 - 8i|$
- ii the locus of points representing $\arg(z - 4 - 2i) = 0$
- iii the locus of points representing $\arg(z - 4 - 2i) = \frac{\pi}{2}$

The region R is defined by the inequalities $|z - 2| \leq |z - 6 - 8i|$ and $0 \leq \arg(z - 4 - 2i) \leq \frac{\pi}{2}$

b On your sketch from part a, identify, by shading, the region R .

(E) 6 On separate Argand diagrams, shade the regions, R , defined by the sets of points:

a $\left\{z \in \mathbb{C} : -\frac{\pi}{2} \leq \arg(z + 1 + i) \leq -\frac{\pi}{4}\right\} \cap \{z \in \mathbb{C} : |z + 1 + 2i| \leq 1\}$ (4 marks)

b $\{z \in \mathbb{C} : 2|z - 6| \leq |z - 3|\} \cap \{z \in \mathbb{C} : \operatorname{Re}(z) \leq 7\}$ (4 marks)

(E/P) 7 a Shade on an Argand diagram the region defined by $|z + 6| \leq 3$. (2 marks)

b The complex number z satisfies $|z + 6| \leq 3$. Find the range of possible values of $\arg z$. (4 marks)

(E/P) 8 a Indicate on an Argand diagram the region consisting of the set of points satisfying both $\frac{3\pi}{4} \leq \arg(z - 8) \leq \pi$ and $\operatorname{Im}(z) \leq \operatorname{Re}(z)$. (3 marks)

b Find the exact area of this region. (3 marks)

(E/P) 9 a Shade on an Argand diagram the region R defined by

$$\{z : |z - 3 + 2i| \geq \sqrt{2}|z - 1|\} \cap \left\{z : 0 \leq \arg(z + 1 + 2i) \leq \frac{\pi}{3}\right\}$$
 (4 marks)

b Find the exact area of region R . (3 marks)

c The complex number z lies in region R . Find the maximum value of $\operatorname{Im}(z)$. (5 marks)

Challenge

5 On an Argand diagram, shade the set of points

$$\{z \in \mathbb{C} : 6 \leq \operatorname{Re}((2 - 3i)z) < 12\} \cap \{z \in \mathbb{C} : (\operatorname{Re} z)(\operatorname{Im} z) \geq 0\}$$

3.3 Transformations of the Complex Plane

A You need to be able to transform simple loci, such as lines and circles, from one complex plane (the z -plane) to another complex plane (the w -plane). Transformations will map points in the z -plane to points in the w -plane by applying a formula relating $z = x + iy$ to $w = u + iv$.

Notation The convention is to use u for the real part and v for the imaginary part of a complex number in the w -plane.

It is helpful to be able to recognise the type of transformation – translation, enlargement, or rotation – from the formula for some simple transformations.

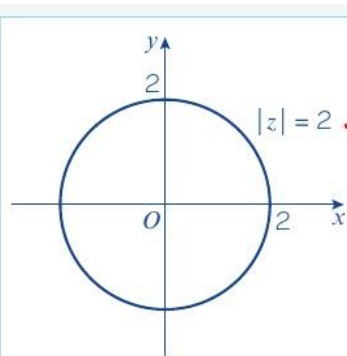
Example 6

A The point P represents the complex number z on an Argand diagram, where $|z| = 2$. T_1 , T_2 and T_3 represent transformations from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$. Describe the locus of the image of P under the transformations:

a $T_1: w = z - 2 + 4i$

b $T_2: w = 3z$

c $T_3: w = \frac{1}{2}z + i$



The locus of P in the z -plane is a circle with centre $(0, 0)$ and radius 2.

This is the locus of P in the z -plane before any transformations have been applied.

a $T_1: w = z - 2 + 4i$

$\Rightarrow w + 2 - 4i = z$

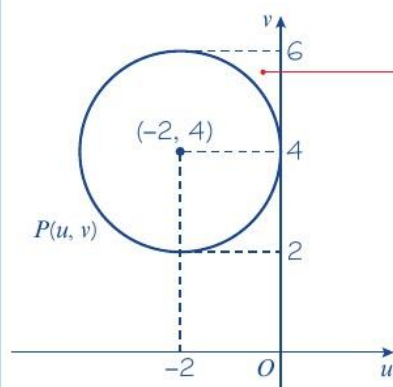
$\Rightarrow |w + 2 - 4i| = |z|$

$\Rightarrow |w + 2 - 4i| = 2$

Rearrange to make z the subject.

Apply the modulus to both sides of the equation.

Use $|z| = 2$.



The image of the locus of P under T_1 is $|w + 2 - 4i| = 2$. This is a circle with centre $(-2, 4)$ and radius 2.

Problem-solving

The transformation $T_1: w = z - 2 + 4i$ represents a **translation** of z by the vector $\begin{pmatrix} -2 \\ 4 \end{pmatrix}$.

Apply the modulus to both sides of the equation.

Use $|z_1 z_2| = |z_1| |z_2|$.

Use $|z| = 2$.

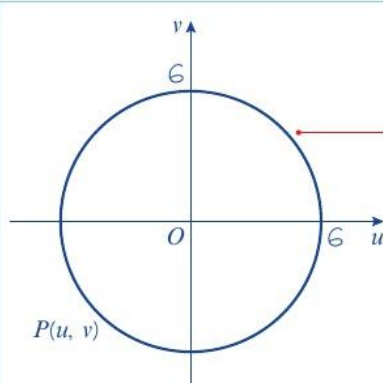
b $T_2: w = 3z$

$\Rightarrow |w| = |3z|$

$\Rightarrow |w| = 3|z|$

$\Rightarrow |w| = 3(2) = 6$

A



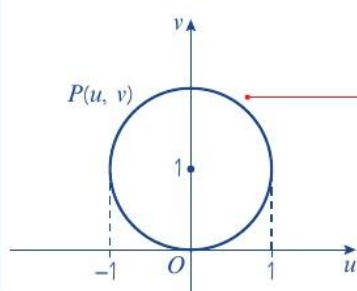
$$c \quad T_3: w = \frac{1}{2}z + i$$

$$\Rightarrow w - i = \frac{1}{2}z$$

$$\Rightarrow |w - i| = \left| \frac{1}{2}z \right|$$

$$\Rightarrow |w - i| = \left| \frac{1}{2} \right| |z|$$

$$\Rightarrow |w - i| = \frac{1}{2}(2) = 1$$



The image of the locus of P under T_2 is $|w| = 6$. This is a circle with centre $(0, 0)$ and radius 6.

Problem-solving

The transformation $T_2: w = 3z$ represents an **enlargement** of z by scale factor 3 with centre $(0, 0)$.

Rearrange to make $\frac{1}{2}z$ the subject.

Apply the modulus to both sides of the equation.

Use $|z_1 z_2| = |z_1| |z_2|$.

Use $|z| = 2$.

The image of the locus of P under T_3 is $|w - i| = 1$. This is a circle with centre $(0, 1)$ and radius 1.

Problem-solving

The transformation $T_3: w = \frac{1}{2}z + i$ represents an enlargement of z by scale factor $\frac{1}{2}$ about the point $(0, 0)$, followed by a translation by the vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Example 7

For the transformation $w = iz - 1$, find the locus of w when z lies on the half-line $\arg(z + 2) = \frac{\pi}{4}$

$$w = iz - 1$$

$$\Rightarrow iz = w + 1$$

$$\Rightarrow z = \frac{w}{i} + \frac{1}{i}$$

$$\Rightarrow z = -iw - i$$

$$\arg(z + 2) = \frac{\pi}{4}$$

$$\Rightarrow \arg(-iw - i + 2) = \frac{\pi}{4}$$

$$\Rightarrow \arg(-iw + 2 - i) = \frac{\pi}{4}$$

$$\Rightarrow \arg(-i(w + 2i + 1)) = \frac{\pi}{4}$$

$$\Rightarrow \arg(-i) + \arg(w + 1 + 2i) = \frac{\pi}{4}$$

$$\Rightarrow -\frac{\pi}{2} + \arg(w + 1 + 2i) = \frac{\pi}{4}$$

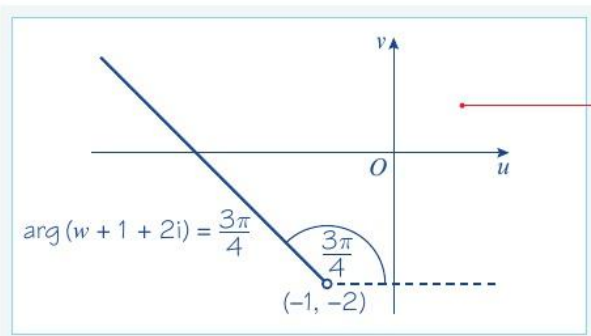
$$\Rightarrow \arg(w + 1 + 2i) = \frac{3\pi}{4}$$

Rearrange the transformation formula $w = iz - 1$ to make z the subject.

Substitute $-iw - i$ for z .

Use $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$

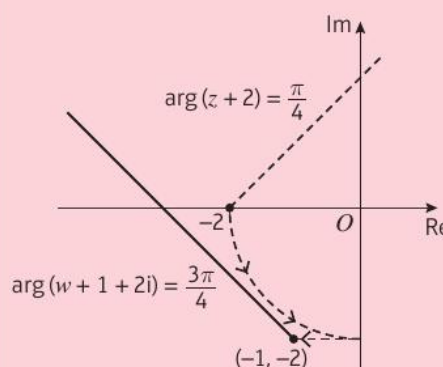
A



The locus of points in the w -plane is the half-line, $\arg(w + 1 + 2i) = \frac{3\pi}{4}$, that extends from the point $(-1, -2)$ at an angle of $\frac{3\pi}{4}$ to the horizontal extending to the right of $(-1, -2)$.

Problem-solving

The transformation $w = iz - 1$ represents an anticlockwise rotation through $\frac{\pi}{2}$ about the origin followed by a translation by the vector $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$.



Examples 6 and 7 lead to the following general results:

- $w = z + a + ib$ represents a translation by the vector $\begin{pmatrix} a \\ b \end{pmatrix}$, where $a, b \in \mathbb{R}$.
- $w = kz$, where $k \in \mathbb{R}$, represents an enlargement by scale factor k with centre $(0, 0)$, where $k \in \mathbb{R}$.
- $w = iz$ represents an anticlockwise rotation through $\frac{\pi}{2}$ about the origin.

Compound transformations, such as the one in Example 7, are represented by transformation formulae which combine more than one of the characteristics listed above. For example, the transformation formula $w = kz + a + ib$ represents an enlargement by scale factor k with centre $(0, 0)$ followed by a translation by the vector $\begin{pmatrix} a \\ b \end{pmatrix}$, where $a, b, k \in \mathbb{R}$.

Example 8

A transformation from the z -plane to the w -plane is given by $w = z^2$, where $z = x + iy$ and $w = u + iv$. Describe the locus of w and give its Cartesian equation when z lies on:

- a circle with equation $x^2 + y^2 = 16$
- the line with equation $x = 1$

Notation

A Cartesian equation for a locus in the z -plane will be in terms of x and y because $z = x + iy$. However, a Cartesian equation for a locus in the w -plane will be in terms of u and v because $w = u + iv$.

A

a $|z| = 4$

$$w = z^2 \Rightarrow |w| = |z^2|$$

$$\Rightarrow |w| = |z| |z|$$

$$\Rightarrow |w| = 4 \times 4$$

$$\Rightarrow |w| = 16$$

Hence the locus of w is a circle with centre $(0, 0)$ and radius 16, and the Cartesian equation for the locus of w is $u^2 + v^2 = 16^2 = 256$

b Let $z = 1 + iy$

$$w = z^2 \Rightarrow w = (1 + iy)^2$$

$$\Rightarrow w = (1 - y^2) + 2yi$$

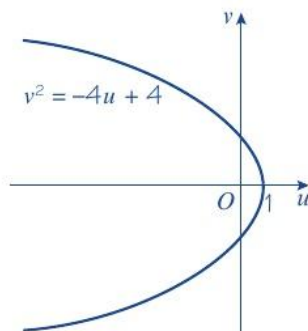
$$\text{So } u = 1 - y^2 \text{ and } v = 2y$$

$$-4u = -4 + 4y^2 \text{ and } v^2 = 4y^2$$

The Cartesian equation for w is

$$v^2 = -4u + 4$$

The locus of w is a parabola that is symmetric about the real axis, with vertex at $(1, 0)$, as shown in the diagram.



This has Cartesian equation $x^2 + y^2 = 16$.

Take the modulus of each side of the equation.

Use $|z_1 z_2| = |z_1| |z_2|$, where $z_1 = z_2 = z$.

Use $|z| = 4$.

The line $x = 1$ in the z -plane is the locus of $\operatorname{Re}(z) = 1$.

This is a parametric equation of a curve in the w -plane with y as the parameter.

Problem-solving

A Cartesian equation in the w -plane should be in terms of u and v . You need to eliminate y from the equations.

- You need to be able to apply transformation formulae of the form $w = \frac{az + b}{cz + d}$, where $a, b, c, d \in \mathbb{C}$, that map points in the z -plane to points in the w -plane.

Note Transformations of this form are called **Möbius transformations**.

Example 9

The transformation T from the z -plane, where $z = x + iy$, to the w -plane, where $w = u + iv$, is given by $w = \frac{5iz + i}{z + 1}$, $z \neq -1$.

- Show that the image, under T , of the circle $|z| = 1$ in the z -plane is a line l in the w -plane.
- Sketch l on an Argand diagram.

A

$$a \quad w = \frac{5iz + i}{z + 1}$$

$$\Rightarrow w(z + 1) = 5iz + i$$

$$\Rightarrow wz + w = 5iz + i$$

$$\Rightarrow wz - 5iz = i - w$$

$$\Rightarrow z(w - 5i) = i - w$$

$$\Rightarrow z = \frac{i - w}{w - 5i}$$

$$\text{So } |z| = \left| \frac{i - w}{w - 5i} \right|$$

$$\Rightarrow 1 = \frac{|i - w|}{|w - 5i|}$$

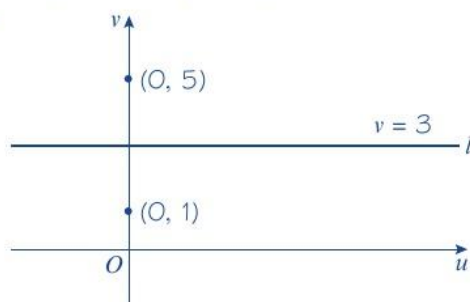
$$\Rightarrow |w - 5i| = |i - w|$$

$$\Rightarrow |w - 5i| = |(-1)(w - i)|$$

$$\Rightarrow |w - 5i| = |-1| |w - i|$$

$$\Rightarrow |w - 5i| = |w - i|$$

b



Therefore the image of $|z| = 1$, under T , is the line l with equation $v = 3$.

Rearrange the transformation equation to make z the subject of the equation.

Take the modulus of each side of the equation.

Use $|z| = 1$ and $\left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|}$

Take out a factor of -1 on the RHS.

Use $|z_1 z_2| = |z_1| |z_2|$.

As you are working in the w -plane, plot v against u . $|w - 5i| = |w - i|$ is in the form $|w - w_1| = |w - w_2|$ so represents points on the perpendicular bisector of the line segment joining $(0, 1)$ and $(0, 5)$. Therefore the line l has equation $v = 3$.

Example 10

The transformation T from the z -plane, where $z = x + iy$, to the w -plane, where $w = u + iv$, is given by $w = \frac{3z - 2}{z + 1}$, $z \neq -1$.

Show that the image, under T , of the circle with equation $x^2 + y^2 = 4$ in the z -plane is a circle C in the w -plane. State the centre and radius of C .

$$w = \frac{3z - 2}{z + 1}$$

$$\Rightarrow w(z + 1) = 3z - 2$$

$$\Rightarrow wz + w = 3z - 2$$

$$\Rightarrow w + 2 = 3z - wz$$

$$\Rightarrow w + 2 = z(3 - w)$$

$$\Rightarrow \frac{w + 2}{3 - w} = z$$

Rearrange the transformation equation $w = \frac{3z - 2}{z + 1}$ to make z the subject of the equation.

A

$x^2 + y^2 = 4$ can also be written as $|z| = 2$.

$$\left| \frac{w+2}{3-w} \right| = |z| = 2$$

$$\Rightarrow \frac{|w+2|}{|3-w|} = 2$$

$$\Rightarrow |w+2| = 2|3-w|$$

$$\Rightarrow |w+2| = 2|-1||w-3|$$

$$\Rightarrow |w+2| = 2|w-3|$$

$$\Rightarrow |u+iv+2| = 2|u+iv-3|$$

$$\Rightarrow |(u+2)+iv| = 2|(u-3)+iv|$$

$$\Rightarrow |(u+2)+iv|^2 = 2^2|(u-3)+iv|^2$$

$$\Rightarrow (u+2)^2 + v^2 = 4((u-3)^2 + v^2)$$

$$\Rightarrow u^2 + 4u + 4 + v^2 = 4(u^2 - 6u + 9 + v^2)$$

$$\Rightarrow u^2 + 4u + 4 + v^2 = 4u^2 - 24u + 36 + 4v^2$$

$$\Rightarrow 3u^2 - 28u + 3v^2 + 32 = 0$$

$$\Rightarrow u^2 - \frac{28}{3}u + v^2 + \frac{32}{3} = 0$$

$$\Rightarrow \left(u - \frac{14}{3}\right)^2 - \frac{196}{9} + v^2 + \frac{32}{3} = 0$$

$$\Rightarrow \left(u - \frac{14}{3}\right)^2 + v^2 = \frac{100}{9}$$

Therefore the image of $x^2 + y^2 = 4$, under T , is a circle C with centre $\left(\frac{14}{3}, 0\right)$ and radius $\frac{10}{3}$.

$x^2 + y^2 = 4$ is the equation of a circle with centre $(0, 0)$ and radius 2.

Take the modulus of each side of the equation.

Use $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$ and $|z| = 2$.

Write w as $u + iv$.

Group the real and imaginary parts.

Square both sides.

Remove the moduli.

Complete the square for u .

Example 11

A transformation T of the z -plane to the w -plane is given by $w = \frac{iz - 2}{1 - z}$, $z \neq 1$.

Show that as z lies on the real axis in the z -plane, then w lies on a line l in the w -plane.

Sketch l on an Argand diagram.

$$w = \frac{iz - 2}{1 - z}$$

$$\Rightarrow w(1 - z) = iz - 2$$

$$\Rightarrow w - wz = iz - 2$$

$$\Rightarrow w + 2 = wz + iz$$

$$\Rightarrow w + 2 = z(w + i)$$

$$\Rightarrow \frac{w+2}{w+i} = z$$

$$\text{So } z = \frac{u+iv+2}{u+iv+i}$$

$$\Rightarrow z = \frac{(u+2)+iv}{u+i(v+1)}$$

$$\Rightarrow z = \frac{(u+2)+iv}{u+i(v+1)} \times \frac{u-i(v+1)}{u-i(v+1)}$$

$$\Rightarrow z = \frac{u(u+2) - i(u+2)(v+1) + iuv + v(v+1)}{u^2 + (v+1)^2}$$

Rearrange the transformation equation $w = \frac{iz - 2}{1 - z}$ to make z the subject of the equation.

Write w as $u + iv$.

Group the real and imaginary parts.

Multiply the numerator and denominator by the complex conjugate of $u + i(v + 1)$.

Use the difference of two squares.

A

$$\Rightarrow z = \frac{u(u+2) + v(v+1)}{u^2 + (v+1)^2} + i \left(\frac{uv - (u+2)(v+1)}{u^2 + (v+1)^2} \right)$$

$$\text{So } x + iy = \frac{u(u+2) + v(v+1)}{u^2 + (v+1)^2} + i \left(\frac{uv - (u+2)(v+1)}{u^2 + (v+1)^2} \right)$$

Since z lies on the real axis, $y = 0$.

$$\text{So } x + 0i = \frac{u(u+2) + v(v+1)}{u^2 + (v+1)^2} + i \left(\frac{uv - (u+2)(v+1)}{u^2 + (v+1)^2} \right)$$

$$\text{Hence, } 0 = \frac{uv - (u+2)(v+1)}{u^2 + (v+1)^2}$$

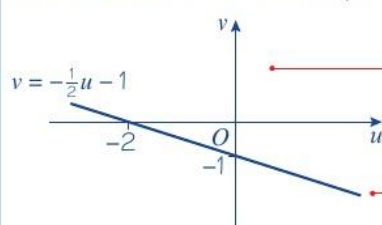
$$\Rightarrow uv - (u+2)(v+1) = 0$$

$$\Rightarrow uv - (uv + u + 2v + 2) = 0$$

$$\Rightarrow uv - uv - u - 2v - 2 = 0$$

$$\Rightarrow 2v = -u - 2$$

So w lies on the line with equation $v = -\frac{1}{2}u - 1$.



Group the real and imaginary parts.

Write z as $x + iy$.

Equate the imaginary parts.

Multiply both sides by $u^2 + (v+1)^2$.

Rearrange to make v the subject.

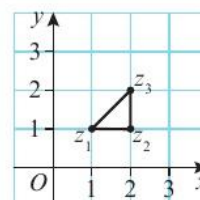
As you are working in the w -plane, plot v against u .

The line l has equation $v = -\frac{1}{2}u - 1$ and cuts the coordinate axes at $(-2, 0)$ and $(0, -1)$.

Exercise 3C

- 1 Consider the triangle shown on the right in the z -plane. For each of the transformation formulae:

- sketch the image of the triangle by plotting the images of z_1 , z_2 and z_3 , in the w -plane
- give a geometrical description of the mapping from the z -plane to the w -plane.



- a $w = z - 3 + 2i$ b $w = 2z$ c $w = iz - 2 + i$ d $w = 3z - 2i$
- 2 A transformation T from the z -plane to the w -plane is a translation by the vector $\begin{pmatrix} -2 \\ 3 \end{pmatrix}$ followed by an enlargement with scale factor 4 and centre O . Write down the transformation T in the form $w = az + b$, where $a, b \in \mathbb{C}$.
- 3 Determine the formula for a transformation from the z -plane to the w -plane in such a way that the locus of w points is the image of the locus of z points rotated 90° anticlockwise and enlarged by a scale factor of 4, both about the point $(0, 0)$.
- 4 For the transformation $w = 2z - 5 + 3i$, find the Cartesian equation of the locus of w as z moves on the circle $|z - 2| = 4$.
- 5 For the transformation $w = z - 1 + 2i$, sketch on separate Argand diagrams the locus of w when z lies on:
- the circle $|z - 1| = 3$
 - the half-line $\arg(z - 1 + i) = \frac{\pi}{4}$
 - the line $y = 2x$

- A** 6 For the transformation $w = \frac{1}{z}$, $z \neq 0$, describe the locus of w when z lies on:
a the circle $|z| = 2$ **b** the half-line with equation $\arg z = \frac{\pi}{4}$
c the line with equation $y = 2x + 1$
- E** 7 For the transformation $w = z^2$,
a show that as z moves once round a circle with centre $(0, 0)$ and radius 3, w moves twice round a circle with centre $(0, 0)$ and radius 9 (6 marks)
b find the locus of w when z lies on the real axis (2 marks)
c find the locus of w when z lies on the imaginary axis. (2 marks)
- E** 8 The transformation T from the z -plane to the w -plane is given by $w = \frac{2}{i - 2z}$, $z \neq \frac{i}{2}$.
 The circle with equation $|z| = 1$ is mapped by T onto the curve C .
a i Show that C is a circle.
ii Find the centre and radius of C . (8 marks)
 The region $|z| \leq 1$ in the z -plane is mapped by T onto the region R in the w -plane.
b Shade the region R on an Argand diagram. (2 marks)
- E/P** 9 For the transformation $w = \frac{1}{2 - z}$, $z \neq 2$, show that the image, under T , of the circle centre O , radius 2 in the z -plane is a line l in the w -plane. Sketch l on an Argand diagram. (6 marks)
- E** 10 A transformation from the z -plane to the w -plane is given by $w = \frac{z - i}{z + i}$, $z \neq -i$.
a Show that the circle with equation $|z - i| = 1$ in the z -plane is mapped to a circle in the w -plane, giving an equation for this circle. (5 marks)
b Sketch the new circle on an Argand diagram. (1 mark)
- E/P** 11 The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = \frac{3}{2 - z}$, $z \neq 2$.
 Show that, under T , the straight line with equation $2y = x$ is transformed to a circle in the w -plane with centre $(\frac{3}{4}, \frac{3}{2})$ and radius $\frac{3\sqrt{5}}{4}$ (7 marks)
- E/P** 12 The transformation T from the z -plane, where $z = x + iy$, to the w -plane, where $w = u + iv$, is given by $w = \frac{-iz + i}{z + 1}$, $z \neq -1$.
a The transformation T maps the points on the circle with equation $x^2 + y^2 = 1$ in the z -plane, to points on a line l in the w -plane. Find the Cartesian equation of l . (4 marks)
b Hence, or otherwise, shade and label on an Argand diagram the region R of the w -plane which is the image of $|z| \leq 1$ under T . (2 marks)
c Show that the image, under T , of the circle with equation $x^2 + y^2 = 4$ in the z -plane is a circle C in the w -plane. Find the equation of C . (4 marks)
- E** 13 The transformation T from the z -plane, where $z = x + iy$, to the w -plane, where $w = u + iv$, is given by $w = \frac{4z - 3i}{z - 1}$, $z \neq 1$.
 Show that the circle $|z| = 3$ is mapped by T onto a circle C , and state the centre and radius of C . (6 marks)

- A** 14 The transformation T from the z -plane, where $z = x + iy$, to the w -plane, where $w = u + iv$, is given by $w = \frac{1}{z+i}$, $z \neq -i$.
- E**
- a** Show that the image, under T , of the real axis in the z -plane is a circle C_1 in the w -plane and find the equation of C_1 . (5 marks)
- b** Show that the image, under T , of the line $x = 4$ in the z -plane is a circle C_2 in the w -plane, and find the equation of C_2 . (5 marks)
- E/P** 15 The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = z + \frac{4}{z}$, $z \neq 0$.
Show that the transformation T maps the points on a circle $|z| = 2$ to points in the interval $[-k, k]$ on the real axis. State the value of the constant k . (7 marks)
- E/P** 16 The transformation T from the z -plane, where $z = x + iy$, to the w -plane, where $w = u + iv$, is given by $w = \frac{1}{z+3}$, $z \neq -3$.
Show that T maps the line with equation $2x - 2y + 7 = 0$ onto a circle C , and state the centre and the exact radius of C . (6 marks)

Challenge

A transformation $T: w = az + b$, $a, b \in \mathbb{C}$ maps the complex numbers 0 , 1 and $1 + i$ in the z -plane to the points $2i$, $3i$ and $-1 + 3i$, respectively, in the w -plane. Find a and b .

Mixed exercise 3

- 1 For each of the following equations:
- i** use an algebraic approach to determine a Cartesian equation for the locus of z on an Argand diagram
- ii** describe the locus geometrically.
- a** $|z| = |z - 4|$
- b** $|z| = 2|z - 4|$
- E/P** 2 **a** Sketch the locus of points that satisfies the equation $|z - 2 + i| = \sqrt{3}$. (3 marks)
The half-line L with equation $y = mx - 1$, $x \geq 0$, $m > 0$ is tangent to the locus from part **a** at point A .
- b** Find the value of m . (3 marks)
- c** Write an equation for L in the form $\arg(z - z_1) = \theta$, $z_1 \in \mathbb{C}$, $-\pi < \theta \leq \pi$. (2 marks)
- d** Find the complex number a represented by point A . (3 marks)
- E** 3 **a** Find the Cartesian equation of the locus of points representing $|z + 2| = |2z - 1|$. (3 marks)
- b** Find the value of z which satisfies both $|z + 2| = |2z - 1|$ and $\arg z = \frac{\pi}{4}$. (3 marks)
- c** Hence shade in the region R on an Argand diagram which satisfies both $|z + 2| \geq |2z - 1|$ and $\frac{\pi}{4} \leq \arg z \leq \pi$. (2 marks)

- E** 4 Given that $\arg\left(\frac{z-4-2i}{z-6i}\right) = \frac{\pi}{2}$,
 a sketch the locus of $P(x, y)$ which represents z on an Argand diagram (4 marks)
 b deduce the exact value of $|z-2-4i|$. (2 marks)
- E/P** 5 A curve has equation $2|z+3| = |z-3|$, where $z \in \mathbb{C}$.
 a Show that the curve is a circle with equation $x^2 + y^2 + 10x + 9 = 0$. (2 marks)
 b Sketch the curve on an Argand diagram. (2 marks)
 The line L has equation $bz^* + b^*z = 0$, where $b \in \mathbb{C}$ and $z \in \mathbb{C}$.
 c Given that the line L is a tangent to the curve and that $\arg b = \theta$, find the possible values of $\tan \theta$. (5 marks)
- E/P** 6 A curve S is described by the equation $\arg\left(\frac{z-5-2i}{z-1-6i}\right) = \frac{\pi}{2}$
 a Show that S is a semicircle, and find its centre and radius. (5 marks)
 b Find the maximum value of $|z|$, and express it exactly. (4 marks)
- E** 7 a Indicate on an Argand diagram the region, R , consisting of the set of points satisfying the inequality $2 \leq |z-2-3i| \leq 3$. (3 marks)
 b Find the exact area of region R . (2 marks)
 c Determine whether or not the point represented by $4+i$ lies inside R . (3 marks)
- A** 8 The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = \frac{1}{z}$, $z \neq 0$.
 a Show that the image, under T , of the line with equation $x = \frac{1}{2}$ in the z -plane is a circle C in the w -plane. Find the equation of C . (4 marks)
 b Hence, or otherwise, shade and label on an Argand diagram the region R of the w -plane with is the image of $x \geq \frac{1}{2}$ under T . (3 marks)
- E** 9 The point P represents the complex number z on an Argand diagram.
 Given that $|z+4i| = 2$,
 a sketch the locus of P on an Argand diagram. (2 marks)
 b Hence find the maximum value of $|z|$. (3 marks)
 T_1, T_2, T_3 and T_4 represent transformations from the z -plane to the w -plane.
 Describe the locus of the image of P under the transformations:
 c i $T_1: w = 2z$ (2 marks)
 ii $T_2: w = iz$ (2 marks)
 iii $T_3: w = -iz$ (2 marks)
 iv $T_4: w = z^*$ (2 marks)
- E** 10 The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = \frac{z+2}{z+i}$, $z \neq -i$.
 a Show that the image, under T , of the imaginary axis in the z -plane is a line l in the w -plane. Find the equation of l . (4 marks)
 b Show that the image, under T , of the line $y = x$ in the z -plane is a circle C in the w -plane. Find the centre of C and show that the radius of C is $\frac{\sqrt{10}}{2}$. (5 marks)

- A** **11** The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = \frac{4-z}{z+i}$, $z \neq -i$.
E/P The circle $|z| = 1$ is mapped by T onto a line l . Show that l can be written in the form $au + bv + c = 0$, where a , b and c are integers to be determined. **(5 marks)**
- E/P** **12** The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = \frac{3iz + 6}{1 - z}$, $z \neq 1$.
 Show that the circle $|z| = 2$ is mapped by T onto a circle C . State the centre of C and show that the radius of C can be expressed in the form $k\sqrt{5}$ where k is an integer to be determined. **(5 marks)**
- E/P** **13** The mapping from the z -plane to the w -plane given by $w_2 = \frac{az_1 + b}{z_1 + c}$, $z_1, z_2 \in \mathbb{C}$, $a, b, c \in \mathbb{R}$ maps the origin onto itself, and reflects the point $1 + 2i$ in the real axis.
a Find the values of a , b and c .
 A second complex number ω is also mapped to itself.
b Find ω .
- E/P** **14** A transformation from the z -plane to the w -plane is defined by $w = \frac{az + b}{z + c}$, where $a, b, c \in \mathbb{R}$.
 Given that $w = 1$ when $z = 0$ and that $w = 3 - 2i$ when $z = 2 + 3i$,
a find the values of a , b and c **(5 marks)**
b find the exact values of the two points in the complex plane which remain invariant under the transformation. **(5 marks)**
- 15** The transformation T from the z -plane, where $z = x + iy$, to the w -plane where $w = u + iv$, is given by $w = \frac{z+i}{z}$, $z \neq 0$.
a The transformation T maps the points on the line with equation $y = x$ in the z -plane, other than $(0, 0)$, to points on the line l in the w -plane. Find an equation of l . **(4 marks)**
b Show that the image, under T , of the line with equation $x + y + 1 = 0$ in the z -plane is a circle in the w -plane, where C has equation $u^2 + v^2 - u - v = 0$. **(4 marks)**
c On the same Argand diagram, sketch l and C . **(3 marks)**

Challenge

The complex function f maps any point in an Argand diagram represented by $z = x + iy$ to its reflection in the line $x + y = 1$. Express f in the form $f(z) = az^* + b$, where $a, b \in \mathbb{C}$.

Summary of key points

- 1 Given $z_1 = x_1 + iy_1$, the locus of points z on an Argand diagram such that $|z - z_1| = r$, or $|z - (x_1 + iy_1)| = r$, is a circle with centre (x_1, y_1) and radius r .
- 2 Given $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, the locus of points z on an Argand diagram such that $|z - z_1| = |z - z_2|$ is the perpendicular bisector of the line segment joining z_1 and z_2 .
- 3 The locus of points z that satisfy $|z - a| = k|z - b|$, where $a, b \in \mathbb{C}$ and $k \in \mathbb{R}, k > 0, k \neq 1$ is a circle.
- 4 Given $z_1 = x_1 + iy_1$, the locus of points z on an Argand diagram such that $\arg(z - z_1) = \theta$ is a half-line from, but not including, the fixed point z_1 making an angle θ with a line from the fixed point z_1 parallel to the real axis.
- 5 The locus of points z that satisfy $\arg\left(\frac{z - a}{z - b}\right) = \theta$, where $\theta \in \mathbb{R}, \theta > 0$ and $a, b \in \mathbb{C}$, is an arc of a circle with endpoints A and B representing the complex numbers a and b , respectively.
 - If $\theta < \frac{\pi}{2}$, then the locus is a major arc of the circle.
 - If $\theta > \frac{\pi}{2}$, then the locus is a minor arc of the circle.
 - If $\theta = \frac{\pi}{2}$, then the locus is a semicircle.
- 6 The inequality $\theta_1 \leq \arg(z - z_1) \leq \theta_2$ describes a region in an Argand diagram that is enclosed by the two half-lines $\arg(z - z_1) = \theta_1$ and $\arg(z - z_1) = \theta_2$, and also includes the two half-lines.
- 7 • $w = z + a + ib$ represents a translation by the vector $\begin{pmatrix} a \\ b \end{pmatrix}$, where $a, b \in \mathbb{R}$.
 • $w = kz$, where $k \in \mathbb{R}$, represents an enlargement by scale factor k with centre $(0, 0)$, where $k \in \mathbb{R}$.
 • $w = iz$ represents an anticlockwise rotation through $\frac{\pi}{2}$ about the origin.
- 8 You need to be able to apply transformation formulae of the form $w = \frac{az + b}{cz + d}$, where $a, b, c, d \in \mathbb{C}$, that map points in the z -plane to points in the w -plane.

A

4

Recurrence relations

Objectives

After completing this chapter you should be able to:

- Use recurrence relations to describe sequences and model situations → pages 000–000
- Find solutions to first-order recurrence relations → pages 000–000
- Find solutions to second-order recurrence relations → pages 000–000
- Use mathematical induction to prove closed forms for recurrence relations → pages 000–000

Prior knowledge check

- 1** A sequence of numbers is defined by the recurrence relation

$$u_{k+1} = 3u_k, \text{ with } u_0 = 2$$

- a** Write down the first five terms of the sequence.
b Find an expression for u_n in terms of n .

← Pure Year 2, Chapter 3

- 2** A sequence of numbers is defined for all $n \in \mathbb{N}$ by
 $u_{n+1} = au_n + b$, with $u_1 = 3$

Given that $u_2 = 5$ and $u_3 = 9$, find the values of a and b .

← Pure Year 2, Chapter 3

- 3** Prove by induction that for all positive integers n , $\sum_{r=1}^n (2r - 1) = n^2$

← Core Pure Book 1, Chapter 8

In population modelling, the final population for one year becomes the starting population for the next year. You can model the population at the end of each year as a sequence and describe it using a recurrence relation. → Exercise 4B Q8

4.1 Forming recurrence relations

You can model many real-life situations using recurrence relations.

For example, suppose that you have £500 in a savings account that pays 0.5% interest every month. Each month, you add another £100 to the savings account.

You can use this information to formulate a recurrence relation that describes the amount in the account at the end of each month.

Let u_m be the amount in pounds in the account after m months. The next month, $m + 1$, you will have the original amount, u_m , plus the interest, $0.005u_m$, plus the additional £100 you add every month. This generates the recurrence relation

$$u_{m+1} = u_m + 0.005u_m + 100, \text{ with } u_0 = 500$$

You need to give the initial amount in the account to fully define the sequence. This is sometimes called an **initial condition** for the recurrence relation.

Links A recurrence relation describes each term of a sequence in terms of the previous term or terms.
← Pure Year 2, Section 3.7

Notation This is an example of a **first-order recurrence relation**, as u_{m+1} is given in terms of one previous term, u_m .
→ Section 4.2

Example 1

You owe £500 on a credit card that charges 1.5% interest each month. You decide to make no new charges and you pay off £50 each month. Formulate a recurrence relation that describes the balance remaining on the credit card after n months.

Let u_n be the amount in pounds owed after n months.

During a month, the interest is $0.015u_n$ and you pay off £50.

$$u_{n+1} = u_n + 0.015u_n - 50 = 1.015u_n - 50, \text{ with } u_0 = 500$$

Define the terms and give any relevant units.

The interest is **added** to the balance and the amount you pay off is **subtracted** from it.

Remember to give the **initial condition**.

Example 2

The deer population of a county was observed to be 1200 in a given year. The population is modelled to increase at a rate of 15% each year. Let d_n be the population of deer n years later. Explain why the deer population is modelled by the recurrence relation

$$d_n = 1.15d_{n-1}, \text{ with } d_0 = 1200$$

After $n - 1$ years the population is d_{n-1}

This is increased by 15%, so the population after n years is $d_{n-1} + 0.15d_{n-1} = 1.15d_{n-1}$

The initial population is 1200, so $d_0 = 1200$

Explain the recurrence relation in the context of the question.

Example 3

A A population of bacteria has initial size 200. After one hour, the population has reached 220. The population grows in such a way that the rate of growth doubles each hour. Write a recurrence relation to describe the number of bacteria, b_n , after n hours.

$$b_0 = 200 \text{ and } b_1 = 220$$

The increase from time $n - 1$ to n is $b_n - b_{n-1}$,
and the increase from time $n - 2$ to $n - 1$ is

$$b_{n-1} - b_{n-2}$$

$$\text{So } b_n - b_{n-1} = 2(b_{n-1} - b_{n-2})$$

$$b_n = 3b_{n-1} - 2b_{n-2}, \text{ with } b_0 = 200, b_1 = 220$$

The **rate** of growth doubles each hour. So the increase from time $n - 1$ to n will be double the increase from time $n - 2$ to $n - 1$.

Notation This is an example of a **second-order recurrence relation**, as b_{n+1} is given in terms of **two previous terms**, b_{n-1} and b_{n-2} . You need **two initial conditions** to define the sequence, given here in terms of b_0 and b_1 . → **Section 4.3**

If you know the general term of a sequence in the form $u_n = f(n)$, you can verify that it satisfies a given recurrence relation by substitution.

Example 4

A sequence has the general term $u_n = 3n - 1$. Verify that the sequence satisfies the recurrence relation $u_n = 3 + u_{n-1}$.

$$u_n = 3n - 1, \text{ so } u_{n-1} = 3(n-1) - 1 = 3n - 4$$

Substituting into the RHS of the recurrence relation,

$$3 + u_{n-1} = 3 + (3n - 4)$$

$$= 3n - 1$$

$$= u_n \text{ as required}$$

Watch out This is not the only general term that satisfies this recurrence relation. Any general term of the form $u_n = 3n + k$, where k is a constant, will also satisfy the recurrence relation. If you want to prove that a general term satisfies a given recurrence relation with an initial condition, you can do this using mathematical induction. → **Section 4.4**

Example 5

A sequence has the general term $u_n = 2 \times 3^{n-1}$. Verify that the sequence satisfies the recurrence relation $u_n = 3 + u_{n-1}$.

$$u_{n-1} = 2 \times 3^{(n-1)-1} = 2 \times 3^{n-2}$$

Substituting into the RHS of the recurrence relation,

$$3u_{n-1} = 3(2 \times 3^{n-2}) = 2 \times 3^{n-1} = u_n$$

Notation $u_n = 3u_{n-1}$ is the **recursive form** of the sequence. $u_n = 2 \times 3^{n-1}$ is the **solution**, or the **closed form** of the sequence. It is also sometimes called the **explicit form** of the sequence. → **Section 4.2**

Exercise 4A

- 1 The value of an endowment policy increases at a rate of 5% per annum. The initial value of the policy is £7000.
 - a Write down a recurrence relation for the value of the policy after n years.
 - b Calculate the value of the policy after 4 years.
- Hint** Remember to include an initial condition in your answer to part a.
- 2 A patient is injected with 156 ml of a drug. Every 8 hours, 22% of the drug passes out of his bloodstream, and a further 25 ml dose of the drug is administered. After $8n$ hours, the amount of the drug in the patient's bloodstream is d_n ml.
 - a Find an expression for d_n in terms of d_{n-1} , and write down the value of d_0 .
 - b Calculate, to the nearest millilitre, the amount of drug in the patient's bloodstream after 24 hours.
- E** 3 Kandace takes out a personal loan of £5000 to buy a car. The interest rate on the loan is 0.5% per month. Interest is calculated and added to the loan balance at the end of each month. At the end of each month, Kandace makes a monthly payment of £200, which is deducted from the balance of the loan. The balance in pounds at the end of the n th month is given by b_n . Explain why $b_n = kb_{n-1} - 200$, with $b_0 = 5000$, and find the value of the constant k . **(3 marks)**
- E** 4 At the time a census is taken, the population of a country is 12.5 million. The annual birth rate is 4% and the annual death rate is 3%. In addition, each year there is a net migration of 50 000 new immigrants into the country. Write a recurrence relation for the population of the country n years after the census, P_n . **(3 marks)**
- 5 A sequence has general term $u_n = 5n + 2$. Verify that the sequence satisfies the recurrence relation $u_n = u_{n-1} + 5$.
- 6 A sequence has general term $u_n = 6 \times 2^n + 1$. Verify that the sequence satisfies the recurrence relation $u_n = 2u_{n-1} - 1$.
- P** 7 Consider the sequence given by $u_n = \sum_{i=1}^n (2i - 1)$
 - a Write down the first 4 terms of the sequence.
 - b Explain why the recurrence relation associated with this sequence is $u_{n+1} = u_n + 2n + 1, n \geq 1$
 - c Verify that $u_n = n^2$ is a solution to this recurrence relation.
- E/P** 8 In January 2010, a small oil company produced 2000 barrels of oil and sold 1800 barrels of oil. Any remaining oil was stockpiled. From January 2010 onwards, the company increased its sales by 20 barrels per month, and increased its oil production by 1% each month.
 - a Find an expression for:
 - i the number of barrels produced by the well in the n th month
 - ii the number of barrels sold in the n th month.

(4 marks)

At the beginning of January 2010, the oil company had no stockpiled oil.

- b Find a recurrence relation for the total number of stockpiled barrels, s_n , at the end of the n th month. (3 marks)

- E/P** 9 There are n people at a gathering. Each person shakes hands with everybody else exactly once. Let $h(n)$ be the number of handshakes that occur.

a Explain why $h(1) = 0$. (1 mark)

b Find a recurrence relation for $h(n + 1)$ in terms of $h(n)$. (2 marks)

- A** 10 Generate the first six terms of each of the following sequences:

a $u_n = 2u_{n-1} + 3u_{n-2}$, with $u_0 = 1$ and $u_1 = 1$

b $u_n = u_{n-1} - 2u_{n-2}$, with $u_0 = 1$ and $u_1 = 1$

c $u_n = u_{n-1} + u_{n-2} + 2n$, with $u_0 = 1$ and $u_1 = 1$

- E** 11 Assume that growth in a bacterial population has the following properties:

- At the beginning of every hour, each bacterium that lived in the previous hour divides into two new bacteria. During the hour, all bacteria that have lived for two hours die.
- At the beginning of the first hour, the population consists of 100 bacteria.

At the end of the n th hour there are B_n bacteria in the population.

Find a recurrence relation for B_n . (3 marks)

- P** 12 A sequence has n th term $u_n = (2 - n)2^{n+1}$.
Verify that the sequence satisfies the recurrence relation $u_n = 4(u_{n-1} - u_{n-2})$.

- E/P** 13 A battery-operated kangaroo is able to make two kinds of jumps: small jumps of length 10 cm or large jumps of length 20 cm. The number of different ways in which the kangaroo can cover a distance of $10n$ cm is denoted by J_n .

a By writing down all possible combinations of jumps for a distance of 40 cm, show that $J_4 = 5$. (2 marks)

b Find a recurrence relation for J_n , stating the initial conditions. (3 marks)

c How many different ways can this kangaroo cover a distance of 80 cm? (1 mark)

- E/P** 14 A female rabbit is modelled as producing 2 surviving female offspring in its first year of life, and 6 in each subsequent year. A population initially has 4 female rabbits, all of whom are more than 1 year old.

a If F_n is the number of female rabbits in the population after n years, explain why F_n is modelled by the recurrence relation

$$F_n = 3F_{n-1} + 4F_{n-2}, \text{ with } F_0 = 4 \text{ and } F_1 = 28 \quad \text{(3 marks)}$$

b Suggest a criticism of this model. (1 mark)

- A** 15 Binary strings consist of 1s and 0s. There are 5 different binary strings of length 3 which **do not** contain consecutive 1s:

000, 001, 010, 100, 101

Let b_n represent the number binary strings of length n with no consecutive 1s.

- a Find b_1 and b_2 . (1 mark)
- b Explain why b_n satisfies the recurrence relation $b_n = b_{n-1} + b_{n-2}$. (3 marks)
- c Hence find b_7 . (1 mark)

Hint For example, 011 is not allowable because it contains consecutive 1s.

4.2 Solving first-order recurrence relations

You need to be able to **solve** recurrence relations. This means finding a **closed form** for the terms in the sequence in the form $u_n = f(n)$.

- **The order of a recurrence relation is the difference between the highest and lowest subscript in the relation.**
- **A first-order recurrence relation is one in which u_n can be given as a function of n and u_{n-1} only.**

Examples of first-order recurrence relations are:

$$u_n = 2u_{n-1} + n$$

$$a_n = (n+1)a_{n-1} - 1$$

$$P_{n+1} = 5P_n + 2n^2$$

Here the subscripts given are $n+1$ and n . This is still a first-order recurrence relation because the difference between them is 1.

In this section you will learn how to solve first-order **linear** recurrence relations.

- **A first-order linear recurrence relation can be written in the form $u_n = au_{n-1} + g(n)$, where a is a real constant.**
 - **If $g(n) = 0$, then the equation is homogeneous.**

You can sometimes find solutions to recurrence relations using a technique called **back substitution**.

Example 6

Find a closed form for the sequence

$$a_n = 5a_{n-1}, n > 0; a_0 = 1$$

$$a_n = 5a_{n-1}$$

$$= 5 \times 5a_{n-2} = 5^2a_{n-2}$$

$$= 5^2 \times 5a_{n-3} = 5^3a_{n-3}$$

$$= \dots = 5^n a_0$$

$a_0 = 1$, so the closed form of this sequence

$$\text{is } a_n = 5^n$$

Watch out When you find a closed form by this method, you need to subsequently **prove** it using mathematical induction. → Section 4.4

$a_{n-1} = 5a_{n-2}$. Substitute this into the expression for a_n .

This is the geometric sequence 1, 5, 25, 125 ...

The recurrence relation in the example above is an example of a **homogeneous** recurrence relation. A first-order homogeneous linear recurrence relation can be written in the form $u_n = au_{n-1}$.

Using back substitution,

$$\begin{aligned} u_n &= au_{n-1} \\ &= a \times au_{n-2} = a^2u_{n-2} \\ &= a^2 \times au_{n-3} = a^3u_{n-3} \\ &\vdots \\ &= a^{n-1}u_1 \\ &= a^n u_0 \end{aligned}$$

■ **The solution to the first-order homogeneous linear recurrence relation $u_n = au_{n-1}$ is given by $u_n = u_0a^n$ or $u_n = u_1a^{n-1}$.**

Unless you are told to prove a recurrence relation by induction, you can write down these solutions in your exam.

Example 7

Solve the recurrence relation $a_n = 2a_{n-1}$, $n \geq 1$, with $a_0 = 3$.

$$\begin{aligned} a_n &= a_0(2^n) \\ &= 3(2^n) \end{aligned}$$

This is a homogeneous linear first-order recurrence relation, so use the rule given above to write down the general solution.

It is useful to think of a **general solution** to the recurrence relation $u_n = au_{n-1}$ in the form $u_n = ca^n$, where c is an arbitrary constant. You can then use the initial conditions to find the value of c . This will give you a **particular solution**.

Links The process of finding general solutions (with arbitrary constants), and then using initial conditions to find particular solutions, is very similar to the process of solving a differential equation. You can think of a recurrence relation as a discrete version of a differential equation. ← Pure Year 2, Section 11.10

Example 8

Solve the recurrence relation $a_n = -3a_{n-1}$, $n \geq 1$, with $a_1 = 6$.

Method 1

$$\begin{aligned} a_n &= a_1(-3)^{n-1} \\ &= 6(-3)^{n-1} \end{aligned}$$

Method 2

General solution is $a_n = c(-3)^n$
 $a_1 = 6 \Rightarrow 6 = c(-3)^1 \Rightarrow c = -2$
 Therefore, the particular solution is $a_n = -2(-3)^n$.

Use the form of the solution $u_n = u_1r^{n-1}$.

Write a general solution with an arbitrary constant, then use the initial condition to find the value of the constant.

Problem-solving

The two solutions are equivalent:

$$-2(-3)^n = -2(-3)(-3)^{n-1} = 6(-3)^{n-1}$$

You can find solutions to some non-homogeneous linear recurrence relations using back-substitution.

Example 9

Find a solution to the recurrence relation $u_n = u_{n-1} + n$, $n \geq 1$, with $u_0 = 0$.

Using iteration,

$$\begin{aligned} u_n &= u_{n-1} + n \\ &= (u_{n-2} + (n-1)) + n \\ &\vdots \\ &= u_0 + 1 + 2 + \dots + n \\ &= u_0 + \sum_{r=1}^n r \\ &= \frac{n(n+1)}{2} \end{aligned}$$

Therefore, the closed form for this recurrence relation is $u_n = \frac{n(n+1)}{2}$

Replace n by $n-1$ in $u_n = u_{n-1} + n$, then substitute.

$u_0 = 0$ and the sum of the first n integers is $\frac{n(n+1)}{2}$

← Core Pure Book 1, Section 3.1

You can apply this method to any recurrence relation of the form $u_n = u_{n-1} + g(n)$:

$$\begin{aligned} u_n &= u_{n-1} + g(n) \\ &= (u_{n-2} + g(n-1)) + g(n) \\ &= ((u_{n-3} + g(n-2)) + g(n-1)) + g(n) \\ &\vdots \\ &= u_0 + \sum_{r=1}^n g(r) \end{aligned}$$

- The solution to the first-order non-homogeneous linear recurrence relation $u_n = u_{n-1} + g(n)$ is given by $u_n = u_0 + \sum_{r=1}^n g(r)$.

Watch out

If u_1 is given instead of u_0 , the solution would be $u_1 + \sum_{r=2}^n g(r)$

Example 10

Solve the following recurrence relations.

- a $u_n = u_{n-1} + 2n + 1$, $n \geq 0$, with $u_0 = 7$
 b $u_n = u_{n-1} + 5^n$, $n \in \mathbb{N}$, with $u_1 = 3$

a $u_n = u_0 + \sum_{r=1}^n g(r)$

$$\begin{aligned} &= 7 + \sum_{r=1}^n (2r + 1) \\ &= 7 + 2 \sum_{r=1}^n r + \sum_{r=1}^n 1 \\ &= 7 + n(n+1) + n \\ &= n^2 + 2n + 7 \end{aligned}$$

Use the formula for the solution to a recurrence relation of the form $u_n = u_{n-1} + g(n)$.

Use the standard results for $\sum_{r=1}^n r$ and $\sum_{r=1}^n 1$.

← Core Pure Book 1, Section 3.1

b Method 1

$$u_0 = u_1 - 5^1 = -2$$

$$u_n = u_0 + \sum_{r=1}^n g(r)$$

$$= -2 + \sum_{r=1}^n 5^r$$

$$= -2 + \frac{5(1 - 5^n)}{1 - 5}$$

Method 2

$$u_n = u_1 + \sum_{r=2}^n g(r) = 3 + \sum_{r=2}^n 5^r$$

$$= 3 + \frac{5^2(1 - 5^{n-1})}{1 - 5}$$

$$= -2 - \frac{5}{4} + \frac{5^{n+1}}{4}$$

$$= \frac{1}{4}(5^{n+1}) - \frac{13}{4}$$

The initial condition is given in terms of u_1 , so you need to find an expression for u_0 before you can use the formula.

$\sum_{r=1}^n 5^r$ is a geometric series with n terms, first term 5 and common ratio 5. ← Pure Year 2, Chapter 3

If you need to solve a recurrence relation of the form $u_n = au_{n-1} + g(n)$, where $a \neq 1$, back substitution gets more complicated. You can solve non-homogeneous recurrence relations of this form by first considering the general solution to the corresponding homogeneous recurrence relation, $u_n = au_{n-1}$. This general solution is called the **complementary function (C.F.)**. You then need to add a **particular solution (P.S.)** to the recurrence relation.

Links

The particular solution plays a similar role to the particular integral which is used when solving a second-order linear differential equation.

→ Core Pure Book 2, Section 7.3

- When solving a recurrence relation of the form $u_n = au_{n-1} + g(n)$, the form of the particular solution will depend on $g(n)$:

Form of $g(n)$	Form of particular solution
p with $a \neq 1$	λ
$pn + q$ with $a \neq 1$	$\lambda n + \mu$
kp^n with $p \neq a$	λk^n
ka^n	λna^n

Watch out

This particular solution will satisfy the whole recurrence relation but will not necessarily satisfy the initial condition.

- To solve the recurrence relation

$$u_n = au_{n-1} + g(n),$$

- Find the **complementary function (C.F.)**, which is the general solution to the associated homogeneous recurrence relation $u_n = au_{n-1}$.
- Choose an appropriate form for a **particular solution (P.S.)** then substitute into the original recurrence relation to find the values of any coefficients.
- The general solution is $u_n = \text{C.F.} + \text{P.S.} = ca^n + \text{P.S.}$
- Use the initial condition to find the value of the arbitrary constant.

Watch out

The term **particular solution** is also sometimes used to refer to the final solution given the initial condition. Both versions satisfy the recurrence relation but only the final solution satisfies the initial condition.

You can use this method when $a = 1$, but in this case the complementary function is a constant, so you need to find a particular solution with no constant terms. You can do this by multiplying the particular solution by n :

Form of $g(n)$	Form of particular solution
p with $a = 1$	λn
$pn + q$ with $a = 1$	$\lambda n^2 + \mu n$

Note For recurrence relations of the form $u_n = u_{n-1} + p$ or $u_n = u_{n-1} + pn + q$, it is usually easier to use the summation formula given on page x.

Example 11

Solve the recurrence relation $u_n = 3u_{n-1} + 2n$, $n \in \mathbb{Z}^+$, with $u_1 = 3$.

Associated homogeneous recurrence relation is $u_n = 3u_{n-1}$

Complementary function: $u_n = c(3^n)$

Particular solution: $u_n = \lambda n + \mu$

$$u_n = 3u_{n-1} + 2n$$

$$\lambda n + \mu = 3(\lambda(n-1) + \mu) + 2n$$

$$\lambda n + \mu = 3\lambda n - 3\lambda + 3\mu + 2n$$

$$0 = (2\lambda + 2)n + (2\mu - 3\lambda)$$

$$\Rightarrow 2\lambda + 2 = 0 \quad \text{and} \quad 2\mu - 3\lambda = 0$$

$$\Rightarrow \lambda = -1, \mu = -\frac{3}{2}$$

So a particular solution to the recurrence relation is $u_n = -n - \frac{3}{2}$

The general solution is $u_n = c(3^n) - n - \frac{3}{2}$

Since $u_1 = 3$,

$$3 = c(3^1) - 1 - \frac{3}{2} \Rightarrow c = \frac{11}{6}$$

The solution is $u_n = \frac{11}{6}(3^n) - n - \frac{3}{2}$

Find the general solution to the associated homogeneous recurrence relation. This is the **complementary function (C.F.)**.

$g(n)$ is of the form $pn + q$, so look for a particular solution of the form $\lambda n + \mu$. You need to include the constant term even though $g(n)$ does not have a constant term.

Problem-solving

Simplify, and group together coefficients of n and constant coefficients. Since the values of λ and μ must satisfy the recurrence relation for **any value of n** , you can consider it as an identity. This means that you can equate coefficients with the same power of n on both sides.

Substitute $u_n = \lambda n + \mu$ and $u_{n-1} = \lambda(n-1) + \mu$ into the full recurrence relation.

Solve these two equations simultaneously.

You could prove this solution using mathematical induction. However, you don't need to do this in your exam unless you are explicitly asked to.

General solution = C.F. + P.S.

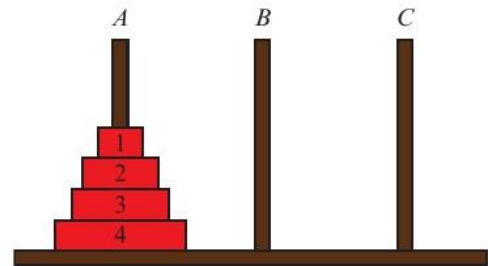
Use the initial condition $u_1 = 3$ to find the value of c .

Example 12

The Tower of Hanoi puzzle involves transferring a pile of different sized disks from one peg to another using an intermediate peg.

The rules are as follows:

- Only one disk at a time can be moved.
- A disk can only be moved if it is the top disk on a pile.
- A larger disk can never be placed on a smaller one.



- Find the minimum number of moves needed to transfer two disks from one peg to another.
- Show that three disks can be transferred from one peg to another in 7 moves.
- Explain why the minimum number of moves, d_n , needed to transfer n disks from one peg to another satisfies the recurrence relation $d_n = 2d_{n-1} + 1$, with $d_1 = 1$.
- Solve this recurrence relation for d_n .
- Hence determine the minimum number of moves needed to transfer 15 disks from one peg to another.

a 3 moves

b

Move number	Disk	From	To
1	1	A	B
2	2	A	C
3	1	B	C
4	3	A	B
5	1	C	A
6	2	C	B
7	1	A	B

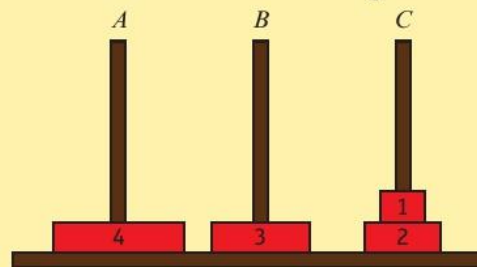
- c Before you can move the largest disk (disk n), you must have transferred all the other disks to a single peg, say C . This requires d_{n-1} moves. You then move disk n in 1 move, to peg B . Finally, transfer the other disks to be on top of disk n , on peg B . This requires a further d_{n-1} moves. So the total number of moves is

$$d_n = d_{n-1} + 1 + d_{n-1} = 2d_{n-1} + 1$$

One disk can be transferred in one move so $d_1 = 1$.

For example, move disk 1 from A to B , disk 2 from A to C , then disk 1 from B to C .

After move 4 the disks are arranged as follows:



Make sure you explain why the initial condition is true as well.

d Associated homogeneous recurrence

relation: $d_n = 2d_{n-1}$

Complementary function: $d_n = c(2^n)$

Particular solution: $d_n = \lambda$

$$d_n = 2d_{n-1} + 1$$

$$\lambda = 2\lambda + 1$$

$$\lambda = -1$$

So a particular solution to the recurrence relation is $d_n = -1$.

The general solution is $d_n = c(2^n) - 1$

Since $d_1 = 1$,

$$1 = c(2^1) - 1 \Rightarrow c = 1$$

The solution is $d_n = 2^n - 1$

e $d_{15} = 2^{15} - 1 = 32767$

Find the general solution to the associated homogeneous recurrence relation.

The recurrence relation is of the form $u_n = au_{n-1} + g(n)$ with $a \neq 1$ and $g(n) = p$, a constant, so try a particular solution of the form $u_n = \lambda$.

Substitute $d_n = \lambda$ and $d_{n-1} = \lambda$ into the full recurrence relation and solve to find λ .

General solution = C.F. + P.S.

Use the initial condition $d_1 = 1$ to find the value of the arbitrary constant, c .

Exercise 4B

1 Find the solution to each of the following recurrence relations.

a $u_n = 2u_{n-1}$, with $u_0 = 5$

b $b_n = \frac{5}{2}b_{n-1}$, with $b_1 = 4$

c $d_n = -\frac{11}{10}d_{n-1}$, with $d_1 = 10$

d $x_{n+1} = -3x_n$, with $x_0 = 2$

2 Find a closed form for the sequences defined by the following recurrence relations.

a $u_n = u_{n-1} + 3$, with $u_0 = 5$

b $x_n = x_{n-1} + n$, with $x_0 = 2$

c $y_n = y_{n-1} + n^2 - 2$, with $y_0 = 3$

d $s_{n+1} = s_n + 2n - 1$, with $s_0 = 1$

Watch out In part **d**, the summation indices are slightly different, so this recurrence relation is not in the form $u_n = u_{n-1} + g(n)$. If you substitute n for $n - 1$ throughout the recurrence relation you can use the formula $u_n = u_0 + \sum_{r=1}^n g(r)$

3 Solve each of the following recurrence relations.

a $a_n = 2a_{n-1} + 1$, with $a_1 = 1$

b $u_n = -u_{n-1} + 2$, with $u_1 = 3$

c $h_n = 3h_{n-1} + 5$, with $h_0 = 1$

d $b_n = -2b_{n-1} + 6$, with $b_1 = 3$

Hint In each case, use a constant particular solution of the form λ .

E 4 In a league of n football teams, each team plays every other team exactly once. In total, g_n matches are played.

a Explain why $g_n = g_{n-1} + n - 1$, and write down a suitable initial condition for this recurrence relation. (3 marks)

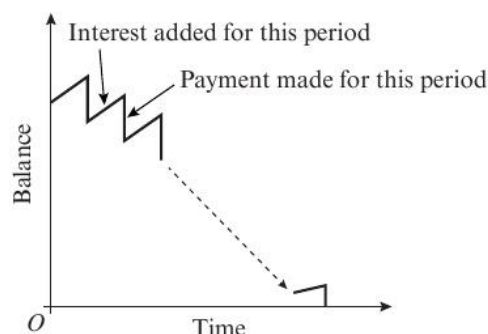
b By solving your recurrence relation, show that $g_n = \frac{n(n-1)}{2}$ (4 marks)

- 5 a Find the general solution to the recurrence relation $u_n = 4u_{n-1} - 1$, $n \geq 2$
 b Hence or otherwise find the particular solution given that:
 i $u_1 = 3$ ii $u_1 = 0$ iii $u_1 = 200$
- (E/P)** 6 a Find the general solution to the recurrence relation $u_n = 3u_{n-1} + n$, $n > 1$. (3 marks)
 b Given that $u_1 = 5$, find the particular solution to this recurrence relation. (1 mark)
- (E)** 7 A sequence is defined by the recurrence relation $u_{n+1} = 0.6u_n + 4$, with $u_0 = 7$.
 a Find u_3 . (1 mark)
 b Find a closed form for the recurrence relation. (3 marks)
 c Find the smallest value of n for which $u_n > 9.9$. (1 mark)
- (E/P)** 8 The deer population in a forest is estimated to drop by 5% each year.
 Each year, 20 additional deer are introduced to the forest.
 The initial deer population is 200, and the population after n years is given by D_n .
 a Write down a recurrence relation for D_n . (3 marks)
 b By solving your recurrence relation, find an expression for D_n in terms of n . (3 marks)
 c Describe the behaviour of the deer population in the long term. (1 mark)
- (E)** 9 Solve the recurrence relation $u_n - 4u_{n-1} + 3 = 0$, with $u_0 = 7$. (3 marks)
- (E)** 10 A sequence of numbers satisfies the recurrence relation
 $u_n = u_{n-1} + 2^n$, $n \geq 2$, with $u_1 = 5$
 Find a closed form for u_n . (3 marks)
- (E)** 11 Solve the recurrence relation $u_n = 4u_{n-1} + 2n$, with $u_0 = 7$. (4 marks)
- (E/P)** 12 A sequence satisfies the recurrence relation $u_n = 2u_{n-1} - 1005$, with $u_0 = 1000$.
 a Solve the recurrence relation to find a closed form for u_n . (4 marks)
 b Hence, or otherwise, find the first negative term in the sequence. (3 marks)
- (E/P)** 13 a Find the general solution to the recurrence relation $u_n = 2u_{n-1} - 2^n$, $n \geq 2$. (4 marks)
 b Find the particular solution to this recurrence relation given that $u_1 = 3$. (1 mark)
- (E/P)** 14 A sequence is defined by the recurrence relation $u_n = ku_{n-1} + 1$, $k \neq 1$, with $u_0 = 0$.
 a Find the value of u_1 , u_2 , and u_3 in terms of k . (2 marks)
 b Find a closed form for this sequence. (3 marks)
 c Describe the behaviour of the sequence as n gets very large in the cases when:
 i $k > 1$ ii $-1 < k < 1$ iii $k = -1$ iv $k < -1$ (4 marks)
- (E/P)** 15 A sequence is defined by the recurrence relation
 $a_n = a_{n-1} + 6n + 1$, $n \in \mathbb{Z}^+$, with $a_0 = 2$
 a Find $\sum_{r=1}^n (6r + 1)$ (2 marks)
 b Hence, or otherwise, find a closed form for this sequence. (3 marks)
 c Given that $a_n = 561$, find the value of n . (2 marks)

- E/P** 16 a Solve the recurrence relation $u_n = u_{n-1} - 6n^2$, with $u_0 = 89$. (3 marks)
 b Hence, or otherwise, find the first negative term of the sequence. (2 marks)
 c Explain why every term of the sequence is an odd number. (2 marks)

- E/P** 17 a Solve the recurrence relation $u_n = u_{n-1} - 2n$, with $u_0 = 3$. (2 marks)
 b Show that -103 is not a term of the sequence. (2 marks)
 c Given that $u_k = -459$, find the value of k . (2 marks)

- E/P** 18 Alison borrows £2000 on her credit card. She intends to pay it back by making 18 monthly payments. At the end of each month, interest of 1.5% is added to the loan balance, and Alison's monthly payment of £ P is deducted from the loan balance. The graph illustrates how the balance of the loan will change over time.



- a Write a recurrence relation for the balance of the loan at the end of n months. (3 marks)
 b Find a solution to your recurrence relation, giving your answer in terms of P . (3 marks)
 Alison wants the balance of the loan to be zero after she makes her 18th payment.
 c Find the value of P that will make this the case. (3 marks)

Challenge

A **restricted** Tower of Hanoi problem requires a player to move a pile of disks of different sizes from peg A to peg C . The rules are as follows:

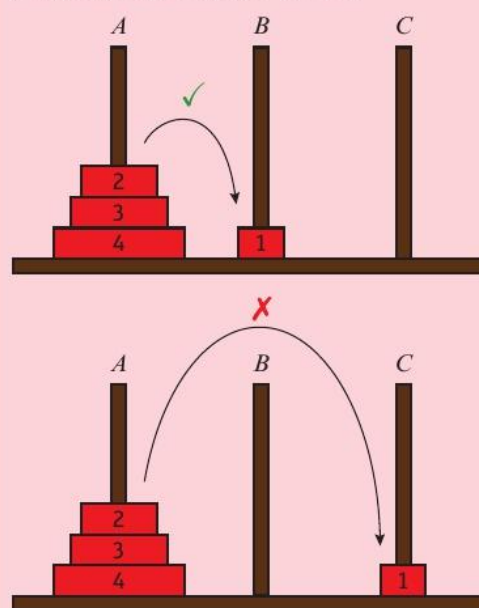
- Only one disk at a time can be moved.
- A disk can only be moved if it is the top disk on a pile.
- A larger disk can never be placed on a smaller one.
- **Disks can only be moved a distance of one peg at a time.**

Let H_n be the minimum number of moves needed to transfer n discs from peg A to peg C .

- a Explain why $H_1 = 2$.
 b Show that 2 disks can be moved from peg A to peg C in 8 moves.
 c Explain why H_n satisfies a recurrence relation of the form $H_n = aH_{n-1} + b$, and determine the values of a and b .
 d i Solve this recurrence relation for H_n .
 ii Hence determine the minimum number of moves needed to transfer 10 disks from peg A to peg C .

Watch out

The fourth rule means that moves between pegs A and B , and pegs B and C are allowed, but direct moves between pegs A and C are not.



4.3 Solving second-order recurrence relations

A In this section you will learn how to solve second-order linear recurrence relations.

■ **A second-order linear recurrence relation can be written in the form**

$$u_n = au_{n-1} + bu_{n-2} + g(n), \text{ where } a \text{ and } b \text{ are real constants.}$$

• **If $g(n) = 0$, then the equation is homogeneous.**

Example 13

Consider the recurrence relation $u_n = 2u_{n-1} - u_{n-2}$, $n \geq 2$.

Verify that the following particular solutions satisfy this recurrence relation.

a $u_n = 3n$ **b** $u_n = 5$ **c** $u_n = 3n + 5$

a $u_n = 3n$, $u_{n-1} = 3(n-1) = 3n-3$
 $u_{n-2} = 3(n-2) = 3n-6$
 $2u_{n-1} - u_{n-2} = 2(3n-3) - (3n-6) = 3n = u_n$
 So $u_n = 3n$ satisfies the recurrence relation.

b $u_n = 5$, $u_{n-1} = 5$, $u_{n-2} = 5$
 $2u_{n-1} - u_{n-2} = 2 \times 5 - 5 = 5 = u_n$
 So $u_n = 5$ satisfies the recurrence relation.

c $u_n = 3n + 5$, $u_{n-1} = 3(n-1) + 5 = 3n + 2$
 $u_{n-2} = 3(n-2) + 5 = 3n - 1$
 $2u_{n-1} - u_{n-2} = 2(3n + 2) - (3n - 1) = 3n + 5 = u_n$
 So $u_n = 3n + 5$ satisfies the recurrence relation.

Find expressions for u_{n-1} and u_{n-2} and substitute them into the RHS of the recurrence relation.

■ **If $u_n = F(n)$ and $u_n = G(n)$ are particular solutions to a linear recurrence relation, then $u_n = aF(n) + bG(n)$, where a and b are constants, is also a solution.**

You can solve a **second-order homogeneous linear** recurrence relation by looking for solutions of the form $u_n = Ar^n$, where A is an arbitrary non-zero constant.

Suppose that $u_n = Ar^n$ is a solution to the recurrence relation $u_n = au_{n-1} + bu_{n-2}$.

Then $Ar^n = Aar^{n-1} + Abr^{n-2}$
 $\Rightarrow r^2 - ar - b = 0$ Multiply both sides by r^{2-n} and simplify.

This quadratic equation is called the **auxiliary equation** of the recurrence relation. $u_n = Ar^n$ is a solution to the recurrence relation if and only if r is a root of this equation.

Notation The auxiliary equation is sometimes called the **characteristic equation**.

However, a second-order recurrence relation requires **two initial conditions** to fully define the sequence. As such, the general solution to a second-order recurrence relation requires **two arbitrary constants**. You can formulate a general solution with two arbitrary constants by adding multiples of two different solutions.

- A** ■ You can find a general solution to a second-order homogeneous linear recurrence relation, $u_n = au_{n-1} + bu_{n-2}$, by considering the auxiliary equation

$$r^2 - ar - b = 0$$

You need to consider three different cases:

• **Case 1: Distinct real roots**

If the auxiliary equation has distinct real roots α and β , then the general solution will have the form $u_n = A\alpha^n + B\beta^n$ where A and B are arbitrary constants.

Links

These three cases are similar to the cases you consider when solving a differential equation of the form $a\frac{d^2y}{dx^2} + b\frac{dy}{dx} + cy = 0$.

→ Core Pure Book 2, Section 7.2

• **Case 2: Repeated root**

If the auxiliary equation has a repeated real root α , then the general solution will have the form $u_n = (A + Bn)\alpha^n$ where A and B are arbitrary constants.

• **Case 3: Complex roots**

If the auxiliary equation has two complex roots $\alpha = re^{i\theta}$ and $\beta = re^{-i\theta}$, then the general solution will have the form $u_n = r^n(A\cos n\theta + B\sin n\theta)$, or $u_n = A\alpha^n + B\beta^n$, where A and B are arbitrary constants.

Example 14

- a Find a general solution to the recurrence relation

$$u_n = 2u_{n-1} + 8u_{n-2}, n \geq 2$$

- b Verify that your general solution from part a satisfies the recurrence relation.

- c Given that $u_0 = 4$ and $u_1 = 10$, find a particular solution.

a $r^2 - 2r - 8 = 0$
 $(r - 4)(r + 2) = 0$
 $\Rightarrow r = 4 \text{ or } r = -2$

General solution is $u_n = A(4^n) + B(-2)^n$

b $2u_{n-1} + 8u_{n-2}$
 $= 2(A(4^{n-1}) + B(-2)^{n-1}) + 8(A(4^{n-2}) + B(-2)^{n-2})$
 $= 2A(4^{n-1}) + 2B(-2)^{n-1} + 8A(4^{n-2}) + 8B(-2)^{n-2}$
 $= 2A(4^{n-1}) + 2B(-2)^{n-1} + 2A(4^{n-1}) - 4B(-2)^{n-1}$
 $= 4A(4^{n-1}) - 2B(-2)^{n-1}$
 $= A(4^n) + B(-2)^n$
 $= u_n$

c $u_0 = 4 \Rightarrow A(4^0) + B(-2)^0 = 4 \Rightarrow A + B = 4$
 $u_1 = 10 \Rightarrow A(4^1) + B(-2)^1 = 10 \Rightarrow 4A - 2B = 10$
 Solving simultaneously, $A = 3$ and $B = 1$
 So the solution is $u_n = 3(4^n) + (-2)^n$

Write down the auxiliary equation and solve it.

The auxiliary equation has two distinct real roots, so the general solution has the form $u_n = A\alpha^n + B\beta^n$.

Substitute your general solution into the RHS of the recurrence relation, then take out factors of 4 and -2 to write the expression in terms of multiples of 4^n and $(-2)^n$.

Use the initial conditions to write two simultaneous equations in A and B . Solve these to find the values of the arbitrary constants.

Example 15

A Solve the recurrence relation $a_n = 3a_{n-1} - 2a_{n-2}$, with $a_1 = 5$ and $a_2 = 3$.

$$r^2 - 3r + 2 = 0$$

$$(r-1)(r-2) = 0$$

$$\Rightarrow r = 1 \text{ or } r = 2$$

So the general solution is $a_n = A(1^n) + B(2^n)$

$$= A + B(2^n)$$

$$a_1 = A + 2B = 5$$

$$a_2 = A + 4B = 3$$

So the solution is $a_n = 7 - 2^n$.

$$\Rightarrow A = 7, B = -1$$

Write down the auxiliary equation and solve it.

One of the roots is 1, so one of the terms in the general solution will be constant.

Use the initial conditions to find the arbitrary constants.

Problem-solving

You can check your answer by generating the first few terms of the sequence using the solution and the original recurrence relation. The first 5 terms here are 5, 3, -1, -9, and -25.

Example 16

Solve the recurrence relation $u_n = 4u_{n-1} - 4u_{n-2}$, with $u_0 = 1$ and $u_1 = 1$.

$$r^2 - 4r + 4 = 0$$

$$(r-2)^2 = 0$$

$$\Rightarrow r = 2$$

So the general solution is $u_n = (A + Bn)2^n$

$$u_0 = 1 \Rightarrow A = 1$$

$$u_1 = 1 \Rightarrow 2(A + B) = 1$$

$$2 + 2B = 1$$

$$B = -\frac{1}{2}$$

The solution is $u_n = (1 - \frac{1}{2}n)2^n$.

The auxiliary equation has one repeated root, so the general solution is of the form $u_n = (A + Bn)\alpha^n$.

Use the initial conditions to form two equations and solve these to find A and B .

You could also write this as $u_n = 2^n - n2^{n-1}$.

Example 17

a Find the general solution to the recurrence relation $u_n = 2u_{n-1} - 2u_{n-2}$.

b Given that $u_0 = 1$ and $u_2 = 2$, find the particular solution to the recurrence relation.

$$r^2 - 2r + 2 = 0$$

$$\Rightarrow r = \frac{2 \pm \sqrt{4-8}}{2} = 1 \pm i = \sqrt{2}e^{\pm i\frac{\pi}{4}}$$

$$\text{Form 1: } u_n = A(1+i)^n + B(1-i)^n$$

$$\text{Form 2: } u_n = (\sqrt{2})^n \left(C \cos \frac{n\pi}{4} + D \sin \frac{n\pi}{4} \right)$$

The auxiliary equation has distinct complex roots. These must be a conjugate pair, so you can write them in the form $x \pm iy$ or $re^{\pm i\theta}$.

← Core Pure Book 2, Chapter 1

The form $u_n = r^n(A \cos n\theta + B \sin n\theta)$ only uses real numbers.

A

b Using form 1:

$$u_0 = A(1+i)^0 + B(1-i)^0 = 1$$

$$\Rightarrow A + B = 1 \quad (1)$$

$$u_1 = A(1+i)^1 + B(1-i)^1 = 2$$

$$\Rightarrow A + B + (A - B)i = 2$$

$$\Rightarrow (A - B)i = 1$$

$$\Rightarrow A - B = -i \quad (2)$$

Solving (1) and (2):

$$A = \frac{1-i}{2} \text{ and } B = \frac{1+i}{2}$$

So the particular solution is

$$u_n = \left(\frac{1-i}{2}\right)(1+i)^n + \left(\frac{1+i}{2}\right)(1-i)^n$$

Using form 2:

$$u_0 = C(\sqrt{2})^0 \cos 0 + D(\sqrt{2})^0 \sin 0 = 1$$

$$\Rightarrow C = 1$$

$$u_1 = C(\sqrt{2})^1 \cos \frac{\pi}{4} + D(\sqrt{2})^1 \sin \frac{\pi}{4} = 2$$

$$\Rightarrow 1 \times \sqrt{2} \times \frac{\sqrt{2}}{2} + D \times \sqrt{2} \times \frac{\sqrt{2}}{2} = 2$$

$$\Rightarrow D = 1$$

So the particular solution is

$$u_n = (\sqrt{2})^n \left(\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right)$$

Watch out

The values of the arbitrary constants will be different depending on which form you use.

 Use the initial conditions to find the values of the arbitrary constants A and B . If you are using this form of the general solution, the arbitrary constants can be **complex**.

Problem-solving

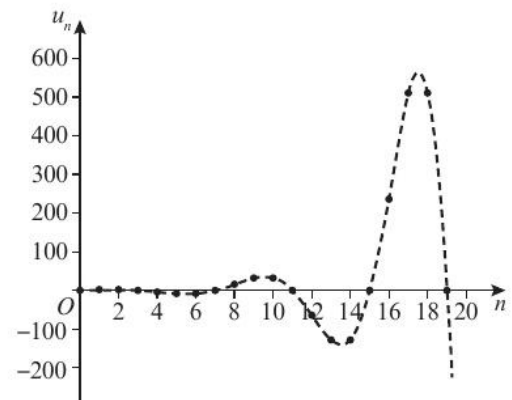
 You can simplify this to $u_n = (1+i)^{n-1} + (1-i)^{n-1}$ by writing, for example,

$$\left(\frac{1-i}{2}\right)(1+i)^n = \frac{(1-i)(1+i)}{2}(1+i)^{n-1} = (1+i)^{n-1}$$

With this form of the general solution, both arbitrary constants will be real numbers.

You can use the addition formula for sine to write the solution to the recurrence relation in Example 17 as

$$u_n = (\sqrt{2})^{n+1} \sin \frac{(n+1)\pi}{4}. \text{ This helps you to see that the}$$

 sequence oscillates between positive and negative values, with the magnitude of the oscillations increasing as n increases. The graph shows the sequence from u_0 to u_{19} . Note that the terms only exist for integer values of n and that, in this case, u_n is always an integer.

Example 18

The Fibonacci sequence is defined recursively as

$$F_n = F_{n-1} + F_{n-2}, n > 2, \text{ with } F_1 = 1 \text{ and } F_2 = 1$$

 Find a closed form for F_n .

$$r^2 - r - 1 = 0$$

$$\Rightarrow r = \frac{1+\sqrt{5}}{2} \text{ or } r = \frac{1-\sqrt{5}}{2}$$

So the general solution is

$$F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Solve the auxiliary equation.

A

Using the initial conditions,

$$F_1 = 1 \Rightarrow A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

$$A(1+\sqrt{5}) + B(1-\sqrt{5}) = 2 \quad (1)$$

$$F_2 = 1 \Rightarrow A\left(\frac{1+\sqrt{5}}{2}\right)^2 + B\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1$$

$$A(3+\sqrt{5}) + B(3-\sqrt{5}) = 2 \quad (2)$$

Solving (1) and (2) simultaneously,

$$A = \frac{1}{\sqrt{5}} \text{ and } B = -\frac{1}{\sqrt{5}}$$

The solution is

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Watch out You can solve these simultaneous equations quickly using your calculator. However, make sure you show enough working to demonstrate that you have used the initial conditions to generate two simultaneous equations.

You can solve **non-homogeneous** linear second-order recurrence relations by considering the complementary function (C.F.) and finding a suitable particular solution (P.S.).

- **To solve the recurrence relation $u_n = au_{n-1} + bu_{n-2} + g(n)$,**
 - **Find the complementary function, which is the general solution to the associated homogeneous recurrence relation $u_n = au_{n-1} + bu_{n-2}$.**
 - **Choose an appropriate form for a particular solution then substitute into the original recurrence relation to find the values of any coefficients.**
 - **The general solution is $u_n = \text{C.F.} + \text{P.S.}$**
 - **Use the initial conditions to find the values of the arbitrary constants.**

The form of the particular solution will depend on $g(n)$.

- **For the recurrence relation $u_n = au_{n-1} + bu_{n-2} + g(n)$, with auxiliary equation with roots α and β , try the following forms for a particular solution:**

Form of $g(n)$	Form of particular solution
p with $\alpha, \beta \neq 1$	λ
$pn + q$, with $\alpha, \beta \neq 1$	$\lambda n + \mu$
kp^n with $p \neq \alpha, \beta$	λp^n
p with $\alpha = 1, \beta \neq 1$	λn
$pn + q$ with $\alpha = 1, \beta \neq 1$	$\lambda n^2 + \mu n$
p with $\alpha = \beta = 1$	λn^2
$pn + q$ with $\alpha = \beta = 1$	$\lambda n^3 + \mu n^2$
$k\alpha^n$ with $\alpha \neq \beta$	$\lambda n\alpha^n$
$k\alpha^n$ with $\alpha = \beta$	$\lambda n^2\alpha^n$

Watch out The particular solution cannot have any terms in common with the complementary function of the associated homogeneous recurrence relation. The last six lines of this table, shown shaded, are special cases to avoid this. When $\alpha = 1$, multiply the expected form of the particular solution by n . When $\alpha = 1$ and $\beta = 1$, multiply the expected form of the particular solution by n^2 .

Example 19

Solve the recurrence relation

$$a_{n+2} + 4a_{n+1} + 3a_n = 5(-2)^n, \quad n > 0, \text{ with } a_0 = 2 \text{ and } a_1 = -1$$

A

Associated homogeneous recurrence relation:

$$a_{n+2} + 4a_{n+1} + 3a_n = 0$$

$$r^2 + 4r + 3 = 0$$

$$(r + 1)(r + 3) = 0$$

$$\Rightarrow r = -1 \text{ or } r = -3$$

So the complementary function is

$$a_n = A(-1)^n + B(-3)^n$$

 Try particular solution $a_n = \lambda(-2)^n$:

$$a_{n+2} + 4a_{n+1} + 3a_n = 5(-2)^n$$

$$\lambda(-2)^{n+2} + 4\lambda(-2)^{n+1} + 3\lambda(-2)^n = 5(-2)^n$$

$$4\lambda - 8\lambda + 3\lambda = 5$$

$$\lambda = -5$$

 So a particular solution is $a_n = -5(-2)^n$, and the general solution to the recurrence relation is

$$a_n = A(-1)^n + B(-3)^n - 5(-2)^n$$

$$a_0 = A(-1)^0 + B(-3)^0 - 5(-2)^0 \Rightarrow A + B - 5 = 2$$

$$A + B = 7$$

$$a_1 = A(-1)^1 + B(-3)^1 - 5(-2)^1 = -1$$

$$-A - 3B + 10 = -1$$

$$A + 3B = 11$$

$$\begin{cases} A + B = 7 \\ A + 3B = 11 \end{cases} \Rightarrow A = 5 \text{ and } B = 2$$

 So the solution is $a_n = 5(-1)^n + 2(-3)^n - 5(-2)^n$

Find the general solution to the associated homogeneous recurrence relation.

 Divide both sides of the equation by $(-2)^n$ and simplify.

General solution = C.F. + P.S.

 The values of A and B can be found by using the initial conditions.

Problem-solving

 Check your answer using $n = 0, 1, 2$.

Closed form:

$$a_0 = 5(-1)^0 + 2(-3)^0 - 5(-2)^0 = 2$$

$$a_1 = 5(-1)^1 + 2(-3)^1 - 5(-2)^1 = -1$$

$$a_2 = 5(-1)^2 + 2(-3)^2 - 5(-2)^2 = 3$$

Recurrence relation:

$$a_0 = 2, a_1 = -1$$

$$a_2 + 4a_1 + 3a_0 = 5(-2)^0 \Rightarrow a_2 = 5 + 4 - 6 = 3.$$

Example 20

 Find the general solution to $s_n = 3s_{n-1} + 4s_{n-2} + 4^n$.

Associated homogeneous recurrence relation:

$$s_n - 3s_{n-1} - 4s_{n-2} = 0$$

$$r^2 - 3r - 4 = 0$$

$$(r + 1)(r - 4) = 0$$

$$\Rightarrow r = -1 \text{ or } r = 4$$

So the complementary function is

$$s_n = A(-1)^n + B(4^n)$$

 Try particular solution $s_n = \lambda n(4^n)$:

$$s_n = 3s_{n-1} + 4s_{n-2} + 4^n$$

$$\lambda n(4^n) = 3\lambda(n-1)(4^{n-1}) + 4\lambda(n-2)(4^{n-2}) + 4^n$$

$$\lambda n(4^n) = \frac{3}{4}\lambda(n-1)(4^n) + \frac{1}{4}\lambda(n-2)(4^n) + 4^n$$

$$\lambda n = \frac{3}{4}\lambda(n-1) + \frac{1}{4}\lambda(n-2) + 1$$

$$\lambda n = \frac{3}{4}\lambda n - \frac{3}{4}\lambda + \frac{1}{4}\lambda n - \frac{1}{2}\lambda + 1$$

$$\text{So } -\frac{5}{4}\lambda + 1 = 0 \Rightarrow \lambda = \frac{4}{5}$$

 So a particular solution is $\frac{4}{5}n(4^n)$, and the general solution is

$$s_n = A(-1)^n + B(4^n) + \frac{4}{5}n(4^n)$$

Write down the auxiliary equation and solve it.

Watch out

 You cannot use a particular solution of the form $\lambda(4^n)$ because the complementary function already features a 4^n term. Look for a particular solution of the form $\lambda n(4^n)$ instead.

 Substitute the particular solution into the full recurrence relation and solve to find λ .

This question only asks for the general solution, so leave your answer in this form with two arbitrary constants.

Exercise 4C

A

- 1 Consider the recurrence relation $u_n = 5u_{n-1} + 6u_{n-2}$. Verify that each of the following solutions satisfies this recurrence relation.

a $u_n = (-1)^n$

b $u_n = 6^n$

c $u_n = A(-1)^n + B(6^n)$, where A and B are arbitrary constants.

- 2 Consider the recurrence relation $u_n - 6u_{n-1} + 9u_{n-2} = 0$. Verify that each of the following solutions satisfies this recurrence relation.

a $u_n = 5(3^n)$

b $u_n = -n3^n$

c $u_n = 5(3^n) - n3^n$

- 3 Consider the recurrence relation $u_{n+2} + u_n = 0$. Verify that each of the following solutions satisfies this recurrence relation.

a $u_n = \cos\left(n\frac{\pi}{2}\right)$

b $u_n = \sin\left(n\frac{\pi}{2}\right)$

c $u_n = A\cos\left(n\frac{\pi}{2}\right) + B\sin\left(n\frac{\pi}{2}\right)$, where A and B are arbitrary constants.

- P 4 $u_n = F(n)$ and $u_n = G(n)$ are particular solutions to the linear homogeneous recurrence relation $u_n = au_{n-1} + bu_{n-2}$

Show that $u_n = cF(n) + dG(n)$ is also a solution, where c and d are arbitrary constants.

- 5 Find the general solution to each of the following recurrence relations.

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

b $u_n - 3u_{n-1} + 2u_{n-2} = 0$

c $x_n = 6x_{n-1} - 9x_{n-2}$

d $t_n = 4t_{n-1} - 5t_{n-2}$

Hint Your general solutions will each contain two arbitrary constants.

- P 6 The recurrence relation $u_{n+2} + au_{n+1} + bu_n = 0$, where a and b are real constants, has general solution $u_n = D + E(7^n)$, where D and E are arbitrary constants. Find the values of a and b .

- 7 Solve each of the following recurrence relations.

a $a_n = 5a_{n-1} - 6a_{n-2}$, with $a_0 = 2$ and $a_1 = 5$

b $u_n = 6u_{n-1} - 9u_{n-2}$, $n \geq 3$, with $u_1 = 2$ and $u_2 = 5$

c $s_n = 7s_{n-1} - 10s_{n-2}$, $n \geq 2$, with $s_0 = 4$ and $s_1 = 17$

d $u_n = 2u_{n-1} - 5u_{n-2}$, with $u_0 = 1$ and $u_1 = 5$

- E/P 8 A sequence satisfies the recurrence relation $u_n = 5u_{n-1} - 4u_{n-2}$, with $u_0 = 20$ and $u_1 = 19$.

a Solve the recurrence relation to find a closed form for u_n . (5 marks)

b Show that the sequence is decreasing, and that $u_n < 0$ for all $n \geq 3$. (3 marks)

- E/P 9 a Find a closed form for the sequence defined by the recurrence relation

$u_n = \sqrt{2}u_{n-1} - u_{n-2}$, with $u_0 = u_1 = 1$ (5 marks)

b Hence show that the sequence is periodic and state its period. (3 marks)

- E 10 The n th Lucas number L_n , is defined by $L_n = L_{n-1} + L_{n-2}$, $n \geq 3$, with $L_1 = 1$, $L_2 = 3$.

a List the first 7 terms of the sequence. (1 mark)

b Show that a closed form for the n th Lucas number is $L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$ (5 marks)

A 11 Find the general solution to each of the following recurrence relations.

- a $x_n = 5x_{n-1} - 6x_{n-2} + 1$ b $u_n - u_{n-1} - 2u_{n-2} = 2n$
 c $a_{n+2} + 4a_{n+1} + 3a_n = 5(-2)^n$ d $a_{n+2} + 4a_{n+1} + 3a_n = 12(-3)^n$
 e $a_{n+2} - 6a_{n+1} + 9a_n = 3^n$ f $u_n = 7u_{n-1} - 10u_{n-2} + 6 + 8n$

12 Solve each of the following recurrence relations.

- a $u_n = 2u_{n-1} + 3u_{n-2} + 1$, $n \geq 3$, with $u_1 = 3$ and $u_2 = 7$
 b $a_{n+1} - 3a_n + 2a_{n-1} = 6(-1)^n$, with $a_0 = a_1 = 12$
 c $u_n = 3u_{n-1} + 10u_{n-2} + 7 \times 5^n$, $n \geq 2$, with $u_0 = 4$ and $u_1 = 3$
 d $x_n = 10x_{n-1} - 25x_{n-2} + 8 \times 5^n$, $n \geq 2$, with $x_0 = 6$ and $x_1 = 10$

Problem-solving

Each of these recurrence relations will require a particular solution. Look at the table on page x to determine the correct form for the particular solution.

E/P 13 Consider the recurrence relation $b_{n+2} + 4b_{n+1} + 4b_n = 7$.

- a Find a constant k such that $b_n = k$ is a particular solution to this recurrence relation. (2 marks)
 b Hence or otherwise, solve the recurrence relation given that $b_0 = 1$ and $b_1 = 2$. (5 marks)

E/P 14 a Find the general solution to the recurrence relation $u_n = 7u_{n-1} - 6u_{n-2} + 75$. (4 marks)

- b Given that $u_0 = u_1 = 2$, find the particular solution. (3 marks)

E/P 15 Consider the recurrence relation $u_{n+2} - 6u_{n+1} + 9u_n = 7(3^n)$.

- a Find a value of k such that $u_n = kn^2(3^n)$ is a particular solution to this recurrence relation. (2 marks)
 b Find the general solution to $u_{n+2} - 6u_{n+1} + 9u_n = 0$. (3 marks)
 c Hence, find the solution to $u_{n+2} - 6u_{n+1} + 9u_n = 7(3^n)$ given that $u_0 = 1$ and $u_1 = 4$. (3 marks)

E/P 16 A sequence of numbers satisfies the recurrence relation $u_n = u_{n-1} - u_{n-2}$, $n \geq 2$.

- a Given that $u_0 = 0$ and $u_1 = 3$, show the solution to this recurrence relation can be written in the form $u_n = p \sin qn$, where p and q are exact real constants to be determined. (6 marks)
 b Hence explain why the sequence u_n is periodic, and state its period. (2 marks)

E/P 17 A monkey sits at a typewriter and types strings of random letters. Unfortunately, the typewriter is broken, so the only keys that work are the letters A, B and C.

- a Find the number of different strings of length 3 which do not contain consecutive letter As. (2 marks)

The number of different strings of length n which do not contain consecutive letter As is given by s_n .

- b Find a recurrence relation for s_n in terms of s_{n-1} and s_{n-2} . (3 marks)
 c i Solve your recurrence relation.
 ii Find the number of strings of length 20 which do not contain consecutive letter As. (3 marks)

Challenge

- 1 Solve the recurrence relation $u_n = \sqrt{\frac{u_{n-2}}{u_{n-1}}}$, $u_0 = 8$, with $u_1 = \frac{1}{2\sqrt{2}}$
 2 The sequence u_n satisfies the recurrence relation $u_n = au_{n-1} + bu_{n-2}$, with $u_0 = 0$ and $u_1 = k$, where a , b and k are real constants, and $k \neq 0$. Find values of a and b such that the sequence is periodic with period 12, and state the maximum and minimum values in the sequence in terms of k .

Hint

Take logs of both sides, and then use a suitable substitution to form a linear recurrence relation.

4.4 Proving closed forms

You can prove that a closed form satisfies a given recurrence relation using mathematical induction.

Example 21

The minimum number of moves, d_n , needed to transfer n disks from one peg to another in the Tower of Hanoi problem is given by the recurrence relation $d_n = 2d_{n-1} + 1$, with $d_1 = 1$.

Prove, by induction, that $d_n = 2^n - 1$.

Basis step:

When $n = 1$, $d_1 = 2^1 - 1 = 1$.

So the closed form is true for $n = 1$.

Assumption step:

Assume the closed form is true for $n = k$.

So $d_k = 2^k - 1$.

Inductive step:

Using the recurrence relation,

$$\begin{aligned} d_{k+1} &= 2d_k + 1 = 2(2^k - 1) + 1 \\ &= 2 \times 2^k - 2 \times 1 + 1 = 2^{k+1} - 1 \end{aligned}$$

So true for $n = k \Rightarrow$ true for $n = k + 1$, and true for $n = 1$. Therefore, by induction, the closed form $d_n = 2^n - 1$ is true for all $n \in \mathbb{N}$.

You are given that $d_1 = 1$. Use this to prove the basis step.

You need to assume that the closed form is true for $n = k$, then use the recurrence relation to show that it is true for $n = k + 1$.

← Core Pure Book 1, Chapter 8

Keep in mind what you are aiming to show. In this case, you need to show that $d_{k+1} = 2^{k+1} - 1$.

Replace d_k with its assumed value of $2^k - 1$.

Remember to write a conclusion, and state that you have used induction.

Example 22

A sequence u_n satisfies the recurrence relation $u_n = u_{n-1} + n$, with $u_0 = 0$.

Prove by induction that $u_n = \frac{n(n+1)}{2}$, $n \geq 0$.

Basis step:

When $n = 0$, $u_1 = \frac{0(0+1)}{2} = 0$.

So the closed form is true for $n = 0$.

Assumption step:

Assume the closed form is true for $n = k$:

$$u_k = \frac{k(k+1)}{2}$$

Inductive step:

Using the recurrence relation $u_k = u_{k-1} + k$,

$$\begin{aligned} u_{k+1} &= u_k + k + 1 = \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2} \end{aligned}$$

So true for $n = k \Rightarrow$ true for $n = k + 1$, and true for $n = 1$. Therefore, by induction, the closed form $u_n = \frac{n(n+1)}{2}$ is true for all $n \in \mathbb{N}$.

$u_0 = 0$ is given, so you can begin your induction at $n = 0$.

Replace u_k by its assumed value of $\frac{k(k+1)}{2}$

Keep in mind what you are aiming to show. In this case you need to show that $u_{k+1} = \frac{(k+1)(k+2)}{2}$

A You can adapt the technique of proof by mathematical induction to prove closed forms for second-order recurrence relations.

■ **When you are proving the closed form of a second-order recurrence relation by mathematical induction, you need to:**

- show that the closed form is true for two consecutive values of n (basis step)
- assume that the closed form is true for $n = k$ and $n = k - 1$ (assumption step), then show that it is true for $n = k + 1$ (inductive step).

Example 23

A sequence a_n satisfies the recurrence relation $a_n = 2a_{n-1} + 8a_{n-2}$, with $a_0 = 4$, $a_1 = 10$. Prove by induction that $a_n = 3(4^n) + (-2)^n$ for all non-negative integers n .

Basis step:

When $n = 0$, $a_0 = 3 \times 4^0 + (-2)^0 = 3 \times 1 + 1 = 4$
 When $n = 1$, $a_1 = 3 \times 4^1 + (-2)^1 = 12 - 2 = 10$
 So the closed form is true for $n = 0$ and $n = 1$.

Assumption step:

Assume the closed form is true for $n = k$ and $n = k - 1$:

$$a_k = 3(4^k) + (-2)^k \text{ and } a_{k-1} = 3(4^{k-1}) + (-2)^{k-1}$$

Inductive step:

Using the recurrence relation $a_k = 2a_{k-1} + 8a_{k-2}$

$$\begin{aligned} a_{k+1} &= 2a_k + 8a_{k-1} \\ &= 2(3(4^k) + (-2)^k) + 8(3(4^{k-1}) + (-2)^{k-1}) \\ &= 2(3(4^k) + (-2)^k) + 8(3(4^{k-1}) + (-2)^{k-1}) \\ &= 6(4^k) + 2(-2)^k + 24(4^{k-1}) + 8(-2)^{k-1} \\ &= 6(4^k) - 2(-2)^{k+1} + 6(4^k) + 2(-2)^{k+1} \\ &= 12(4^k) + (-2)^{k+1} = 3(4^{k+1}) + (-2)^{k+1} \end{aligned}$$

So true for $n = k$ and $n = k - 1 \Rightarrow$ true for $n = k + 1$, and true for $n = 0$ and $n = 1$.

Therefore, by induction, the closed form for the n th term, $a_n = 3(4^n) + (-2)^n$, is true for all non-negative integers.

Show that the closed form is true for **two consecutive** values of n . You are given $a_0 = 4$ and $a_1 = 10$, so substitute $n = 0$ and $n = 1$ into the closed form.

Keep in mind what you are aiming to show. In this case you need to show that $a_{k+1} = 3(4^{k+1}) + (-2)^{k+1}$

Replace a_k with its assumed value of $3(4^k) + (-2)^k$ and a_{k-1} with its assumed value of $3(4^{k-1}) + (-2)^{k-1}$

Simplify and factorise. Simplify by replacing $+2(-2)^k$ with $-(-2)(-2)^k = -(-2)^{k+1}$, $24(4^{k-1})$ with $6(4^k)$ and $8(-2)^{k-1}$ with $2(-2)^2(-2)^{k-1} = 2(-2)^{k+1}$

Example 24

The Fibonacci sequence is defined recursively by

$$u_n = u_{n-1} + u_{n-2}, n > 2, \text{ with } u_1 = u_2 = 1$$

Show that the closed form for the n th term of the Fibonacci sequence is given by

$$u_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \sqrt{5}}, n > 2$$

A

Basis step:

$$\text{When } n = 1, u_1 = \frac{(1 + \sqrt{5})^1 - (1 - \sqrt{5})^1}{2\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1$$

$$\begin{aligned} \text{When } n = 2, u_2 &= \frac{(1 + \sqrt{5})^2 - (1 - \sqrt{5})^2}{2^2\sqrt{5}} \\ &= \frac{1 + 2\sqrt{5} + 5 - 1 + 2\sqrt{5} - 5}{4\sqrt{5}} = \frac{4\sqrt{5}}{4\sqrt{5}} = 1 \end{aligned}$$

So the closed form is true for $n = 1$ and $n = 2$.

Assumption step:

Assume the closed form is true for $n = k - 1$ and $n = k$.

$$\text{So } u_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k\sqrt{5}} \text{ and } u_{k-1} = \frac{(1 + \sqrt{5})^{k-1} - (1 - \sqrt{5})^{k-1}}{2^{k-1}\sqrt{5}}$$

Inductive step:

Using the recurrence relation $u_{k+1} = u_k + u_{k-1}$,

$$\begin{aligned} u_{k+1} &= \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k\sqrt{5}} + \frac{(1 + \sqrt{5})^{k-1} - (1 - \sqrt{5})^{k-1}}{2^{k-1}\sqrt{5}} \\ &= \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k + 2(1 + \sqrt{5})^{k-1} - 2(1 - \sqrt{5})^{k-1}}{2^k\sqrt{5}} \\ &= \frac{((1 + \sqrt{5})^k + 2(1 + \sqrt{5})^{k-1}) - ((1 - \sqrt{5})^k + 2(1 - \sqrt{5})^{k-1})}{2^k\sqrt{5}} \\ &= \frac{(1 + \sqrt{5})^k \left(1 + \frac{2}{1 + \sqrt{5}}\right) - (1 - \sqrt{5})^k \left(1 + \frac{2}{1 - \sqrt{5}}\right)}{2^k\sqrt{5}} \\ &= \frac{(1 + \sqrt{5})^k \left(\frac{1 + \sqrt{5}}{2}\right) - (1 - \sqrt{5})^k \left(\frac{1 - \sqrt{5}}{2}\right)}{2^k\sqrt{5}} \\ &= \frac{(1 + \sqrt{5})^{k+1} - (1 - \sqrt{5})^{k+1}}{2^{k+1}\sqrt{5}} \end{aligned}$$

So true for $n = k - 1$ and $n = k \Rightarrow$ true for $n = k + 1$, and true for $n = 1$ and $n = 2$. Therefore, by induction, the closed form for the n th term of Fibonacci sequence,

$$u_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n\sqrt{5}}, \text{ is true for all } n \in \mathbb{N}.$$

Watch out

This is a second-order recurrence relation, so to prove it by induction you need to show that it is true for $n = 1$ **and** $n = 2$ as your basis step. You then assume it is true for $n = k - 1$ and $n = k$ and show that it is true for $n = k + 1$.

Keep in mind what you are aiming to show. In this case you need to show that

$$u_{k+1} = \frac{(1 + \sqrt{5})^{k+1} - (1 - \sqrt{5})^{k+1}}{2^{k+1}\sqrt{5}}$$

Look for factors of $(1 + \sqrt{5})$ and $(1 - \sqrt{5})$.

You must write down a conclusion statement, and state that you are using mathematical induction.

Exercise 4D

- (P) 1 Given that $u_{n+1} = 5u_n + 4$, with $u_1 = 4$, prove by induction that $u_n = 5^n - 1$.
- (P) 2 Given that $u_{n+1} = 2u_n + 5$, with $u_1 = 3$, prove by induction that $u_n = 2^{n+2} - 5$.
- (P) 3 Given that $u_{n+1} = 5u_n - 8$, with $u_1 = 3$, prove by induction that $u_n = 5^{n-1} + 2$.
- (P) 4 Given that $u_{n+1} = 3u_n + 1$, with $u_1 = 1$, prove by induction that $u_n = \frac{3^n - 1}{2}$.
- (E/P) 5 A sequence $u_1, u_2, u_3, u_4, \dots$ is defined by $u_{n+1} = \frac{3u_n - 1}{4}$, with $u_1 = 2$.

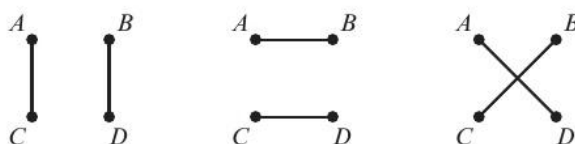
a Find the first four terms of the sequence.

(1 mark)

b Prove, by induction for $n \in \mathbb{Z}^+$, that $u_n = 4\left(\frac{3}{4}\right)^n - 1$.

(5 marks)

- E/P** 6 Given that $u_{n+1} = 4u_n - 9n$, with $u_1 = 8$, use mathematical induction to prove that $u_n = 4^n + 3n + 1$, $n \in \mathbb{Z}^+$. (5 marks)
- E/P** 7 Given that $u_{n+1} = 2n - u_n$, with $u_1 = 0$, use mathematical induction to prove that $2u_n = 2n - 1 + (-1)^n$, $n \in \mathbb{Z}^+$. (5 marks)
- E/P** 8 Given that $2u_{n+1} + u_n = 6$, with $u_1 = 4$, use mathematical induction to prove that $u_n = 2 - \left(-\frac{1}{2}\right)^{n-2}$, $n \in \mathbb{Z}^+$. (5 marks)
- E/P** 9 Given that $u_n = 3nu_{n-1}$, with $u_1 = 1$, use mathematical induction to prove that $u_n = 3^{n-1}n!$ (5 marks)
- E/P** 10 The diagram shows the three different ways that 4 people can be paired up.



Let P_n be the number of ways of pairing up a group of $2n$ people, so that $P_1 = 1$ and $P_2 = 3$.

- a Explain why P_n satisfies the recurrence relation $P_n = (2n - 1)P_{n-1}$ (3 marks)
- b Hence prove by induction that $P_n = \frac{(2n)!}{2^n n!}$ for all $n \in \mathbb{Z}^+$. (5 marks)
- A** 11 Given that $u_{n+2} = 5u_{n+1} - 6u_n$, with $u_1 = 1$ and $u_2 = 5$, prove by induction that $u_n = 3^n - 2^n$.
- P** 12 Given that $u_{n+2} = 6u_{n+1} - 9u_n$, with $u_1 = -1$ and $u_2 = 0$, prove by induction that $u_n = (n - 2)3^{n-1}$.
- P** 13 Given that $u_{n+2} = 7u_{n+1} - 10u_n$, with $u_1 = 1$ and $u_2 = 8$, prove by induction that $u_n = 2(5^{n-1}) - 2^{n-1}$.
- P** 14 Given that $u_{n+2} = 6u_{n+1} - 9u_n$, $u_1 = 3$ and $u_2 = 36$ prove by induction that $u_n = (3n - 2)3^n$.
- E/P** 15 A sequence $u_1, u_2, u_3, u_4, \dots$ is defined by $u_{n+1} = 5u_n - 3(2^n)$, with $u_1 = 7$.
- a Find the first four terms of the sequence. (1 mark)
- b Prove, by induction for $n \in \mathbb{Z}^+$, that $u_n = 5^n + 2^n$. (7 marks)
- E/P** 16 The n th Lucas number L_n , is defined as follows.
- $$L_n = L_{n-1} + L_{n-2}, n \geq 3, \text{ with } L_1 = 1 \text{ and } L_2 = 3.$$
- Use mathematical induction to prove that the closed form for Lucas numbers is
- $$L_n = \left(\frac{1 + \sqrt{5}}{2}\right)^n + \left(\frac{1 - \sqrt{5}}{2}\right)^n \quad (7 \text{ marks})$$

Mixed exercise 4

- E** 1 Solve the recurrence relation $u_n - 2u_{n-1} + 1 = 0$, with $u_0 = 4$. (3 marks)
- E/P** 2 a Solve the recurrence relation $u_n = u_{n-1} - n$, with $u_0 = 2000$. (3 marks)
- b Hence, or otherwise, find the first negative term of the sequence. (2 marks)

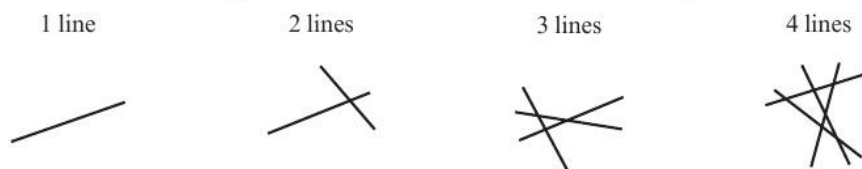
- E/P** 3 a Solve the recurrence relation $u_n = 3u_{n-1} + 5$, with $u_0 = 0$. (3 marks)
 b Find u_{10} . (1 mark)
 c Find the first term of the sequence to exceed 10 million. (2 marks)

- E/P** 4 At the end of each year, a sustainable lumber company harvests 20% of its trees. To replace this stock they plant 1000 new trees. At the beginning of the first year, the company has 12 000 trees. Let T_n represent the number of trees remaining at the end of the n th year.
 a Explain why the number of trees owned by the company can be modelled by the recurrence relation $T_n = 0.8T_{n-1} + 1000$, with $T_0 = 12000$. (3 marks)
 b Solve this recurrence relation to find a closed form for T_n . (3 marks)
 c In the long run, how many trees can the lumber company expect to have at the end of each year? (1 mark)

- E/P** 5 At a salmon farm, the population of salmon increases by 25% each month. At the end of each month, X salmon are removed for sale. At the beginning of the first month there are 2000 salmon in the farm. Let S_n represent the number of salmon remaining at the end of the n th month.
 a Explain why the number of salmon in the farm can be modelled by the recurrence relation $S_n = \frac{5S_{n-1} - 4X}{4}$, with $S_0 = 2000$. (3 marks)
 b Prove, by induction, that $S_n = \left(\frac{5}{4}\right)^n (2000 - 4X) + 4X$, $n \geq 0$ (5 marks)
 c Explain how the long-term population of the fish farm varies for different values of X . (2 marks)

- E/P** 6 The Smiths buy a new house in March 2018, costing £200 000. They have a deposit of £25 000. At the end of each month, interest of 0.25% is added to the balance, and the Smiths' monthly payment of £1200 is deducted from the balance.
 a Write a recurrence relation showing the balance in pounds, b_n , at the end of the n th month. (3 marks)
 b By solving your recurrence relation, determine the year in which the Smiths will pay off their mortgage. (5 marks)

- E/P** 7 The diagrams show intersecting lines drawn on a two-dimensional plane.

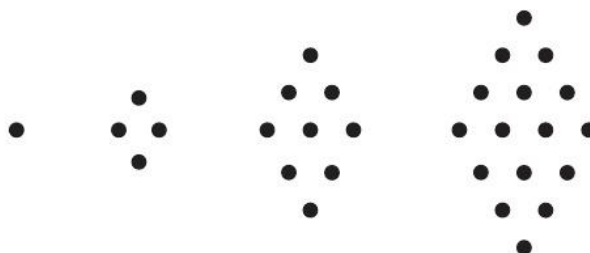


Assuming that all the lines are non-parallel, and that no three lines intersect at a common point, the number of points of intersection when n lines are drawn, P_n , is given by

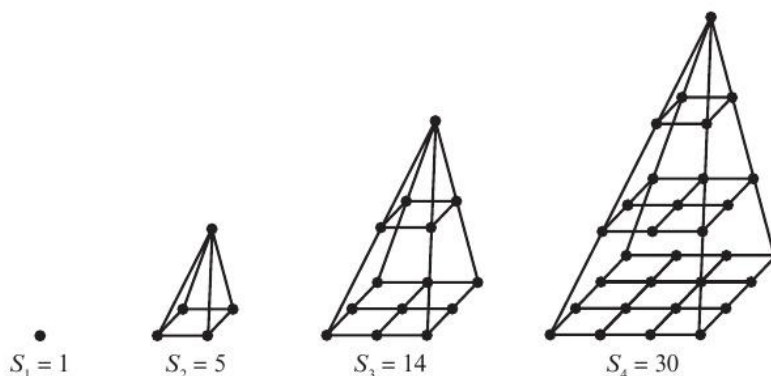
$$P_1 = 0, \quad P_2 = 1, \quad P_3 = 3$$

- a Use the diagram above to write down the value of P_4 . (1 mark)
 b By forming and solving a suitable recurrence relation, show that $P_n = \frac{1}{2}n(n-1)$. (4 marks)
 c Hence find the number of intersections formed when 100 such lines are drawn on the plane. (1 mark)

- E/P** 8 A sequence of patterns is formed by drawing dots in the shape of a rhombus, as shown in the diagram. The number of dots needed to draw the n th shape is represented by t_n .



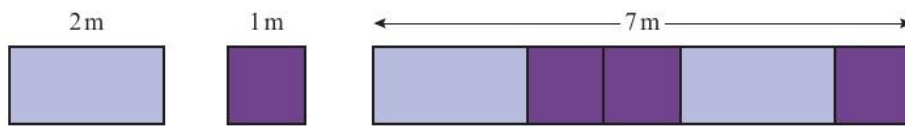
- a Write down the values of t_5 , t_6 , and t_7 . (1 mark)
- b Find in term of t_{n-1} , the recurrence relation for t_n . (2 marks)
- c Solve your recurrence relation for t_n , and hence determine the number of dots in the 100th pattern. (3 marks)
- E/P** 9 a Calculate $\begin{pmatrix} 1 & p \\ 0 & q \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 3 \end{pmatrix}$, giving your answer as a 2×2 matrix with elements given in terms of p and q . (3 marks)
- b Given that $\begin{pmatrix} 1 & 4 \\ 0 & 3 \end{pmatrix}^n = \begin{pmatrix} 1 & a_n \\ 0 & b_n \end{pmatrix}$, write down recurrence relations for a_n in terms of a_{n-1} and b_n in terms of b_{n-1} . (2 marks)
- c Solve your recurrence relations, and hence find $\begin{pmatrix} 1 & 4 \\ 0 & 3 \end{pmatrix}^n$, giving your answer as a 2×2 matrix with elements given in terms of n . (4 marks)
- E/P** 10 Square pyramidal numbers S_n are positive integers that can be represented by square pyramidal shapes. The first four square pyramidal numbers are 1, 5, 14, and 30, as shown in the diagram below.



- a Write down S_5 , S_6 , and S_7 . (1 marks)
- b Find a recurrence relation for S_n in terms of S_{n-1} . (2 marks)
- c Solve your recurrence relation to find a closed form for S_n . (3 marks)
- E/P** 11 A sequence of numbers is defined by $u_n = (n^2 + n)u_{n-1}$, with $u_1 = 1$. Prove, by induction, that $u_n = \frac{1}{2}n!(n+1)!$ (5 marks)
- E/P** 12 A sequence of numbers is defined by $u_n = (n+2)u_{n-1}$, with $u_1 = 1$. Prove, by induction, that $u_n = \frac{(n+2)!}{6}$ (5 marks)

- E/P** 13 In a drug trial, a bacterial population is modelled as increasing at a rate of 20% each hour. A proposed antibacterial agent is introduced, and kills bacteria at a rate of $k(2^n)$ bacteria per hour, where k is a measure of the concentration of the agent. At the beginning of the trial there are 100 bacteria present, and after n hours there are u_n bacteria present.
- Form a recurrence relation for u_n in terms of u_{n-1} , stating the initial condition. (2 marks)
 - Show that $u_n = \left(100 + \frac{5k}{2}\right)(1.2^n) - \frac{5k}{2}(2^n)$ (5 marks)

- A** 14 Flagstones come in two different sizes. Large flagstones have a length of 2 m, and small flagstones have a length of 1 m. The diagram shows a large and small flagstone, and a path of length 7 m made from a combination of these flagstones.



Let f_n represent the number of ways in which a path of length n m can be made from a combination of large and small flagstones.

- Draw the three possible paths of length 3 m. (1 mark)
- Explain why f_n satisfies the recurrence relation

$$f_n = f_{n-1} + f_{n-2}, \text{ with } f_1 = 1 \text{ and } f_2 = 2 \quad (3 \text{ marks})$$

A path of length 200 m is to be made.

- Show that the number of ways in which this path could be constructed is given by

$$\frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{201} - \left(\frac{1 - \sqrt{5}}{2} \right)^{201} \right) \quad (5 \text{ marks})$$

- E/P** 15 A **ternary string** is a sequence of digits, where each digit can be either 0, 1 or 2. There are 8 different ternary strings of length 2 which **do not** contain consecutive 0s. 01, 10, 02, 20, 11, 12, 21, 22

Let t_n represent the number of ternary strings of length n with no consecutive 0s.

- Find t_2 and t_3 . (1 mark)
- Explain why t_n satisfies the recurrence relation $t_n = 2t_{n-1} + 2t_{n-2}$. (3 marks)
- Find t_6 . (1 mark)
- Find:
 - a closed form for t_n in terms of n
 - the number of different ternary strings length 15 which do not contain consecutive 0s. (5 marks)

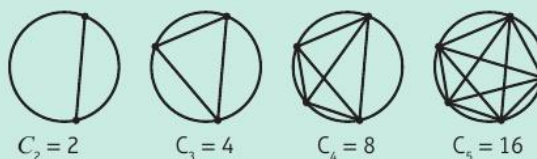
- E** 16 a Find the general solution to the recurrence relation $u_{n+2} = u_{n+1} + 2u_n, n \geq 1$ (3 marks)
- Given that $u_1 = 1$ and $u_2 = 2$, find the particular solution to the recurrence relation. (3 marks)

- E/P** 17 a Find the general solution to the recurrence relation $x_{n+2} = 7x_{n+1} - 10x_n + 3, n \geq 1$ (4 marks)
- Given that $x_1 = 1$ and $x_2 = 2$, find the particular solution to the recurrence relation. (3 marks)

- A** 18 Solve the recurrence relation $a_n = 2a_{n-1} + 15a_{n-2} + 2^n$, with $a_1 = 2$ and $a_2 = 4$. (8 marks)
- E/P** 19 A sequence satisfies the recurrence relation $u_n = -2nu_{n-1} + 3n(n-1)u_{n-2}$, with $u_0 = 1$ and $u_1 = 2$.
Prove, by induction, that a closed form for this sequence is $u_n = \frac{n!}{4}(5 - (-3)^n)$ (7 marks)
- E/P** 20 a Find a closed form for the sequence defined by the recurrence relation $u_n = \sqrt{2}u_{n-1} - u_{n-2}$, with $u_0 = u_1 = 1$ (5 marks)
b Hence show that the sequence is periodic and state its period. (3 marks)
- E/P** 21 Messages are transmitted over a network using two types of signal packet. Type *A* signal packets require 1 microsecond to transmit, and type *B* signal packets require 2 microseconds to transmit. The packets are transmitted consecutively with no gaps between them. The number of different messages consisting of sequences of these two types of signal packet that can be sent in n microseconds is denoted by S_n .
a Write a recurrence relation for S_{n+2} in terms of S_{n+1} and S_n . State the initial conditions for your recurrence relation. (3 marks)
b Solve your recurrence relation to find an expression for S_n in terms of n . (5 marks)

Challenge

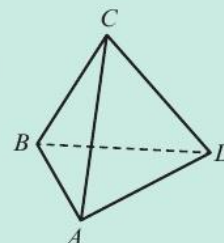
- 1 The circles in the diagram have been subdivided into regions by drawing all possible chords between points drawn on the circumference of the circle. Let C_n denote the maximum number of regions that are formed in this way when n points are drawn on the circumference of a circle.



- a Find C_6 .
b Explain why it is always possible to choose a new point on the circumference of the circle such that all the new chords drawn from that point do not intersect the existing chords at any existing points of intersection.
c Find, in terms of C_{n-1} and n , a recurrence relation for C_n .
d Solve your recurrence relation, and hence determine the maximum number of regions created by 100 points.

- 2 The diagram shows a tetrahedron $ABCD$. A spider walks along the edges of the tetrahedron, starting and ending at vertex A . A walk of length n traverses exactly n edges, so that there are three possible walks of length 2:

$A \rightarrow B \rightarrow A$
 $A \rightarrow C \rightarrow A$
 $A \rightarrow D \rightarrow A$



- a Explain why there are no possible walks of length 1.
b Find the number of possible walks of length 3.
c By formulating and solving a suitable recurrence relation find a closed form for the total number of possible walks of length n .

Summary of key points

- 1 A recurrence relation is an equation that defines a sequence based on a rule that gives the each term as a function of the previous term(s).
- 2 The **order** of a recurrence relation is the difference between the highest and lowest subscript in the relation.
- 3 A sequence u_n is called a **solution** of a recurrence relation if its terms satisfy the recurrence relation. It is also called the **closed form** of the sequence.
- 4 A **first-order** recurrence relation is one in which u_n can be given as a function of n and u_{n-1} only.
- 5 A **first-order linear** recurrence relation can be written in the form $u_n = au_{n-1} + g(n)$.
 - If $g(n) = 0$, then the equation is homogeneous.
 - The solution to the first-order homogeneous linear recurrence relation $u_n = au_{n-1}$ is given by $u_n = u_0a^n$ or $u_n = u_1a^{n-1}$.
 - The solution to the first-order non-homogeneous linear recurrence relation $u_n = u_{n-1} + g(n)$ is given by $u_n = u_0 + \sum_{r=1}^n g(r)$.
 - When solving a recurrence relation of the form $u_n = au_{n-1} + g(n)$, the form of the particular solution will depend on $g(n)$:

Form of $g(n)$	Form of particular solution
p with $a \neq 1$	λ
$pn + q$ with $a \neq 1$	$\lambda n + \mu$
kp^n with $p \neq a$	λk^n
ka^n	λna^n

- 6 To solve the recurrence relation $u_n = au_{n-1} + g(n)$,
 - Find the complementary function, which is the general solution to the associated homogeneous recurrence relation $u_n = au_{n-1}$.
 - Choose an appropriate form for a particular solution then substitute into the original recurrence relation to find the values of any coefficients.
 - The general solution is $u_n = \text{C.F.} + \text{P.S.} = ca^n + \text{P.S.}$
 - Use the initial condition to find the value of the arbitrary constant.
- 7 If $u_n = F(n)$ and $u_n = G(n)$ are particular solutions to a linear recurrence relation, then $u_n = aF(n) + bG(n)$, where a and b are constants, is also a solution.
- 8 A **second-order linear** recurrence relation can be written in the form $u_n = au_{n-1} + bu_{n-2} + g(n)$, where a and b are real constants.
 - If $g(n) = 0$, then the equation is homogeneous.
- 9 You can find a general solution to a **second-order homogeneous** linear recurrence relation, $u_n = au_{n-1} + bu_{n-2}$, by considering the auxiliary equation, $r^2 - ar - b = 0$. You need to consider three different cases:

A

Case 1: Distinct real roots

If the auxiliary equation has distinct real roots α and β , then the general solution will have the form $u_n = A\alpha^n + B\beta^n$ where A and B are arbitrary constants.

Case 2: Repeated root

If the auxiliary equation has a repeated real root α , then the general solution will have the form $u_n = (A + Bn)\alpha^n$ where A and B are arbitrary constants.

Case 3: Complex roots

If the auxiliary equation has two complex roots $\alpha = re^{i\theta}$ and $\beta = re^{-i\theta}$, then the general solution will have the form $u_n = r^n(A \cos n\theta + B \sin n\theta)$, or $u_n = A\alpha^n + B\beta^n$, where A and B are arbitrary constants.

10 To solve the recurrence relation $u_n = au_{n-1} + bu_{n-2} + g(n)$,

- Find the complementary function, which is the general solution to the associated homogeneous recurrence relation $u_n = au_{n-1} + bu_{n-2}$.
- Choose an appropriate form for a particular solution then substitute into the original recurrence relation to find the values of any coefficients.
- The general solution is $u_n = \text{C.F.} + \text{P.S.}$
- Use the initial conditions to find the values of the arbitrary constants.

11 For the recurrence relation $u_n = au_{n-1} + bu_{n-2} + g(n)$, with auxiliary equation with roots α and β , try the following forms for a particular solution:

Form of $g(n)$	Form of particular solution
p with $\alpha, \beta \neq 1$	λ
$pn + q$, with $\alpha, \beta \neq 1$	$\lambda n + \mu$
kp^n with $p \neq \alpha, \beta$	λp^n
p with $\alpha = 1, \beta \neq 1$	λn
$pn + q$ with $\alpha = 1, \beta \neq 1$	$\lambda n^2 + \mu n$
p with $\alpha = \beta = 1$	λn^2
$pn + q$ with $\alpha = \beta = 1$	$\lambda n^3 + \mu n^2$
$k\alpha^n$ with $\alpha \neq \beta$	$\lambda n\alpha^n$
$k\alpha^n$ with $\alpha = \beta$	$\lambda n^2\alpha^n$

12 You can prove that a closed form satisfies a given recurrence relation using mathematical induction.

13 When you are proving the closed form of a second-order recurrence relation by mathematical induction, you need to:

- show that the closed form is true for two consecutive values of n (basis step)
- assume that the closed form is true for $n = k$ and $n = k - 1$ (assumption step), then show that it is true for $n = k + 1$ (inductive step).

Matrix algebra

5

Objectives

After completing this chapter you should be able to:

- Find the eigenvalues of a matrix → pages 000–000
- Find the eigenvectors of a matrix → pages 000–000
- Reduce matrices to diagonal form → pages 000–000
- Understand and use the Cayley–Hamilton theorem → pages 000–000

Reducing a given matrix to diagonal form can help to solve a system of coupled differential equations in a problem involving a closed ecosystem such as a predator–prey model.

← Core Pure Book 2, Chapter 8
→ Exercise 5C, Challenge

Prior knowledge check

1 Find the determinants of the following matrices.

a $\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$

b $\begin{pmatrix} 1 & 2 & 3 \\ -1 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix}$

← Core Pure Book 1,
Chapter 6

2 $\mathbf{A} = \begin{pmatrix} -3 & k \\ 2 & -4 \end{pmatrix}$

Find the value of k such that the matrix $\mathbf{A}$ is singular.

← Core Pure Book 1, Chapter 6

3 The matrix $\begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ represents a transformation.

Show that the line with equation $3y + 2x = 0$ is invariant under this transformation. ← Core Pure Book 1, Section 7.2

5.1 Eigenvalues and eigenvectors

You need to be able to find the **eigenvectors** and **eigenvalues** associated with a square matrix.

- An **eigenvector** of a matrix **A** is a non-zero column vector **x** which satisfies the equation

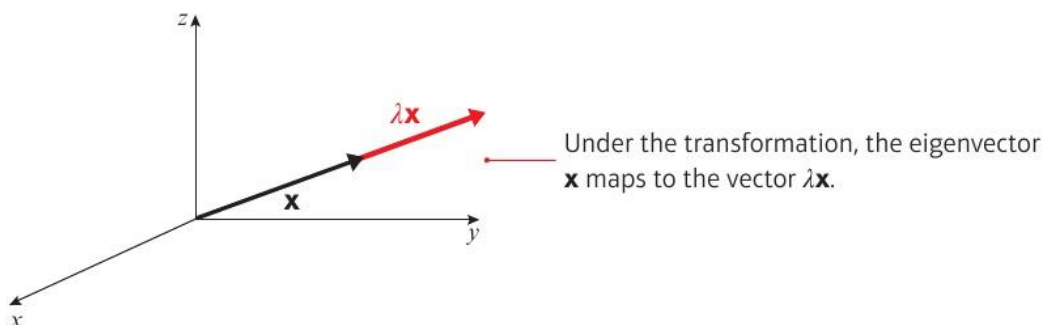
$$\mathbf{Ax} = \lambda \mathbf{x}$$

where λ is a scalar.

- The value of the scalar λ is the **eigenvalue** of the matrix corresponding to the eigenvector **x**.

Notation The word **eigen** is German and means 'particular' or 'special'.

The magnitude of an eigenvector may be changed by the linear transformation represented by the matrix but the direction of the eigenvector is unchanged or **invariant**. The eigenvalue can be interpreted as the magnification factor of the eigenvector under the transformation.



- If **x** is an eigenvector of a matrix **M** representing a linear transformation, then the straight line that passes through the origin in the direction of **x** is an **invariant line** under that transformation.

If the corresponding eigenvalue is 1, then every point on this line is an invariant point.

If **x** is an eigenvector of the matrix **A** then, by definition

$$\mathbf{Ax} = \lambda \mathbf{x} = \lambda \mathbf{Ix}$$

Rearranging,

$$\mathbf{Ax} - \lambda \mathbf{Ix} = (\mathbf{A} - \lambda \mathbf{I})\mathbf{x} = \mathbf{0}$$

As by definition **x** is non-zero, the matrix $(\mathbf{A} - \lambda \mathbf{I})$ is singular and has determinant zero, that is

$$\det(\mathbf{A} - \lambda \mathbf{I}) = 0$$

Note You can show that if matrix **M** is such that $\mathbf{Mx} = \mathbf{0}$ and **x** is non-zero, then **M** is singular. → Exercise 5A, Q12

This means that if you can find a scalar λ that satisfies this equation, then it will be an eigenvalue of **A**.

- The equation $\det(\mathbf{A} - \lambda \mathbf{I}) = 0$ is called the **characteristic equation** of **A**. The solutions to the characteristic equation are the **eigenvalues** of **A**.

In the case of a 2×2 matrix, the characteristic equation is quadratic.

Example 1

Find the eigenvalues and corresponding eigenvectors of the matrix $\mathbf{A} = \begin{pmatrix} 2 & 5 \\ -1 & -4 \end{pmatrix}$.

$$\begin{aligned}\mathbf{A} - \lambda \mathbf{I} &= \begin{pmatrix} 2 & 5 \\ -1 & -4 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 5 \\ -1 & -4 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 2 - \lambda & 5 \\ -1 & -4 - \lambda \end{pmatrix}\end{aligned}$$

$$\begin{aligned}\det(\mathbf{A} - \lambda \mathbf{I}) &= \begin{vmatrix} 2 - \lambda & 5 \\ -1 & -4 - \lambda \end{vmatrix} \\ &= (2 - \lambda)(-4 - \lambda) - 5 \times (-1) \\ &= -8 - 2\lambda + 4\lambda + \lambda^2 + 5 \\ &= \lambda^2 + 2\lambda - 3\end{aligned}$$

$$\begin{aligned}\det(\mathbf{A} - \lambda \mathbf{I}) = 0 &\Rightarrow \lambda^2 + 2\lambda - 3 = 0 \\ &(\lambda - 1)(\lambda + 3) = 0 \\ &\lambda = 1 \text{ or } -3\end{aligned}$$

The eigenvalues of $\mathbf{A}$ are 1 and -3 .

Find an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue 1:

$$\begin{aligned}\begin{pmatrix} 2 & 5 \\ -1 & -4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &= 1 \begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} 2x + 5y \\ -x - 4y \end{pmatrix} &= \begin{pmatrix} x \\ y \end{pmatrix}\end{aligned}$$

Equating the upper elements,

$$2x + 5y = x$$

$$\Rightarrow x = -5y$$

$$\text{Let } y = 1, \text{ then } x = -5 \times 1 = -5$$

An eigenvector corresponding to 1 is $\begin{pmatrix} -5 \\ 1 \end{pmatrix}$.

Find an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue -3 :

$$\begin{aligned}\begin{pmatrix} 2 & 5 \\ -1 & -4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &= -3 \begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} 2x + 5y \\ -x - 4y \end{pmatrix} &= \begin{pmatrix} -3x \\ -3y \end{pmatrix}\end{aligned}$$

The eigenvalues are the solutions to $\det(\mathbf{A} - \lambda \mathbf{I}) = 0$. You begin by finding $\mathbf{A} - \lambda \mathbf{I}$, and then finding its determinant as a polynomial in λ .

This equation is the **characteristic equation** of $\mathbf{A}$.

An eigenvector is a solution to $\mathbf{Ax} = \lambda \mathbf{x}$. In this case, you have to find a column vector $\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix}$ satisfying the equation when $\lambda = 1$.

Equating the lower elements gives $-x - 4y = y$, which leads to $x = -5y$. This is the same equation as you obtain from the upper elements and so gives you no extra information. With 2×2 matrices, one equation gives sufficient information to find an eigenvector.

Here you have a free choice of one variable. You can choose any non-zero value of y and then evaluate x . It is sensible to choose a simple number that avoids fractions.

Problem-solving

There are infinitely many eigenvectors for any given eigenvalue. Any non-zero scalar multiple of $\begin{pmatrix} -5 \\ 1 \end{pmatrix}$ will also be an eigenvector of $\mathbf{A}$ with eigenvalue 1.

Repeat the procedure used for $\lambda = 1$ with $\lambda = -3$.

Equating the upper elements,

$$2x + 5y = -3x$$

$$5x + 5y = 0 \Rightarrow y = -x$$

Let $x = 1$, then $y = -1$

An eigenvector corresponding to -3 is $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

The lower elements would give $-x - 4y = -3y$, which is equivalent to $y = -x$.

Any multiple of this vector is also an eigenvector of $\mathbf{A}$ with eigenvalue -3 .

You are sometimes asked to find a **normalised** eigenvector.

- If $\mathbf{a} = \begin{pmatrix} a \\ b \end{pmatrix}$ is an eigenvector of a matrix $\mathbf{A}$, then the unit vector $\hat{\mathbf{a}} = \begin{pmatrix} \frac{a}{|\mathbf{a}|} \\ \frac{b}{|\mathbf{a}|} \end{pmatrix}$ is a normalised eigenvector of $\mathbf{A}$.

Links For any non-zero vector $\mathbf{a}$, the **unit vector** in the direction of $\mathbf{a}$ is written as $\hat{\mathbf{a}}$.

← Pure Year 1, Chapter 11

In the example above, the normalised eigenvectors are

$$\begin{pmatrix} \frac{-5}{\sqrt{(-5)^2 + 1^2}} \\ \frac{1}{\sqrt{(-5)^2 + 1^2}} \end{pmatrix} = \begin{pmatrix} -\frac{5}{\sqrt{26}} \\ \frac{1}{\sqrt{26}} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \frac{1}{\sqrt{1^2 + (-1)^2}} \\ \frac{-1}{\sqrt{1^2 + (-1)^2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Sometimes, the characteristic equation has a single repeated solution or no real solutions. This leads to either **repeated eigenvalues** or **complex eigenvalues**.

Example 2

Find the eigenvalues and corresponding eigenvectors for these matrices:

a $\mathbf{A} = \begin{pmatrix} 3 & -18 \\ 2 & -9 \end{pmatrix}$

b $\mathbf{B} = \begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix}$

c $\mathbf{C} = \begin{pmatrix} 3 & -2 \\ 4 & -1 \end{pmatrix}$

a $\mathbf{A} - \lambda\mathbf{I} = \begin{pmatrix} 3 - \lambda & -18 \\ 2 & -9 - \lambda \end{pmatrix}$

$$\begin{aligned} \det(\mathbf{A} - \lambda\mathbf{I}) &= \begin{vmatrix} 3 - \lambda & -18 \\ 2 & -9 - \lambda \end{vmatrix} \\ &= (3 - \lambda)(-9 - \lambda) - (-18)(2) \\ &= \lambda^2 + 6\lambda + 9 \end{aligned}$$

$$\lambda^2 + 6\lambda + 9 = 0 \Rightarrow (\lambda + 3)^2 = 0$$

Hence $\lambda = -3$ is a repeated eigenvalue.

Find the corresponding eigenvector(s):

$$\begin{pmatrix} 3 & -18 \\ 2 & -9 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -3 \begin{pmatrix} x \\ y \end{pmatrix}$$

Equating the upper elements,

$$3x - 18y = -3x \Rightarrow x = 3y$$

So a corresponding eigenvector is $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$.

Solve the characteristic equation for matrix $\mathbf{A}$.

Setting $y = 1$ gives $x = 3$.

$$\text{b } \mathbf{B} - \lambda \mathbf{I} = \begin{pmatrix} -3 - \lambda & 0 \\ 0 & -3 - \lambda \end{pmatrix}$$

$$\begin{aligned} \det(\mathbf{B} - \lambda \mathbf{I}) &= \begin{vmatrix} -3 - \lambda & 0 \\ 0 & -3 - \lambda \end{vmatrix} \\ &= (-3 - \lambda)(-3 - \lambda) \\ &= (-3 - \lambda)^2 \end{aligned}$$

Hence $\lambda = -3$ is a repeated eigenvalue.

Find the corresponding eigenvector(s):

$$\begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -3 \begin{pmatrix} x \\ y \end{pmatrix}$$

Equating the upper elements,

$$-3x = -3x$$

This equation does not establish a relationship between x and y .

Hence x and y can take any arbitrary value and every vector is an eigenvector of $\mathbf{B}$.

The simplest pair of linearly independent eigenvectors is $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

$$\text{c } \mathbf{C} - \lambda \mathbf{I} = \begin{pmatrix} 3 - \lambda & -2 \\ 4 & -1 - \lambda \end{pmatrix}$$

$$\begin{aligned} \det(\mathbf{C} - \lambda \mathbf{I}) &= \begin{vmatrix} 3 - \lambda & -2 \\ 4 & -1 - \lambda \end{vmatrix} \\ &= (3 - \lambda)(-1 - \lambda) - (-2)(4) \\ &= \lambda^2 - 2\lambda + 5 \end{aligned}$$

$$\lambda^2 - 2\lambda + 5 = 0$$

$$(\lambda - 1)^2 + 4 = 0$$

$$\lambda = 1 \pm 2i$$

Find the corresponding eigenvectors:

$$\text{For } \lambda = 1 + 2i, \begin{pmatrix} 3 & -2 \\ 4 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = (1 + 2i) \begin{pmatrix} x \\ y \end{pmatrix}$$

Equating the upper elements,

$$3x - 2y = (1 + 2i)x \Rightarrow (2 - 2i)x = 2y$$

$$\text{Set } x = 1, \text{ so } 2 - 2i = 2y \Rightarrow y = 1 - i$$

So the eigenvector corresponding to

$$1 + 2i \text{ is } \begin{pmatrix} 1 \\ 1 - i \end{pmatrix}.$$

$$\text{Set } x = 1, \text{ so } 2 + 2i = 2y \Rightarrow y = 1 + i$$

So the eigenvector corresponding to

$$1 - 2i \text{ is } \begin{pmatrix} 1 \\ 1 + i \end{pmatrix}.$$

Notation A set of vectors is **linearly independent** if no vector in the set can be written as a linear combination of the others. For a set of two vectors, this means that one cannot be written as a scalar multiple of the other.

Similarly, equating the lower elements leads to $-3y = -3y$.

You could give **any** two linearly independent vectors as your eigenvectors but it is convention to choose $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

This matrix has two distinct complex eigenvalues. Note that if a matrix with real elements has complex eigenvalues, they will occur in a conjugate pair. ← Core Pure Book 1, Chapter 1

Problem-solving

The eigenvectors corresponding to complex eigenvalues can be written with one real and one complex element. In this form, the complex elements will be conjugates of each other.

Example 3

A transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is represented by the matrix

$$\mathbf{A} = \begin{pmatrix} 4 & -5 \\ 1 & -2 \end{pmatrix}$$

- a** Find the eigenvalues of $\mathbf{A}$.
b Find Cartesian equations of the two lines passing through the origin which are invariant under T .

$$\mathbf{a} \quad \mathbf{A} - \lambda \mathbf{I} = \begin{pmatrix} 4 & -5 \\ 1 & -2 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 4 - \lambda & -5 \\ 1 & -2 - \lambda \end{pmatrix}$$

$$\begin{aligned} \det(\mathbf{A} - \lambda \mathbf{I}) &= \begin{vmatrix} 4 - \lambda & -5 \\ 1 & -2 - \lambda \end{vmatrix} \\ &= (4 - \lambda)(-2 - \lambda) + 5 \\ &= -8 - 4\lambda + 2\lambda + \lambda^2 + 5 \\ &= \lambda^2 - 2\lambda - 3 \\ &= (\lambda - 3)(\lambda + 1) \end{aligned}$$

$$\det(\mathbf{A} - \lambda \mathbf{I}) = 0 \Rightarrow \lambda = 3 \text{ or } -1$$

The eigenvalues of $\mathbf{A}$ are 3 and -1.

$$\mathbf{b} \quad \begin{pmatrix} 4 & -5 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 3 \begin{pmatrix} x \\ y \end{pmatrix}$$

Equating the upper elements,

$$4x - 5y = 3x \Rightarrow x = 5y$$

So an eigenvector is $\begin{pmatrix} 5 \\ 1 \end{pmatrix}$.

The line through the origin in the direction of $\begin{pmatrix} 5 \\ 1 \end{pmatrix}$ is invariant under T .

The equation of this line is $y = \frac{1}{5}x$.

$$\begin{pmatrix} 4 & -5 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -1 \begin{pmatrix} x \\ y \end{pmatrix}$$

Equating the upper elements,

$$4x - 5y = -x \Rightarrow x = y$$

So an eigenvector is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

The line through the origin in the direction of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is invariant under T .

The equation of this line is $y = x$.

With practice, you can write down this line without the previous working.

Problem-solving

Find the eigenvectors. The directions of the eigenvectors are not changed by the transformation, so each eigenvector will specify an invariant line through the origin.

Check your answer:

$$\begin{pmatrix} 4 & -5 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 5y \\ y \end{pmatrix} = \begin{pmatrix} 20y - 5y \\ 5y - 2y \end{pmatrix} = \begin{pmatrix} 15y \\ 3y \end{pmatrix} \quad \checkmark$$

$$\begin{pmatrix} 4 & -5 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ x \end{pmatrix} = \begin{pmatrix} 4x - 5x \\ x - 2x \end{pmatrix} = \begin{pmatrix} -x \\ -x \end{pmatrix} \quad \checkmark$$

Exercise 5A

- 1 Find the eigenvalues and corresponding eigenvectors of the matrices

a $\begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$

b $\begin{pmatrix} 4 & -1 \\ -1 & 4 \end{pmatrix}$

c $\begin{pmatrix} 3 & -2 \\ 0 & 4 \end{pmatrix}$

- 2 Find the eigenvalues and corresponding eigenvectors of the following matrices.

a $\mathbf{M} = \begin{pmatrix} -2 & 1 \\ -1 & 0 \end{pmatrix}$

b $\mathbf{N} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$

Hint For part **b**, give two linearly independent eigenvectors.

- 3 Find the eigenvalues and corresponding eigenvectors of the following matrices.

a $\mathbf{A} = \begin{pmatrix} -3 & -1 \\ 4 & -3 \end{pmatrix}$

b $\mathbf{B} = \begin{pmatrix} 2 & -1 \\ 2 & 4 \end{pmatrix}$

Hint The eigenvalues will be complex.

- (P)** 4 A transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is represented by the matrix

$$\mathbf{A} = \begin{pmatrix} 3 & 4 \\ -2 & 9 \end{pmatrix}$$

- a** Find the eigenvalues of $\mathbf{A}$.

- b** Find Cartesian equations of the two lines passing through the origin which are invariant under T .

- 5 Show that the matrix $\mathbf{M} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has a repeated eigenvalue and find the corresponding eigenvector.

- (E/P)** 6 The matrix $\mathbf{A} = \begin{pmatrix} 3 & k \\ 1 & -1 \end{pmatrix}$ has a repeated eigenvalue.

Find the value of k .

(4 marks)

- (E/P)** 7 The matrix $\mathbf{M} = \begin{pmatrix} 1 & -1 \\ k & -3 \end{pmatrix}$ has complex eigenvalues.

Find the set of possible values of k .

(4 marks)

- (E/P)** 8 Show that any 2×2 matrix of the form $\mathbf{A} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$, has eigenvalues $a \pm bi$. **(3 marks)**

- (E/P)** 9 The linear transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ maps the point $(5, 2)$ to the point $(-15, -6)$. Write down an eigenvector of the matrix representing T and its corresponding eigenvalue.

(3 marks)

- E/P** 10 a Show that the matrix $\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ has no real eigenvalues and the corresponding linear transformation has no invariant lines. **(4 marks)**
 b Hence explain why the corresponding linear transformation has no invariant lines. **(1 mark)**
- P** 11 The matrix $\mathbf{M} = \begin{pmatrix} -\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix}$ represents a linear transformation T .
 a Find the eigenvalues and corresponding eigenvectors of this matrix. **(3 marks)**
 b Show that the eigenvectors are perpendicular. **(2 marks)**
 c Explain why every point on the line $y = 2x$ is invariant. **(1 mark)**
 d Fully describe the transformation T . **(3 marks)**
- E/P** 12 Show that that if λ is an eigenvalue of matrix $\mathbf{A}$, then λ^2 is an eigenvalue of $\mathbf{A}^2$. **(3 marks)**
- P** 13 $\mathbf{M}$ is a 2×2 matrix, and $\mathbf{x}$ is a non-zero vector.
 Given that $\mathbf{M}\mathbf{x} = 0$, show that $\mathbf{M}$ is singular. **(3 marks)**

Challenge

The linear transformation T is represented by the matrix $\begin{pmatrix} -1 & 0 \\ -2 & 1 \end{pmatrix}$.

Explain why T has infinitely many invariant lines, and fully describe all such invariant lines.

A You can also find the eigenvalues and eigenvectors of a 3×3 matrix.

3×3 matrices have cubic characteristic equations. Often questions will give you a hint which will help you to factorise the cubic. However, if a hint is not given, you may have to search for one of the eigenvalues using the factor theorem.

Links The **factor theorem** states that, for a polynomial $f(x)$, $f(p) = 0$ if and only if $(x - p)$ is a factor of $f(x)$. **← Pure Year 1, Chapter 7**

Example 4**A**

Find the eigenvalues and corresponding eigenvectors of the matrix $\mathbf{A} = \begin{pmatrix} 2 & 1 & -3 \\ 0 & 2 & 1 \\ 0 & -4 & -3 \end{pmatrix}$.

$$\begin{aligned}\mathbf{A} - \lambda \mathbf{I} &= \begin{pmatrix} 2 & 1 & -3 \\ 0 & 2 & 1 \\ 0 & -4 & -3 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 1 & -3 \\ 0 & 2 & 1 \\ 0 & -4 & -3 \end{pmatrix} - \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} = \begin{pmatrix} 2-\lambda & 1 & -3 \\ 0 & 2-\lambda & 1 \\ 0 & -4 & -3-\lambda \end{pmatrix} \\ \det(\mathbf{A} - \lambda \mathbf{I}) &= \begin{vmatrix} 2-\lambda & 1 & -3 \\ 0 & 2-\lambda & 1 \\ 0 & -4 & -3-\lambda \end{vmatrix} \\ &= (2-\lambda) \begin{vmatrix} 2-\lambda & 1 \\ -4 & -3-\lambda \end{vmatrix} - 1 \begin{vmatrix} 0 & 1 \\ 0 & -3-\lambda \end{vmatrix} + (-3) \begin{vmatrix} 0 & 2-\lambda \\ 0 & -4 \end{vmatrix} \\ &= (2-\lambda)((2-\lambda)(-3-\lambda) + 4) - 0 + 0 \\ &= (2-\lambda)(-6 - 2\lambda + 3\lambda + \lambda^2 + 4) \\ &= (2-\lambda)(\lambda^2 + \lambda - 2) \\ &= (2-\lambda)(\lambda + 2)(\lambda - 1)\end{aligned}$$

$$\det(\mathbf{A} - \lambda \mathbf{I}) = 0 \Rightarrow (2 - \lambda)(\lambda + 2)(\lambda - 1) = 0$$

$$\Rightarrow \lambda = 2, -2 \text{ or } 1$$

The eigenvalues of $\mathbf{A}$ are -2 , 1 and 2 .

Find an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue -2 :

$$\begin{pmatrix} 2 & 1 & -3 \\ 0 & 2 & 1 \\ 0 & -4 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -2 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\begin{pmatrix} 2x + y - 3z \\ 2y + z \\ -4y - 3z \end{pmatrix} = \begin{pmatrix} -2x \\ -2y \\ -2z \end{pmatrix}$$

Equating the middle elements,

$$2y + z = -2y \Rightarrow z = -4y$$

Let $y = 1$, then $z = -4$.

Equating the top elements and substituting $y = 1$ and $z = -4$,

$$2x + y - 3z = -2x$$

$$4x = -y + 3z$$

$$= -1 - 12 = -13 \Rightarrow x = -\frac{13}{4}$$

An eigenvector corresponding to -2 is $\begin{pmatrix} -\frac{13}{4} \\ 1 \\ -4 \end{pmatrix}$.

As with 2×2 matrices, the eigenvalues are the solutions to $\det(\mathbf{A} - \lambda \mathbf{I}) = 0$. You begin by finding $\mathbf{A} - \lambda \mathbf{I}$ and finding its determinant. With a 3×3 matrix the characteristic equation is a cubic which will have 3 roots and hence 3 eigenvalues.

An eigenvector is a solution to $\mathbf{Ax} = \lambda \mathbf{x}$. In this case, you have to find a column vector $\mathbf{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ satisfying the equation when $\lambda = -2$.

Here you have a free choice of one variable. You can choose any non-zero value for y or x and then evaluate the other variable.

Equating the lowest elements gives an equivalent equation to the one you obtained from the middle elements and so gives you no extra information. With 3×3 matrices, usually two equations will give you all the information you need to find an eigenvector.

A

Find an eigenvector of **A** corresponding to the eigenvalue 1:

$$\begin{pmatrix} 2 & 1 & -3 \\ 0 & 2 & 1 \\ 0 & -4 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\begin{pmatrix} 2x + y - 3z \\ 2y + z \\ -4y - 3z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Equating the middle elements,

$$2y + z = y \Rightarrow y = -z$$

Let $z = 1$, then $y = -1$.Equating the top elements and substituting $y = -1$ and $z = 1$,

$$2x + y - 3z = x$$

$$x = -y + 3z = 1 + 3 = 4$$

An eigenvector corresponding to 1 is $\begin{pmatrix} 4 \\ -1 \\ 1 \end{pmatrix}$.Find an eigenvector of **A** corresponding to the eigenvalue 2:

$$\begin{pmatrix} 2 & 1 & -3 \\ 0 & 2 & 1 \\ 0 & -4 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 2 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\begin{pmatrix} 2x + y - 3z \\ 2y + z \\ -4y - 3z \end{pmatrix} = \begin{pmatrix} 2x \\ 2y \\ 2z \end{pmatrix}$$

Equating the middle elements,

$$2y + z = 2y \Rightarrow z = 0$$

Equating the bottom elements and using $z = 0$,

$$-4y - 3z = 2z \Rightarrow 4y = -5z = 0 \Rightarrow y = 0$$

Equating the top elements,

$$2x + y - 3z = 2x \Rightarrow y = 3z \Rightarrow y = 0, z = 0$$

Let $x = 1$.An eigenvector corresponding to 2 is $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.Repeat the procedure with $\lambda = 1$.

Any non-zero multiple of this eigenvector would also be a correct eigenvector.

This calculation differs from the calculation for the other two eigenvalues in that these two equations give you that $y = z = 0$ and there is no choice of values.The variable x appears in no equation and so can take any value. 1 is the simplest value to take.

A 3×3 matrix will always have at least one real eigenvalue since a cubic equation always has at least one real solution.

Example 5**A**

The matrix $\mathbf{A} = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & 5 \\ 2 & 1 & 0 \end{pmatrix}$

- a** Show that -2 is the only real eigenvalue of $\mathbf{A}$.
b Find a normalised eigenvector of $\mathbf{A}$ corresponding to the eigenvalue -2 .

$$\mathbf{a} \quad \mathbf{A} - \lambda \mathbf{I} = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & 5 \\ 2 & 1 & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} = \begin{pmatrix} 2-\lambda & -1 & 1 \\ 0 & 3-\lambda & 5 \\ 2 & 1 & -\lambda \end{pmatrix}$$

$$\begin{aligned} \det(\mathbf{A} - \lambda \mathbf{I}) &= \begin{vmatrix} 2-\lambda & -1 & 1 \\ 0 & 3-\lambda & 5 \\ 2 & 1 & -\lambda \end{vmatrix} \\ &= (2-\lambda) \begin{vmatrix} 3-\lambda & 5 \\ 1 & -\lambda \end{vmatrix} - (-1) \begin{vmatrix} 0 & 5 \\ 2 & -\lambda \end{vmatrix} + 1 \begin{vmatrix} 0 & 3-\lambda \\ 2 & 1 \end{vmatrix} \\ &= (2-\lambda)(-3\lambda + \lambda^2 - 5) - 10 - 2(3-\lambda) \\ &= -6\lambda + 2\lambda^2 - 10 + 3\lambda^2 - \lambda^3 + 5\lambda - 10 - 6 + 2\lambda \\ &= -\lambda^3 + 5\lambda^2 + \lambda - 26 \end{aligned}$$

$$\det(\mathbf{A} - \lambda \mathbf{I}) = 0 \Rightarrow -\lambda^3 + 5\lambda^2 + \lambda - 26 = 0$$

$$\lambda^3 - 5\lambda^2 - \lambda + 26 = 0$$

$$(\lambda + 2)(\lambda^2 + k\lambda + 13) = 0$$

Equating coefficients of λ^2 ,

$$-5 = 2 + k \Rightarrow k = -7$$

$$(\lambda + 2)(\lambda^2 - 7\lambda + 13) = 0$$

The discriminant of $\lambda^2 - 7\lambda + 13 = 0$ is

$$b^2 - 4ac = 49 - 52 = -3 < 0$$

The quadratic factor $\lambda^2 - 7\lambda + 13$ has no real roots.

So -2 is the only real eigenvalue of $\mathbf{A}$.

$$\mathbf{b} \quad \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & 5 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -2 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\begin{pmatrix} 2x - y + z \\ 3y + 5z \\ 2x + y \end{pmatrix} = \begin{pmatrix} -2x \\ -2y \\ -2z \end{pmatrix}$$

Equating the middle elements,

$$3y + 5z = -2y \Rightarrow y = -z$$

Let $z = 1$, then $y = -1$.

Equating the bottom elements,

$$2x + y = -2z \Rightarrow x = \frac{-y - 2z}{2}$$

The question implies that $\lambda = -2$ is a root of the characteristic equation and so $(\lambda + 2)$ must be a factor of the cubic. Equating a coefficient has been used here to complete the factorisation but you can use any appropriate method.

To show that there is only one real root of the cubic, show that the discriminant of the quadratic factor is negative.

A

Substituting $y = -1$ and $z = 1$,

$$x = \frac{1-2}{2} = -\frac{1}{2}$$

An eigenvector of $\mathbf{A}$ is $2 \begin{pmatrix} -\frac{1}{2} \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 2 \end{pmatrix}$

The magnitude of this eigenvector is

$$\sqrt{(-1)^2 + (-2)^2 + 2^2} = 3$$

A normalised eigenvector of $\mathbf{A}$ is

$$\frac{1}{3} \begin{pmatrix} -1 \\ -2 \\ 2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ \frac{2}{3} \end{pmatrix}$$

The working gives $\begin{pmatrix} -\frac{1}{2} \\ -1 \\ 1 \end{pmatrix}$ as the eigenvector but,

as any multiple of this is also an eigenvector, it is sensible to multiply this by 2, or -2 , to avoid working in fractions.

A normalised eigenvector is found by dividing all of the terms by the magnitude of the original eigenvector.

$\begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ -\frac{2}{3} \end{pmatrix}$ would also be correct. If a column vector $\mathbf{x}$ is

a normalised eigenvector of a matrix, then $-\mathbf{x}$ is also a normalised eigenvector.

Example 6

The matrix $\mathbf{A} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$

- Show that 1 is a repeated eigenvalue of $\mathbf{A}$ and find the other distinct eigenvalue.
- Find two linearly independent eigenvectors corresponding to the eigenvalue 1.

$$\begin{aligned} \text{a } \det(\mathbf{A} - \lambda \mathbf{I}) &= \begin{vmatrix} 2-\lambda & 1 & 1 \\ 1 & 2-\lambda & 1 \\ 1 & 1 & 2-\lambda \end{vmatrix} \\ &= (2-\lambda) \begin{vmatrix} 2-\lambda & 1 \\ 1 & 2-\lambda \end{vmatrix} - 1 \begin{vmatrix} 1 & 1 \\ 1 & 2-\lambda \end{vmatrix} + 1 \begin{vmatrix} 1 & 2-\lambda \\ 1 & 1 \end{vmatrix} \\ &= (2-\lambda)((2-\lambda)^2 - 1) - (1-\lambda) + (\lambda-1) \\ &= (2-\lambda)(\lambda^2 - 4\lambda + 3) + 2\lambda - 2 \\ &= (2-\lambda)(\lambda-3)(\lambda-1) + 2(\lambda-1) \\ &= (\lambda-1)(2\lambda-6-\lambda^2+3\lambda+2) \\ &= -(\lambda-1)(\lambda^2-5\lambda+4) = -(\lambda-1)^2(\lambda-4) \end{aligned}$$

The solutions to $\det(\mathbf{A} - \lambda \mathbf{I}) = 0$ are 1 repeated and 4.

So 1 is a repeated eigenvalue and 4 is the other eigenvalue.

$$\text{b } \begin{pmatrix} 2x+y+z \\ x+2y+z \\ x+y+2z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Equating the top elements,

$$2x+y+z = x \Rightarrow x+y+z = 0$$

Factorise the cubic. Since you know that 1 is a root of the cubic, look for the factor $(\lambda-1)$.

Equating the middle and bottom elements both give you the same equation so the elements of the eigenvectors only need to satisfy this one equation.

A

To find two linearly independent eigenvectors,

$$y = 0 \text{ and } z = 1 \Rightarrow x = -1$$

$$y = 1 \text{ and } z = 0 \Rightarrow x = -1$$

So two linearly independent eigenvectors are $\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$.

The choices of $y = 0$ and $z = 1$, and $y = 1$ and $z = 0$ are arbitrary but guarantee that the eigenvectors are linearly independent.

Watch out Not all repeated eigenvectors will give two linearly independent eigenvectors.

Exercise 5B

- 1 Find the eigenvalues and corresponding eigenvectors of the matrices

a $\begin{pmatrix} 3 & 0 & 0 \\ 2 & 4 & 2 \\ -2 & 0 & 1 \end{pmatrix}$

b $\begin{pmatrix} 4 & -2 & -4 \\ 2 & 3 & 0 \\ 2 & -5 & -4 \end{pmatrix}$

E/P

2 $\mathbf{M} = \begin{pmatrix} 7 & 0 & -3 \\ -9 & -2 & 3 \\ 18 & 0 & -8 \end{pmatrix}$

- a** Show that -2 is a repeated eigenvalue of $\mathbf{M}$ and find the other distinct eigenvalue. (4 marks)
b Find two linearly independent eigenvectors corresponding to the eigenvalue -2 . (3 marks)

3 $\mathbf{A} = \begin{pmatrix} 3 & -1 & 2 \\ 3 & -1 & 6 \\ -2 & 2 & -2 \end{pmatrix}$

Find the eigenvalues and corresponding eigenvectors for matrix $\mathbf{A}$.

4 The matrix $\mathbf{A} = \begin{pmatrix} 2 & 2 & -2 \\ -3 & 2 & 0 \\ 1 & 4 & -3 \end{pmatrix}$

- a** Show that -1 is the only real eigenvalue of $\mathbf{A}$.
b Find an eigenvector corresponding to the eigenvalue -1 .
c Find the two complex eigenvalues and their corresponding eigenvectors.

Hint Find the roots of the quadratic factor in the characteristic equation for matrix $\mathbf{A}$.

E

5 The matrix $\mathbf{A} = \begin{pmatrix} 2 & -1 & 3 \\ 0 & 2 & 4 \\ 0 & 2 & 0 \end{pmatrix}$

- a** Show that 4 is an eigenvalue of $\mathbf{A}$ and find the other two eigenvalues of $\mathbf{A}$. (4 marks)
b Find an eigenvector corresponding to the eigenvalue 4 . (2 marks)

- A**
E 6 The matrix $A = \begin{pmatrix} 1 & 1 & 3 \\ 2 & 4 & -1 \\ 4 & 4 & 3 \end{pmatrix}$
Given that 3 is an eigenvalue of A ,
a find the other two eigenvalues of A (4 marks)
b find the eigenvector corresponding to each of the eigenvalues of A . (4 marks)
- E** 7 The matrix $A = \begin{pmatrix} 2 & 2 & 1 \\ -2 & 4 & 0 \\ 4 & 2 & 5 \end{pmatrix}$
a Show that 2 is an eigenvalue of A . (2 marks)
b Find the other two eigenvalues of A . (2 marks)
c Find a normalised eigenvector of A corresponding to the eigenvalue 2. (2 marks)
- E** 8 The matrix $A = \begin{pmatrix} 4 & 2 & 1 \\ -2 & 0 & 5 \\ 0 & 3 & 4 \end{pmatrix}$
a Show that -2 is an eigenvalue of A and that there is only one other eigenvalue. (4 marks)
b Find an eigenvector corresponding to each of the eigenvalues. (4 marks)
- E** 9 The matrix $A = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix}$.
Given that 2 is an eigenvalue of A ,
a find the other two eigenvalues of A (4 marks)
b find the eigenvector corresponding to each of the eigenvalues of A . (4 marks)
- E/P** 10 Given that $\begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix}$ is an eigenvector of the matrix A where $A = \begin{pmatrix} 4 & 1 & 2 \\ 1 & a & 0 \\ -1 & 1 & b \end{pmatrix}$
a find the eigenvalue of A corresponding to $\begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix}$ (2 marks)
b find the value of a and the value of b (4 marks)
c show that A has only one real eigenvalue. (2 marks)
d Find the two complex eigenvalues and their corresponding eigenvectors. (6 marks)
- E/P** 11 $A = \begin{pmatrix} 3 & 0 & 0 \\ 1 & 1 & 1 \\ 4 & -1 & 3 \end{pmatrix}$
a Find the eigenvalues of matrix A and hence find a set of eigenvectors. (6 marks)
Matrix A represents the linear transformation $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$.
b Find vector equations of the invariant lines under T . (4 marks)
- E/P** 12 Explain why every linear transformation from $\mathbb{R}^3$ to $\mathbb{R}^3$ must have at least one invariant line. (2 marks)

Challenge**A**

The matrix $\mathbf{M} = \begin{pmatrix} \frac{1}{9} & \frac{8}{9} & -\frac{4}{9} \\ \frac{8}{9} & \frac{1}{9} & \frac{4}{9} \\ -\frac{4}{9} & \frac{4}{9} & \frac{7}{9} \end{pmatrix}$ represents a reflection in plane Π .

Find the eigenvalues and eigenvectors of $\mathbf{M}$ and hence find the Cartesian equation of the plane Π .

5.2 Reducing matrices to diagonal form

Calculations with matrices can often be simplified by reducing a matrix to a given form. In this section you will learn how to reduce some matrices to **diagonal** form.

- A **diagonal matrix** is a square matrix in which all of the elements which are not on the diagonal from the top left to the bottom right of the matrix are zero. The diagonal from the top left to the bottom right of the matrix is called the **leading diagonal**.



- The general 2×2 diagonal matrix is $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

For example, $\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}$, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and (1) are all diagonal matrices.

Watch out Any non-zero elements must be on

the **leading diagonal**. For example, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

and $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ are not diagonal matrices.

- To reduce a given matrix $\mathbf{A}$ to diagonal form, use the following procedure.

- Find the eigenvalues and eigenvectors of $\mathbf{A}$.
- Form a matrix $\mathbf{P}$ which consists of the eigenvectors of $\mathbf{A}$.
- Find $\mathbf{P}^{-1}$.
- A diagonal matrix $\mathbf{D}$ is given by $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$.

Note A matrix which can be reduced to diagonal form in this way is called a **diagonalisable** matrix. Not every matrix can be diagonalised, although any $n \times n$ matrix with n distinct eigenvalues can be. In your exam you will only be asked to diagonalise matrices of this type.

Example 7

$$\mathbf{A} = \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$$

- a Find a matrix $\mathbf{P}$ such that $\mathbf{D} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ is diagonal.
 b Write down the diagonal matrix $\mathbf{D}$.

$$\begin{aligned} \text{a } \begin{vmatrix} 4-\lambda & 2 \\ 1 & 3-\lambda \end{vmatrix} &= (4-\lambda)(3-\lambda) - 2 \times 1 \\ &= \lambda^2 - 7\lambda + 10 \\ \lambda^2 - 7\lambda + 10 &= 0 \Rightarrow \lambda = 5 \text{ or } 2 \end{aligned}$$

Find the eigenvalues of $\mathbf{A}$.

$$\begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

For $\lambda = 2$, $4x + 2y = 2x$ so $x = -y$ A corresponding eigenvector is $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$.For $\lambda = 5$, $4x + 2y = 5x$ so $2y = x$ A corresponding eigenvector = $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$.Find the eigenvectors of $\mathbf{A}$.

$$\text{So } \mathbf{P} = \begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$\text{b } \det \mathbf{P} = -1 \times 1 - 2 \times 1 = -3$$

$$\text{Hence } \mathbf{P}^{-1} = -\frac{1}{3} \begin{pmatrix} 1 & -2 \\ -1 & -1 \end{pmatrix}$$

$$\mathbf{D} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$$

$$\mathbf{D} = -\frac{1}{3} \begin{pmatrix} 1 & -2 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$= -\frac{1}{3} \begin{pmatrix} 1 & -2 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} -2 & 10 \\ 2 & 5 \end{pmatrix}$$

$$= -\frac{1}{3} \begin{pmatrix} -6 & 0 \\ 0 & -15 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}$$

Find $\mathbf{P}^{-1}$. Remember that for any non-singular

$$\text{matrix } \mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

← Core Pure Book 1, Chapter 6

The matrix $\mathbf{D}$ consists of the eigenvalues of $\mathbf{A}$ along the leading diagonal in the same order as the eigenvectors are given in matrix $\mathbf{P}$. All other elements are zero as required.

- When you reduce a matrix $\mathbf{A}$ to a diagonal matrix $\mathbf{D}$, the elements on the diagonal are the eigenvalues of $\mathbf{A}$.

The above process for diagonalising a matrix relies on finding the inverse of $\mathbf{P}$. For larger matrices this can be a time-consuming process. If a matrix is **symmetric** you can diagonalise it more easily.

- A matrix, $\mathbf{A}$, is **symmetric** if $\mathbf{A} = \mathbf{A}^T$.
 The elements of a symmetric matrix are symmetric with respect to the leading diagonal.

Watch out

Don't confuse the matrix $\mathbf{P}$ which diagonalises a given matrix, $\mathbf{A}$, with the diagonal matrix $\mathbf{D}$. $\mathbf{P}$ is formed from the **eigenvectors** of $\mathbf{A}$, and $\mathbf{D}$ has the **eigenvalues** of $\mathbf{A}$ on its leading diagonal.

Links

$\mathbf{A}^T$ is the **transpose** of matrix $\mathbf{A}$. It is the matrix formed by interchanging the rows and columns of matrix $\mathbf{A}$.

← Core Pure Book 1, Section 6.5

For example, $\begin{pmatrix} 1 & 3 \\ 3 & -2 \end{pmatrix}$ and $\begin{pmatrix} 1 & b & 3 \\ b & a & 0 \\ 3 & 0 & 0 \end{pmatrix}$ are symmetric matrices.

If the matrix **A** is symmetric, you can carry out **orthogonal diagonalisation**.

■ **The procedure for orthogonal diagonalisation of a symmetric matrix A is:**

- **Find the normalised eigenvectors of A.**
- **Form a matrix P which consists of the normalised eigenvectors of A.**
- **Write down P^T .**
- **A diagonal matrix D is given by P^TAP .**

Note For any symmetric matrix, the normalised eigenvectors are mutually perpendicular. This means that the matrix formed from the normalised eigenvectors has the property that $P^{-1} = P^T$. Matrices which have this property are called **orthogonal matrices**.

Example 8

The matrix $A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$. Reduce A to a diagonal matrix.

$$A - \lambda I = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 2-\lambda & -1 \\ -1 & 2-\lambda \end{pmatrix}$$

$$\begin{vmatrix} 2-\lambda & -1 \\ -1 & 2-\lambda \end{vmatrix} = (2-\lambda)(2-\lambda) - 1 \\ = \lambda^2 - 4\lambda + 3 = (\lambda - 1)(\lambda - 3)$$

$$\det(A - \lambda I) = 0 \Rightarrow (\lambda - 1)(\lambda - 3) = 0 \\ \Rightarrow \lambda = 1 \text{ or } 3$$

$\lambda = 1$:

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 1 \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\begin{pmatrix} 2x - y \\ -x + 2y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Equating the upper elements,

$$2x - y = x \Rightarrow y = x$$

Let $x = 1$, then $y = 1$.

An eigenvector corresponding to the eigenvalue 1 is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

The magnitude of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is $\sqrt{1^2 + 1^2} = \sqrt{2}$.

A normalised eigenvector corresponding to

the eigenvalue 1 is $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$.

To diagonalise a symmetric matrix, you need to find normalised eigenvectors of the matrix, so start by finding the eigenvalues.

Watch out If you are using orthogonal diagonalisation, you need to find the **normalised** eigenvectors.

To convert an eigenvector **x** to a normalised eigenvector, divide each of the elements of **x** by the magnitude of **x**.

$\lambda = 3$:

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 3 \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\begin{pmatrix} 2x - y \\ -x + 2y \end{pmatrix} = \begin{pmatrix} 3x \\ 3y \end{pmatrix}$$

Equating the upper elements,

$$2x - y = 3x \Rightarrow y = -x$$

Let $x = 1$, then $y = -1$.

An eigenvector corresponding to the eigenvalue 3 is $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

The magnitude of $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is $\sqrt{1^2 + (-1)^2} = \sqrt{2}$.

A normalised eigenvector corresponding to

the eigenvalue 1 is $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$.

$$\mathbf{P} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\mathbf{P}^T = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\mathbf{P}^T \mathbf{A} \mathbf{P} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{2}{\sqrt{2}} - \frac{1}{\sqrt{2}} & \frac{2}{\sqrt{2}} + \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} + \frac{2}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - \frac{2}{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{3}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{3}{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{2} + \frac{1}{2} & \frac{3}{2} - \frac{3}{2} \\ \frac{1}{2} - \frac{1}{2} & \frac{3}{2} + \frac{3}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$$

The diagonal matrix is given by $\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$.

The negative of this vector, $\begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$, is also correct and would just as appropriate for diagonalising the matrix.

Form the orthogonal matrix $\mathbf{P}$ from the normalised eigenvectors by using the eigenvectors as the columns of the matrix.

In this case, as $\mathbf{P}$ is symmetric, $\mathbf{P}^T = \mathbf{P}$.

The non-zero number in the first column, 1, is the eigenvalue corresponding to the eigenvector $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ used as the first column of $\mathbf{P}$.

The non-zero number in the second column, 3, is the eigenvalue corresponding to the eigenvector $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$ used as the first column of $\mathbf{P}$.

If you had taken $\mathbf{P}$ as $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ then $\mathbf{D}$ would be $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$.

A similar result is true for 3×3 matrices.

A The process of diagonalising matrices is the same for 3×3 matrices.

Example 9

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & -3 \\ 4 & 2 & 3 \end{pmatrix}$$

Find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{D} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$.

$$\begin{vmatrix} 1-\lambda & 1 & 2 \\ 4 & 2-\lambda & -3 \\ 4 & 2 & 3-\lambda \end{vmatrix} = (1-\lambda)(2-\lambda)(3-\lambda) + 6 \\ - (4(3-\lambda) + 12) + 2(8 - 4(2-\lambda)) \\ = -(\lambda+1)(\lambda-3)(\lambda-4)$$

So eigenvalues are -1 , 3 and 4 .

$$\begin{pmatrix} 1 & 1 & 2 \\ 4 & 2 & -3 \\ 4 & 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$\lambda = -1$:

Equating the top elements,

$$x + y + 2z = -x \Rightarrow 2x + y + 2z = 0 \quad (1)$$

Equating the middle elements,

$$4x + 2y - 3z = -y \Rightarrow 4x + 3y - 3z = 0 \quad (2)$$

Equating the bottom elements,

$$4x + 2y + 3z = -z \Rightarrow 4x + 2y + 4z = 0 \quad (3)$$

$(2) - (3)$ gives $y - 7z = 0$

Setting $z = 1$ gives $y = 7$ and $x = -\frac{9}{2}$.

A corresponding eigenvector is $\begin{pmatrix} -9 \\ 14 \\ 2 \end{pmatrix}$.

$\lambda = 3$:

Equating the top elements,

$$x + y + 2z = 3x \Rightarrow -2x + y + 2z = 0 \quad (1)$$

Equating the middle elements,

$$4x + 2y - 3z = 3y \Rightarrow 4x - y - 3z = 0 \quad (2)$$

Equating the bottom elements,

$$4x + 2y + 3z = 3z \Rightarrow 4x + 2y = 0 \quad (3)$$

Equation (3) gives $y = -2x$

Setting $x = 1$ gives $y = -2$ and $z = 2$.

A corresponding eigenvector is $\begin{pmatrix} 1 \\ -2 \\ 2 \end{pmatrix}$.

Note that equation (1) is just a multiple of equation (3), so the system can be solved using just equations (2) and (3).

It is conventional to give an eigenvector in integer form, so multiply the x , y and z values through by 2 before stating the eigenvector.

A

 $\lambda = 4$:

Equating the top elements,

$$x + y + 2z = 4x \Rightarrow -3x + y + 2z = 0 \quad (1)$$

Equating the middle elements,

$$4x + 2y - 3z = 4y \Rightarrow 4x - 2y - 3z = 0 \quad (2)$$

Equating the bottom elements,

$$4x + 2y + 3z = 4z \Rightarrow 4x + 2y - z = 0 \quad (3)$$

(3) - (2) gives $4y + 2z = 0$ Setting $y = 1$ gives $z = -2$ and $x = -1$.A corresponding eigenvector is $\begin{pmatrix} -1 \\ 1 \\ -2 \end{pmatrix}$.

$$\text{So } \mathbf{P} = \begin{pmatrix} -9 & 1 & -1 \\ 14 & -2 & 1 \\ 2 & 2 & -2 \end{pmatrix} \text{ and } \mathbf{D} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

You can write down matrix **D** by entering the eigenvalues corresponding to the order of the eigenvectors in **P** in the leading diagonal of **D**.

You can check your solution by finding the inverse of **P** using your calculator, and then finding the matrix product $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$.

Example 10

The matrix $\mathbf{A} = \begin{pmatrix} 7 & 5 & 5 \\ 5 & -2 & 4 \\ 5 & 4 & -2 \end{pmatrix}$

- a Verify that $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ is an eigenvector of **A** and find the corresponding eigenvalue.
- b Show that -6 is another eigenvalue of **A** and find the corresponding eigenvector.
- c Given that the third eigenvector of **A** is $\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}$, find a matrix **P** and a diagonal matrix **D** such that $\mathbf{P}^T\mathbf{A}\mathbf{P} = \mathbf{D}$.

$$\text{a } \begin{pmatrix} 7 & 5 & 5 \\ 5 & -2 & 4 \\ 5 & 4 & -2 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 14 + 5 + 5 \\ 10 - 2 + 4 \\ 10 + 4 - 2 \end{pmatrix} = \begin{pmatrix} 24 \\ 12 \\ 12 \end{pmatrix} = 12 \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$$

Hence $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ is an eigenvector of **A** corresponding to the eigenvalue 12.

$$\begin{aligned} \text{b } \mathbf{A} - \lambda\mathbf{I} &= \begin{pmatrix} 7 & 5 & 5 \\ 5 & -2 & 4 \\ 5 & 4 & -2 \end{pmatrix} - \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \\ &= \begin{pmatrix} 7 - \lambda & 5 & 5 \\ 5 & -2 - \lambda & 4 \\ 5 & 4 & -2 - \lambda \end{pmatrix} \end{aligned}$$

To show that **x** is an eigenvector of **A**, you have to find a constant, λ , such that $\mathbf{A}\mathbf{x} = \lambda\mathbf{x}$.

A

When $\lambda = -6$,

$$\begin{aligned}\det(\mathbf{A} - \lambda\mathbf{I}) &= \begin{vmatrix} 7 - (-6) & 5 & 5 \\ 5 & -2 - (-6) & 4 \\ 5 & 4 & -2 - (-6) \end{vmatrix} = \begin{vmatrix} 13 & 5 & 5 \\ 5 & 4 & 4 \\ 5 & 4 & 4 \end{vmatrix} \\ &= 13 \begin{vmatrix} 4 & 4 \\ 4 & 4 \end{vmatrix} - 5 \begin{vmatrix} 5 & 5 \\ 4 & 4 \end{vmatrix} + 5 \begin{vmatrix} 5 & 5 \\ 4 & 4 \end{vmatrix} \\ &= 13(16 - 16) - 5(20 - 20) + 5(20 - 20) = 0\end{aligned}$$

So -6 is an eigenvalue of $\mathbf{A}$.Find an eigenvector corresponding to -6 :

$$\begin{pmatrix} 7 & 5 & 5 \\ 5 & -2 & 4 \\ 5 & 4 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -6 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\begin{pmatrix} 7x + 5y + 5z \\ 5x - 2y + 4z \\ 5x + 4y - 2z \end{pmatrix} = \begin{pmatrix} -6x \\ -6y \\ -6z \end{pmatrix}$$

Equating the top elements,

$$7x + 5y + 5z = -6x \Rightarrow 5y + 5z = -13x$$

$$y + z = -\frac{13}{5}x \quad (1)$$

Equating the middle elements,

$$5x - 2y + 4z = -6y \Rightarrow 4y + 4z = -5x$$

$$y + z = -\frac{5}{4}x \quad (2)$$

From (1) and (2),

$$-\frac{13}{5}x = -\frac{5}{4}x \Rightarrow x = 0$$

Substituting $x = 0$ into (1),

$$y + z = 0 \Rightarrow y = -z$$

Let $y = 1$, then $z = -1$.An eigenvector corresponding to the eigenvalue -6 is $\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$.c Find the eigenvalue corresponding to $\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}$:

$$\begin{pmatrix} 7 & 5 & 5 \\ 5 & -2 & 4 \\ 5 & 4 & -2 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 7 - 5 - 5 \\ 5 + 2 - 4 \\ 5 - 4 + 2 \end{pmatrix} = \begin{pmatrix} -3 \\ 3 \\ 3 \end{pmatrix} = -3 \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}$$

The corresponding eigenvalue is -3 .The magnitude of $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ is $\sqrt{2^2 + 1^2 + 1^2} = \sqrt{6}$

To show that -6 is an eigenvalue, it is sufficient to show that substituting $\lambda = -6$ into $\det(\mathbf{A} - \lambda\mathbf{I})$ gives 0. You do not have to solve the cubic characteristic equation completely.

Watch out The matrix product in part c is given as $\mathbf{P}^T\mathbf{A}\mathbf{P}$. This tells you that you need to use **orthogonal diagonalisation**. This is possible because the matrix $\mathbf{A}$ is symmetric.

You will need the eigenvalue corresponding to this eigenvector for the third non-zero element of the diagonal matrix $\mathbf{D}$. You already know that the other two elements are 12 and -6 .

A

A normalised eigenvector corresponding to 12 is $\begin{pmatrix} \frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}$.

The magnitude of $\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$ is $\sqrt{0^2 + 1^2 + (-1)^2} = \sqrt{2}$.

A normalised eigenvector corresponding to -6 is $\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$.

The magnitude of $\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}$ is $\sqrt{1^2 + (-1)^2 + (-1)^2} = \sqrt{3}$.

A normalised eigenvector corresponding to -3 is $\begin{pmatrix} \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{3}} \end{pmatrix}$.

So $\mathbf{P} = \begin{pmatrix} \frac{2}{\sqrt{6}} & 0 & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{3}} \end{pmatrix}$ and $\mathbf{D} = \begin{pmatrix} 12 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & -3 \end{pmatrix}$.

The matrix $\mathbf{P}$ is made up of columns of normalised eigenvectors. $\mathbf{P}$ is an orthogonal matrix and so $\mathbf{P}^T = \mathbf{P}^{-1}$. Hence there is no difference between the expression $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$, used to diagonalise $\mathbf{A}$ in this example and the expression $\mathbf{P}^T\mathbf{A}\mathbf{P}$, used in Example 8.

You know that $\mathbf{P}$ is a matrix with the normalised eigenvectors as its columns and that $\mathbf{D}$ is the diagonal matrix with the corresponding eigenvalues as the elements of the leading diagonal. Multiplying the matrices out is a laborious process and you should not do this unless the question requires it.

There are many applications in which diagonal matrices are easier to work with. For example, you can use matrix diagonalisation to solve problems involving coupled differential equations or coupled recurrence relations.

Example 11

The two sequences x_n and y_n satisfy the recurrence relations

$$x_{n+1} = 4x_n + y_n, \quad x_1 = 1$$

$$y_{n+1} = 2x_n + 3y_n, \quad y_1 = 2 \quad n \geq 1$$

These recurrence relations can be written in matrix form as

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \mathbf{A} \begin{pmatrix} x_n \\ y_n \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad n \geq 1$$

where $\mathbf{A} = \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix}$.

- Find the eigenvalues and corresponding eigenvectors of $\mathbf{A}$.
- Hence write down matrices $\mathbf{P}$ and $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$ where $\mathbf{D}$ is a diagonal matrix.

New sequences u_n and v_n can be formed from x_n and y_n using the transformation

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \mathbf{P}^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

c Show that $\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \mathbf{D} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$.

d Hence find closed form expressions for the original sequences x_n and y_n .

$$\begin{aligned} \text{a } \begin{vmatrix} 4 - \lambda & 1 \\ 2 & 3 - \lambda \end{vmatrix} &= (4 - \lambda)(3 - \lambda) - 2 \times 1 \\ &= \lambda^2 - 7\lambda + 10 \\ &= (\lambda - 5)(\lambda - 2) \end{aligned}$$

So eigenvalues are 5 and 2.

$$\begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

$\lambda = 5$:

Equating the top elements,

$$4x + y = 5x \Rightarrow y = x$$

A corresponding eigenvector is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

$\lambda = 2$:

Equating the top elements,

$$4x + y = 2x \Rightarrow y = -2x$$

A corresponding eigenvector is $\begin{pmatrix} 1 \\ -2 \end{pmatrix}$.

$$\text{b } \mathbf{P} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix} \text{ and } \mathbf{D} = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$$

$$\begin{aligned} \text{c } \begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} &= \mathbf{P}^{-1} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \\ &= \mathbf{P}^{-1} \mathbf{A} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \\ &= \mathbf{P}^{-1} \mathbf{A} \mathbf{P} \mathbf{P}^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \\ &= \mathbf{D} \mathbf{P}^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \mathbf{D} \begin{pmatrix} u_n \\ v_n \end{pmatrix} \text{ as required.} \end{aligned}$$

$$\text{d } \begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$

$$\text{So } u_{n+1} = 5u_n \text{ and } v_{n+1} = 2v_n$$

$$\text{Hence } u_{n+1} = u_1 \times 5^{n-1} \text{ and } v_{n+1} = v_1 \times 2^{n-1}$$

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \mathbf{P}^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \Rightarrow \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \mathbf{P} \begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$

$$x_n = u_n + v_n = u_1 \times 5^{n-1} + v_1 \times 2^{n-1}$$

$$y_n = u_n - 2v_n = u_1 \times 5^{n-1} - 2v_1 \times 2^{n-1}$$

Links **Closed form** means that you need to find x_n and y_n in terms of n only. ← Chapter 4

Use the transformation with n replaced by $n + 1$.

Replace $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix}$ with $\mathbf{A} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$.

Use the fact that $\mathbf{P}\mathbf{P}^{-1} = \mathbf{I}$.

Replace $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ with $\mathbf{D}$.

Use the result from part c and your answer for $\mathbf{D}$ to set up recurrence relations for u and v .

Use standard results for recurrence relations to write down closed forms for u_n and v_n . ← Section 4.2

Use the transformation to set up a relationship between $\begin{pmatrix} x_n \\ y_n \end{pmatrix}$ and $\begin{pmatrix} u_n \\ v_n \end{pmatrix}$ in terms of $\mathbf{P}$.

Form two equations for x_n and y_n in terms of u_1 , v_1 and n .

When $n = 1$,

$$1 = u_1 + v_1$$

$$2 = u_1 - 2v_1$$

So $u_1 = \frac{4}{3}$ and $v_1 = -\frac{1}{3}$.

Hence:

$$x_n = \frac{4}{3}(5^{n-1}) - \frac{1}{3}(2^{n-1})$$

$$y_n = \frac{4}{3}(5^{n-1}) + \frac{2}{3}(2^{n-1})$$

Watch out You know the initial values of x_n and y_n , but you need to find the initial values of u_n and v_n .

Substitute $n = 1$ and solve the resulting simultaneous equations to find u_1 and v_1 .

Write the expressions for x_n and y_n in closed form.

Diagonalisation can also be used to compute large powers of matrices efficiently.

■ For a diagonal matrix $\mathbf{D} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, $\mathbf{D}^k = \begin{pmatrix} a^k & 0 \\ 0 & d^k \end{pmatrix}$.

This result holds for diagonal matrices of higher dimension as well.

Consider the matrix product $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$ where $\mathbf{D}$ is a diagonal matrix.

Then $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$ and $\mathbf{A}^k = (\mathbf{P}\mathbf{D}\mathbf{P}^{-1})^k$.

$$\begin{aligned} \mathbf{A}^k &= (\mathbf{P}\mathbf{D}\mathbf{P}^{-1})(\mathbf{P}\mathbf{D}\mathbf{P}^{-1}) \dots (\mathbf{P}\mathbf{D}\mathbf{P}^{-1}) \\ &= \mathbf{P}(\mathbf{P}^{-1}\mathbf{P})\mathbf{D}(\mathbf{P}^{-1}\mathbf{P}) \dots (\mathbf{P}^{-1}\mathbf{P})\mathbf{D}\mathbf{P}^{-1} \\ &= \mathbf{P}\mathbf{D}^k\mathbf{P}^{-1} \end{aligned}$$

Hence to calculate $\mathbf{A}^k$, you only need to find matrices $\mathbf{P}$, $\mathbf{D}$ and $\mathbf{P}^{-1}$ and apply the result from above.

Example 12

$$\mathbf{A} = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}$$

a Find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$.

b Hence find $\mathbf{A}^6$.

a Find the eigenvalues and the eigenvectors of $\mathbf{A}$:

$$\begin{vmatrix} 3-\lambda & 1 \\ 2 & 2-\lambda \end{vmatrix} = 0 \Rightarrow \lambda = 1 \text{ or } 4$$

For $\lambda = 1$, a corresponding eigenvector is $\begin{pmatrix} -1 \\ 2 \end{pmatrix}$.

For $\lambda = 4$, a corresponding eigenvector is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

$$\mathbf{P} = \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} \text{ and } \mathbf{D} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$$

$$\mathbf{A}^6 = \mathbf{P}\mathbf{D}^6\mathbf{P}^{-1}$$

$$\mathbf{P}^{-1} = \frac{1}{3} \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$\mathbf{D}^6 = \begin{pmatrix} 1 & 0 \\ 0 & 4096 \end{pmatrix}$$

Find the eigenvalues and the eigenvectors of $\mathbf{A}$ in the usual way.

Use your calculator to find the inverse of matrix $\mathbf{P}$.

Find $\mathbf{D}^6$, $4^6 = 4096$

$$\begin{aligned}
 \text{b } \mathbf{A}^{46} &= \frac{1}{3} \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4096 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} \\
 &= \frac{1}{3} \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 8192 & 4096 \end{pmatrix} \\
 &= \frac{1}{3} \begin{pmatrix} 8193 & 4095 \\ 8190 & 4098 \end{pmatrix} = \begin{pmatrix} 2731 & 1365 \\ 2730 & 1366 \end{pmatrix}.
 \end{aligned}$$

Compute the matrix product. If you were working with a larger power you could leave your elements in index form.

Exercise 5C

- 1 For each of these matrices, find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$.

a $\mathbf{A} = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix}$ b $\mathbf{A} = \begin{pmatrix} -3 & -2 \\ 5 & 4 \end{pmatrix}$

- 2 Reduce the following matrices to diagonal matrices.

a $\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$ b $\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix}$

(E) 3 $\mathbf{Q} = \begin{pmatrix} 4 & -2 \\ -1 & 3 \end{pmatrix}$

Find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{D} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$. (7 marks)

4 The matrix $\mathbf{A} = \begin{pmatrix} 3 & \sqrt{2} \\ \sqrt{2} & 4 \end{pmatrix}$.

(E) a Find the eigenvalues of $\mathbf{A}$. (3 marks)

b Find normalised eigenvectors of $\mathbf{A}$ corresponding to each of the two eigenvalues of $\mathbf{A}$. (4 marks)

c Write down a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^T\mathbf{A}\mathbf{P} = \mathbf{D}$. (2 marks)

(E/P) 5 $\mathbf{A} = \begin{pmatrix} 7 & 4 \\ 4 & 1 \end{pmatrix}$

a Show that $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} -1 \\ 2 \end{pmatrix}$ are eigenvectors of $\mathbf{A}$. (4 marks)

Adam says that because $\mathbf{A}$ is symmetric, the matrix $\mathbf{P} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ is such that $\mathbf{P}^T\mathbf{A}\mathbf{P}$ is a diagonal matrix.

b Explain Adam's mistake, and find a matrix $\mathbf{Q}$ such that $\mathbf{Q}^T\mathbf{A}\mathbf{Q}$ is diagonal. (3 marks)

(E) 6 The two sequences x_n and y_n satisfy the recurrence relations

$$\begin{aligned}
 x_{n+1} &= 2x_n + 4y_n, \quad x_1 = 3 \\
 y_{n+1} &= 3x_n + y_n, \quad y_1 = 1 \quad n \geq 1
 \end{aligned}$$

These recurrence relations can be written in matrix form as

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \mathbf{A} \begin{pmatrix} x_n \\ y_n \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} \quad n \geq 1$$

where $\mathbf{A} = \begin{pmatrix} 2 & 4 \\ 3 & 1 \end{pmatrix}$.

- a Find the eigenvalues and corresponding eigenvectors of $\mathbf{A}$. (5 marks)
 b Hence write down matrices $\mathbf{P}$ and $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$ where $\mathbf{D}$ is a diagonal matrix. (2 marks)

New sequences u_n and v_n can be formed from x_n and y_n using the transformation

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \mathbf{P}^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

- c Show that $\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \mathbf{D} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. (2 marks)
 d Hence find closed form expressions for the original sequences x_n and y_n . (5 marks)

E/P 7 $\mathbf{M} = \begin{pmatrix} 3 & -1 \\ 2 & 0 \end{pmatrix}$

- a Find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{M}\mathbf{P} = \mathbf{D}$. (7 marks)
 b Hence, or otherwise, find $\mathbf{M}^{100}$, giving each element in terms of suitable powers of 2. (5 marks)

- A** 8 For each of these matrices, find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$.

a $\mathbf{A} = \begin{pmatrix} 1 & 4 & -1 \\ -1 & 6 & -1 \\ 2 & -2 & 4 \end{pmatrix}$ b $\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 6 & -1 & 0 \\ -1 & -2 & -1 \end{pmatrix}$

Hint You can use your calculator to find $\mathbf{P}^{-1}$.

- E** 9 The matrix $\mathbf{M}$ is given by

$$\mathbf{M} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 3 & 0 \end{pmatrix}$$

- a Explain why matrix $\mathbf{M}$ is not orthogonally diagonalisable. (1 mark)
 b Show that 3 is an eigenvalue of $\mathbf{M}$ and find the other two eigenvalues. (4 marks)
 c For each of the eigenvalues, find a corresponding eigenvector. (4 marks)
 d Find a matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{M}\mathbf{P}$ is a diagonal matrix. (2 marks)

P 10 The matrix $\mathbf{P} = \begin{pmatrix} \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} \\ \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} & 0 \end{pmatrix}$.

- a Show that $\mathbf{P}$ is an orthogonal matrix.

The matrix $\mathbf{A} = \begin{pmatrix} \frac{3}{2} & -\frac{3}{2} & 1 \\ -\frac{3}{2} & \frac{3}{2} & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

- b Show that $\mathbf{P}^T\mathbf{A}\mathbf{P}$ is a diagonal matrix.

- A**
P 11 The matrix $\mathbf{A} = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$. Reduce $\mathbf{A}$ to a diagonal matrix.

- E** 12 The matrix $\mathbf{A} = \begin{pmatrix} 5 & 3 & 3 \\ 3 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix}$

The eigenvalues of $\mathbf{A}$ are 0, -1 and 8.

- a** Find a normalised eigenvector corresponding to the eigenvalue 0. (2 marks)

Given that $\begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$ is an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue -1 and that $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ is an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue 8,

- b** find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$. (3 marks)

- E** 13 The matrix $\mathbf{A} = \begin{pmatrix} 7 & 0 & -2 \\ 0 & 5 & -2 \\ -2 & -2 & 6 \end{pmatrix}$.

- a** Given that 9 is an eigenvalue of $\mathbf{A}$, find the other two eigenvalues of $\mathbf{A}$. (4 marks)

- b** Find eigenvectors of $\mathbf{A}$ corresponding to each of the three eigenvalues of $\mathbf{A}$. (4 marks)

- c** Show that the eigenvectors found in part **b** are mutually perpendicular. (2 marks)

- d** Find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^T\mathbf{A}\mathbf{P} = \mathbf{D}$. (2 marks)

- E** 14 The matrix $\mathbf{A} = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & \sqrt{5} \\ 0 & \sqrt{5} & 1 \end{pmatrix}$

- a** Show that 4 is an eigenvalue of $\mathbf{A}$ and find the other two eigenvalues of $\mathbf{A}$. (4 marks)

- b** Find a normalised eigenvector of $\mathbf{A}$ corresponding to the eigenvalue 4. (3 marks)

Given that $\begin{pmatrix} -2 \\ 3 \\ -\sqrt{5} \end{pmatrix}$ and $\begin{pmatrix} \sqrt{5} \\ 0 \\ -2 \end{pmatrix}$ are eigenvectors of $\mathbf{A}$,

- c** find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$. (3 marks)

- E** 15 The eigenvalues of the matrix

$$\mathbf{A} = \begin{pmatrix} 2 & 2 & -3 \\ 2 & 2 & 3 \\ -3 & 3 & 3 \end{pmatrix}$$

are $\lambda_1, \lambda_2, \lambda_3$, where $\lambda_1 > \lambda_2 > \lambda_3$.

- a** Show that $\lambda_1 = 6$ and find the other two eigenvalues λ_2 and λ_3 . (4 marks)

- b** Verify that $|\mathbf{A}| = \lambda_1 \lambda_2 \lambda_3$. (2 marks)

- c** Find an eigenvector corresponding to the eigenvalue $\lambda_1 = 6$. (2 marks)

- A** Given that $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$ are eigenvectors corresponding to λ_2 and λ_3 ,
- d** write down a matrix $\mathbf{P}$ such that $\mathbf{P}^T \mathbf{A} \mathbf{P}$ is a diagonal matrix. (3 marks)

Challenge

A closed ecosystem has a population of kingfishers and a population of fish. The number of kingfishers, x , and the number of fish, y , at time t years are modelled using the differential equations

$$\begin{aligned} x' &= -0.3x - 0.2y \\ y' &= -0.1x + 0.4y \end{aligned} \quad (1)$$

At time $t = 0$, the number of kingfishers is 5 and the number of fish is 20.

This information can be written in matrix form as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \mathbf{A} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 5 \\ 20 \end{pmatrix}$$

where $\mathbf{A} = \begin{pmatrix} 0.3 & -0.2 \\ -0.1 & 0.4 \end{pmatrix}$.

- Find the eigenvalues and corresponding eigenvectors of $\mathbf{A}$.
 - Hence write down matrices $\mathbf{P}$ and $\mathbf{D}$ such that $\mathbf{P} \mathbf{D} \mathbf{P}^{-1} = \mathbf{A}$, where $\mathbf{D}$ is a diagonal matrix.
- New variables u and v can be formed from x and y using the transformation
- $$\begin{pmatrix} u \\ v \end{pmatrix} = \mathbf{P}^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$
- Show that $\begin{pmatrix} u' \\ v' \end{pmatrix} = \mathbf{D} \begin{pmatrix} u \\ v \end{pmatrix}$.
 - Show that $u = c_1 e^{0.5t}$ and that $v = c_2 e^{0.2t}$ where c_1 and c_2 are unknown constants.
 - Hence solve the system (1) of differential equations.

5.3 The Cayley–Hamilton theorem

Consider the matrix $\mathbf{M} = \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix}$.

The characteristic equation for this matrix is

$$\begin{vmatrix} 1-\lambda & 3 \\ 4 & 2-\lambda \end{vmatrix} = 0 \Rightarrow (1-\lambda)(2-\lambda) - 12 = 0 \Rightarrow -10 - 3\lambda + \lambda^2 = 0$$

and $\mathbf{M}^2 = \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix} = \begin{pmatrix} 13 & 9 \\ 12 & 16 \end{pmatrix}$

Now consider the matrix expression

$$-10\mathbf{I} - 3\mathbf{M} + \mathbf{M}^2$$

where $\mathbf{I}$ is the identity matrix and $\mathbf{M}$ is the matrix above.

$$-10 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - 3 \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix} + \begin{pmatrix} 13 & 9 \\ 12 & 16 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Hence $-10\mathbf{I} - 3\mathbf{M} + \mathbf{M}^2 = \mathbf{0}$, the zero matrix.

This result illustrates the **Cayley–Hamilton theorem**.

- The Cayley–Hamilton theorem states that every square matrix $\mathbf{M}$ satisfies its own characteristic equation.

Example 13

Demonstrate that the matrix $\mathbf{A} = \begin{pmatrix} 5 & 2 \\ 3 & 3 \end{pmatrix}$ satisfies its own characteristic equation.

$$\begin{vmatrix} 5-\lambda & 2 \\ 3 & 3-\lambda \end{vmatrix} = (5-\lambda)(3-\lambda) - 6 = 9 - 8\lambda + \lambda^2$$

Find the characteristic equation of $\mathbf{A}$.

$$\mathbf{A}^2 = \begin{pmatrix} 5 & 2 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 3 & 3 \end{pmatrix} = \begin{pmatrix} 31 & 16 \\ 24 & 15 \end{pmatrix}$$

Find $\mathbf{A}^2$.

$$\begin{aligned} 9\mathbf{I} - 8\mathbf{A} + \mathbf{A}^2 &= 9\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - 8\begin{pmatrix} 5 & 2 \\ 3 & 3 \end{pmatrix} + \begin{pmatrix} 31 & 16 \\ 24 & 15 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ as required.} \end{aligned}$$

Substitute $\mathbf{I}$, $\mathbf{A}$ and $\mathbf{A}^2$ into the characteristic equation and show that it equals $\mathbf{0}$.

Example 14

Given that

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & -3 \end{pmatrix}$$

- find the characteristic equation of $\mathbf{A}$.
- Hence show that $\mathbf{A}^3 = 13\mathbf{A} - 18\mathbf{I}$.

$$\text{a } \begin{vmatrix} 1-\lambda & 2 \\ 3 & -3-\lambda \end{vmatrix} = (1-\lambda)(-3-\lambda) - 6$$

So characteristic equation is $\lambda^2 + 2\lambda - 9 = 0$.

- By the Cayley–Hamilton theorem,

$$\mathbf{A}^2 = 9\mathbf{I} - 2\mathbf{A} \quad (1)$$

$$\mathbf{A}^3 = 9\mathbf{A} - 2\mathbf{A}^2 \quad (2)$$

Substitute (1) into (2):

$$\mathbf{A}^3 = 9\mathbf{A} - 2(9\mathbf{I} - 2\mathbf{A})$$

Hence $\mathbf{A}^3 = 13\mathbf{A} - 18\mathbf{I}$ as required.

Use the Cayley–Hamilton theorem to produce an equation in $\mathbf{A}$ and $\mathbf{I}$.

Multiply both sides of (1) by $\mathbf{A}$.

Substitute for $\mathbf{A}^2$.

Example 15**A**

Given that

$$\mathbf{M} = \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

- a find the characteristic equation of $\mathbf{M}$.
 b Hence, by using the Cayley–Hamilton theorem, find $\mathbf{M}^{-1}$.

$$\begin{aligned} \text{a } \begin{vmatrix} 1-\lambda & 2 & 1 \\ -1 & -\lambda & 2 \\ 2 & 1 & -\lambda \end{vmatrix} &= (1-\lambda)(\lambda^2-2) - 2(\lambda-4) + (-1+2\lambda) \\ &= -\lambda^3 + \lambda^2 + 2\lambda + 5 \end{aligned}$$

So the characteristic equation is $\lambda^3 - \lambda^2 - 2\lambda - 5 = 0$.

- b By the Cayley–Hamilton theorem,

$$\mathbf{M}^3 - \mathbf{M}^2 - 2\mathbf{M} = 5\mathbf{I}$$

$$\Rightarrow \mathbf{M}^2 - \mathbf{M} - 2\mathbf{I} = 5\mathbf{M}^{-1} \quad (1)$$

$$\mathbf{M}^2 = \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \\ 3 & 0 & -1 \\ 1 & 4 & 4 \end{pmatrix}$$

$$\begin{aligned} \mathbf{M}^2 - \mathbf{M} - 2\mathbf{I} &= \begin{pmatrix} 1 & 3 & 5 \\ 3 & 0 & -1 \\ 1 & 4 & 4 \end{pmatrix} - \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} - \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \\ &= \begin{pmatrix} -2 & 1 & 4 \\ 4 & -2 & -3 \\ -1 & 3 & 2 \end{pmatrix} \end{aligned}$$

$$\text{Hence } \mathbf{M}^{-1} = \frac{1}{5} \begin{pmatrix} -2 & 1 & 4 \\ 4 & -2 & -3 \\ -1 & 3 & 2 \end{pmatrix}$$

Use the Cayley–Hamilton theorem.

Multiply by $\mathbf{M}^{-1}$. Remember that $\mathbf{M}\mathbf{M}^{-1} = \mathbf{I}$ and $\mathbf{I}\mathbf{M}^{-1} = \mathbf{M}^{-1}$.

Find $\mathbf{M}^2$, substitute into equation (1) and solve for $\mathbf{M}^{-1}$.

Exercise 5D

- 1 Demonstrate that the following matrices satisfy their own characteristic equations:

a $\begin{pmatrix} 3 & 4 \\ -1 & 2 \end{pmatrix}$

b $\begin{pmatrix} -2 & 1 \\ 3 & 0 \end{pmatrix}$

c $\begin{pmatrix} 7 & -4 \\ 0 & 3 \end{pmatrix}$

- E** 2 Given that

$$\mathbf{A} = \begin{pmatrix} 6 & 2 \\ -1 & 3 \end{pmatrix}$$

- a find the characteristic equation of $\mathbf{A}$. (2 marks)
 b Hence show that $\mathbf{A}^3 = 61\mathbf{A} - 180\mathbf{I}$. (3 marks)

- E** 3 Given that

$$\mathbf{M} = \begin{pmatrix} 4 & -2 \\ 0 & 6 \end{pmatrix}$$

- a find the characteristic equation of $\mathbf{M}$. (2 marks)
 b Hence, use the Cayley–Hamilton theorem to find $\mathbf{M}^{-1}$. (3 marks)

E/P 4 $\mathbf{A} = \begin{pmatrix} 6 & 3 \\ 0 & 4 \end{pmatrix}$

Find the values of p and q such that $\mathbf{A} = p\mathbf{A}^2 + q\mathbf{I}$. (3 marks)

- A** 5 Demonstrate that the following matrices satisfy their own characteristic equations.

a $\begin{pmatrix} 1 & 0 & 1 \\ 2 & 2 & 2 \\ 0 & -1 & 3 \end{pmatrix}$

b $\begin{pmatrix} 7 & 2 & -1 \\ 0 & -1 & 3 \\ 1 & 0 & 2 \end{pmatrix}$

- E** 6 Given that

$$\mathbf{M} = \begin{pmatrix} 1 & 4 & 1 \\ 2 & 0 & -1 \\ 3 & 2 & 0 \end{pmatrix}$$

- a show that the characteristic equation of $\mathbf{M}$ can be written as $\lambda^3 = \lambda^2 + 9\lambda - 6$. (3 marks)
 b Hence show that $\mathbf{M}^4 = 10\mathbf{M}^2 + 3\mathbf{M} - 6\mathbf{I}$. (3 marks)

- E** 7 Given that

$$\mathbf{A} = \begin{pmatrix} -1 & 1 & 1 \\ -2 & 0 & 4 \\ 4 & -1 & 3 \end{pmatrix}$$

- a find the characteristic equation of $\mathbf{A}$. (3 marks)
 b Show that $\mathbf{A}^2 - 2\mathbf{A} - \mathbf{I} = 20\mathbf{A}^{-1}$. (3 marks)
 c Hence find $\mathbf{A}^{-1}$. (3 marks)

E/P 8 $\mathbf{M} = \begin{pmatrix} -3 & 2 & -1 \\ 1 & 2 & 3 \\ 1 & 0 & 0 \end{pmatrix}$

Find the values of a , b and c such that $\mathbf{M} = a\mathbf{M}^3 + b\mathbf{M}^2 + c\mathbf{I}$. (4 marks)

Challenge

Show that any 2×2 matrix of the form $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies its own characteristic equation and hence prove the Cayley–Hamilton theorem for 2×2 matrices.

Problem-solving

You can change the scalar 0 into the zero matrix $\mathbf{0}$ by multiplying by the identity matrix: $0\mathbf{I} = \mathbf{0}$.

Mixed exercise 5

- (E)** 1 The matrix $\mathbf{M} = \begin{pmatrix} 1 & 8 \\ 8 & -11 \end{pmatrix}$ has eigenvalues $\lambda_1 = 5$ and $\lambda_2 = -15$.
- a For each eigenvalue, find a corresponding eigenvector. (4 marks)
- b Find a matrix $\mathbf{P}$ such that $\mathbf{P}^T \mathbf{A} \mathbf{P} = \begin{pmatrix} 5 & 0 \\ 0 & -15 \end{pmatrix}$. (3 marks)

- (E)** 2 A transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is represented by the matrix

$$\mathbf{A} = \begin{pmatrix} -5 & 8 \\ 3 & -7 \end{pmatrix}$$

- a Find the eigenvalues of $\mathbf{A}$. (3 marks)
- b Find Cartesian equations of the two lines passing through the origin which are invariant under T . (3 marks)

- (E/P)** 3 The matrix $\mathbf{A} = \begin{pmatrix} 4 & k \\ 2 & -2 \end{pmatrix}$ has a repeated eigenvalue.

- a Find the value of k . (4 marks)
- b Hence find any eigenvectors for the matrix $\mathbf{A}$. (3 marks)

The matrix represents a transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$.

- c Find the Cartesian equation of any lines passing through the origin that are invariant under the transformation T . (2 marks)

- (E/P)** 4 The matrix $\mathbf{M} = \begin{pmatrix} a & a \\ 2 & 1 \end{pmatrix}$ has complex eigenvalues.

- a Find the set of possible values of a . (6 marks)
- b Given that $a = -1$, find the eigenvectors of $\mathbf{M}$. (4 marks)

The matrix represents a transformation $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$.

- c Explain why there are no invariant lines under the transformation T . (1 mark)

- (E)** 5 The matrix $\mathbf{A}$ is given by

$$\mathbf{A} = \begin{pmatrix} 4 & -3 \\ 2 & -1 \end{pmatrix}$$

- a Show that 2 is an eigenvalue of $\mathbf{A}$ and find a corresponding eigenvector. (4 marks)

Given that the other eigenvalue of $\mathbf{A}$ is 1,

- b find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{D} = \mathbf{P}^{-1} \mathbf{A} \mathbf{P}$. (4 marks)

- (E)** 6 The two sequences x_n and y_n satisfy the recurrence relations

$$x_{n+1} = 2x_n - y_n, \quad x_1 = 2$$

$$y_{n+1} = 4x_n - 3y_n, \quad y_1 = 3 \quad n \geq 1$$

These recurrence relations can be written in matrix form as

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \mathbf{A} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \quad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad n \geq 1$$

where $\mathbf{A} = \begin{pmatrix} 2 & -1 \\ 4 & -3 \end{pmatrix}$.

a Find the eigenvalues and corresponding eigenvectors of $\mathbf{A}$. (5 marks)

b Hence write down matrices $\mathbf{P}$ and $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$ where $\mathbf{D}$ is a diagonal matrix. (2 marks)

New sequences u_n and v_n can be formed from x_n and y_n using the transformation

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \mathbf{P}^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

c Show that $\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \mathbf{D} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. (2 marks)

d Hence find closed form expressions for the original sequences x_n and y_n . (5 marks)

E/P 7 $\mathbf{A} = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$

a Find a matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$. (5 marks)

b Hence, or otherwise, find $\mathbf{A}^{50}$. (3 marks)

E 8 Given that

$$\mathbf{A} = \begin{pmatrix} 4 & 5 \\ -1 & 2 \end{pmatrix}$$

a Find the characteristic equation of $\mathbf{A}$. (2 marks)

b Hence show that $\mathbf{A}^3 = 23\mathbf{A} - 78\mathbf{I}$. (3 marks)

E/P 9 $\mathbf{A} = \begin{pmatrix} 7 & 1 \\ -1 & 2 \end{pmatrix}$

Find the values of p and q such that $\mathbf{A} = p\mathbf{A}^2 + q\mathbf{I}$. (3 marks)

A 10 Given that 1 is an eigenvalue of the matrix

$$\begin{pmatrix} 3 & 1 & 0 \\ 2 & 4 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

a find a corresponding eigenvector (2 marks)

b find the other eigenvalues of the matrix. (3 marks)

E 11 $\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & -1 \\ -6 & -5 & -3 \end{pmatrix}$

a Find the eigenvalues of matrix $\mathbf{A}$ and hence find a set of eigenvectors. (7 marks)

Matrix $\mathbf{A}$ represents a transformation $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$.

b Explain why every linear transformation from $\mathbb{R}^3$ to $\mathbb{R}^3$ must have at least one invariant line. (1 mark)

c Find the vector equations of the invariant lines under T . (3 marks)

A
E 12 $\mathbf{A} = \begin{pmatrix} 2 & 0 & 2 \\ 2 & 2 & 0 \\ 0 & 1 & 3 \end{pmatrix}$

a Show that 4 is an eigenvalue of $\mathbf{A}$ and find the other two eigenvalues. (4 marks)

b Find the corresponding eigenvectors of $\mathbf{A}$. (4 marks)

Matrix $\mathbf{A}$ represents a transformation $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$.

c Write down the vector equations of any invariant lines under T . (2 marks)

13 The matrix $\mathbf{M}$ is given by

E $\mathbf{M} = \begin{pmatrix} 4 & 1 & -1 \\ 1 & 0 & 3 \\ 1 & 2 & 1 \end{pmatrix}$

a Show that -2 is an eigenvalue of $\mathbf{M}$ and find the other two eigenvalues. (4 marks)

b For each of the eigenvalues, find a corresponding eigenvector. (4 marks)

c Find a matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{M}\mathbf{P}$ is a diagonal matrix and write down the diagonal matrix $\mathbf{D}$. (3 marks)

E 14 $\mathbf{A} = \begin{pmatrix} 3 & 4 & -4 \\ 4 & 5 & 0 \\ -4 & 0 & 1 \end{pmatrix}$

a Show that 3 is an eigenvalue of $\mathbf{A}$ and find the other two eigenvalues. (4 marks)

b Find an eigenvector corresponding to the eigenvalue 3. (2 marks)

Given that the vectors $\begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix}$ are eigenvectors corresponding to the other two eigenvalues,

c find a matrix $\mathbf{P}$ such that $\mathbf{P}^T \mathbf{A} \mathbf{P}$ is a diagonal matrix. (3 marks)

E 15 $\mathbf{A} = \begin{pmatrix} 2 & -2 & 0 \\ -2 & 1 & 2 \\ 0 & 2 & 5 \end{pmatrix}$

a Show that $\begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$ are eigenvectors of $\mathbf{A}$, giving their corresponding eigenvalues. (4 marks)

b Given that 6 is the third eigenvalue of $\mathbf{A}$, find a corresponding eigenvector. (2 marks)

c Hence write down a matrix such that $\mathbf{P}^{-1} \mathbf{A} \mathbf{P}$ is a diagonal matrix. (3 marks)

16 **a** Show that for all values of the constant α , an eigenvalue of the matrix $\mathbf{A}$ is 1, where

E $\mathbf{A} = \begin{pmatrix} \alpha & 0 & 2 \\ 4 & 3 & 0 \\ -2 & -1 & 1 \end{pmatrix}$ (3 marks)

An eigenvector of the matrix $\mathbf{A}$ is $\begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}$ and the corresponding eigenvalue is β ($\beta \neq 1$).

- A** b Find the value of α and the value of β . (4 marks)
 c For your value of α , find the third eigenvalue of $\mathbf{A}$. (2 marks)

E 17 $\mathbf{M} = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 2 & 0 \\ 0 & 1 & 3 \end{pmatrix}$

- a Show that the matrix $\mathbf{M}$ has only two distinct eigenvalues. (4 marks)
 b Find a set of eigenvectors for the matrix. (4 marks)

- E** 18 a Determine the eigenvalues of the matrix

$$\mathbf{A} = \begin{pmatrix} 3 & -3 & 6 \\ 0 & 2 & -8 \\ 0 & 0 & -2 \end{pmatrix} \quad (4 \text{ marks})$$

- b Show that $\begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$ is an eigenvector of $\mathbf{A}$. (2 marks)

$$\mathbf{B} = \begin{pmatrix} 7 & -6 & 2 \\ 1 & 2 & 3 \\ 1 & -3 & 2 \end{pmatrix}$$

- c Show that $\begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$ is an eigenvector of $\mathbf{B}$ and write down the corresponding eigenvalue. (3 marks)

- d Hence, or otherwise, write down an eigenvector of the matrix $\mathbf{AB}$, and state the corresponding eigenvalue. (2 marks)

- 19 Given that

E $\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ 3 & 3 & -3 \end{pmatrix}$

- a Find the characteristic equation of $\mathbf{A}$. (3 marks)
 b Show that $\mathbf{A}^2 + 2\mathbf{A} + 11\mathbf{I} = -6\mathbf{A}^{-1}$. (3 marks)
 c Hence find $\mathbf{A}^{-1}$. (3 marks)

Challenge

The **trace** (tr) of a matrix is defined as the sum of the elements along the leading diagonal.

Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$

- a Show that $\text{tr}(\mathbf{AB}) = \text{tr}(\mathbf{BA})$.
 b Hence prove that, if there exists a non-singular matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{MP} = \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$, then the trace of matrix $\mathbf{M}$ is equal to $p + q$.

Summary of key points

- 1 An **eigenvector** of a matrix **A** is a non-zero column vector **x** which satisfies the equation $\mathbf{Ax} = \lambda \mathbf{x}$, where λ is a scalar.
The value of the scalar λ is the eigenvalue of the matrix corresponding to the eigenvector **x**.
- 2 If **x** is an eigenvector of a matrix **M** representing a linear transformation, then the straight line that passes through the origin in the direction of **x** is an invariant line under that transformation.
- 3 The equation $\det(\mathbf{A} - \lambda \mathbf{I}) = 0$ is called the **characteristic equation** of **A**. The solutions to the characteristic equation are the eigenvalues of **A**.

- 4 If $\mathbf{a} = \begin{pmatrix} a \\ b \end{pmatrix}$ is an eigenvector of a matrix **A**, then the unit vector $\hat{\mathbf{a}} = \begin{pmatrix} \frac{a}{|\mathbf{a}|} \\ \frac{b}{|\mathbf{a}|} \end{pmatrix}$ is a **normalised eigenvector** of **A**.

- 5 A **diagonal matrix** is a square matrix in which all of the elements which are not on the diagonal from the top left to the bottom right of the matrix are zero. The diagonal from the top left to the bottom right of the matrix is called the **leading diagonal**.



The general 2×2 diagonal matrix is $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

- 6 To reduce a given matrix **A** to diagonal form, use the following procedure:
 - Find the eigenvalues and eigenvectors of **A**.
 - Form a matrix **P** which consists of the eigenvectors of **A**.
 - Find $\mathbf{P}^{-1}$.
 - A diagonal matrix **D** is given by $\mathbf{P}^{-1}\mathbf{AP}$.
- 7 When you reduce a matrix **A** to a diagonal matrix **D**, the elements on the diagonal are the eigenvalues of **A**.
- 8 A matrix, **A**, is **symmetric** if $\mathbf{A} = \mathbf{A}^T$. The elements of a symmetric matrix are symmetric with respect to the leading diagonal.
- 9 The procedure for **orthogonal diagonalisation** of a symmetric matrix **A** is:
 - Find the normalised eigenvectors of **A**.
 - Form a matrix **P** which consists of the normalised eigenvectors of **A**.
 - Write down $\mathbf{P}^T$.
 - A diagonal matrix **D** is given by $\mathbf{P}^T\mathbf{AP}$.
- 10 For a diagonal matrix $\mathbf{D} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, $\mathbf{D}^k = \begin{pmatrix} a^k & 0 \\ 0 & d^k \end{pmatrix}$.
- 11 The **Cayley–Hamilton theorem** states that every square matrix **M** satisfies its own characteristic equation.

Integration techniques

6

Objectives

After completing this chapter you should be able to:

- derive and use integration reduction formulae → pages 00-00
- use integration to calculate the length of an arc → pages 00-00
- use integration to calculate the area of a surface of revolution → pages 00-00

The solid formed by revolving the curve $y = \frac{1}{x}$, $x > 0$ about the x -axis has infinite surface area, but finite volume. This shape is sometimes called Torricelli's Trumpet, after Evangelista Torricelli who discovered these results in the 17th century.

→ Exercise 6C Challenge

Prior knowledge check

- 1 a** By considering $\sin(x + 2x)$, show that $\sin^3 x \equiv \frac{3}{4} \sin x - \frac{1}{4} \sin 3x$
b Hence, or otherwise find $\int \sin^3 x \, dx$.
← Pure Year 2, Sections 11.3, 11.4
- 2** Use integration by parts to find:
a $\int x \cos x \, dx$
b $\int x \sqrt{1-x} \, dx$
c $\int \frac{\sin x}{e^x} \, dx$ ← Pure Year 2, Section 11.6
- 3** Use the substitution $x = \sinh u$ to find $\int \sqrt{1+x^2} \, dx$
← Pure Year 2, Section 11.5
← Core Pure Book 2, Chapter 6
- 4** Evaluate $\int_0^{\ln 2} x \sqrt{1 + \sinh^2 x} \, dx$.
← Core Pure Book 2, Section 6.5

6.1 Reduction formulae

A In your A level course you used trigonometric identities to find indefinite integrals such as $\int \sin^2 x \, dx$, and integration by parts to find indefinite integrals such as $\int x^2 e^x \, dx$. However, when integrals similar to these involve higher powers, such as $\int \sin^5 x \, dx$, or $\int x^4 e^x \, dx$, the working can become very tedious.

In some cases, you can write an integral such as $\int \sin^n x \, dx$ or $\int x^n e^x \, dx$ in terms of similar integrals involving lower powers. A relationship such as this is called a **reduction formula**.

- A reduction formula allows you to write a recurrence relation for an integral $I_n = \int f(x, n) \, dx$ in terms of related integrals I_{n-1} , I_{n-2} , etc.

Links You need to be able to apply the formula for integration by parts:

$$\int u \frac{dv}{dx} \, dx = uv - \int v \frac{du}{dx} \, dx$$

← Pure Year 2, Section 11.6

Notation The symbol I_n is used to represent an integral involving a parameter n . Usually the parameter will appear as a power of n .

By applying such a formula repeatedly, you can eventually express the integral in terms of a value of n low enough so that you can find it directly.

Example 1

Given that $I_n = \int x^n e^x \, dx$, where n is a positive integer,

- show that $I_n = x^n e^x - nI_{n-1}$, $n \geq 1$
- Hence find $\int x^4 e^x \, dx$.

a Let $u = x^n$ and $\frac{dv}{dx} = e^x$

So that $\frac{du}{dx} = nx^{n-1}$ and $v = e^x$

$$\begin{aligned} \text{Then } I_n &= \int x^n e^x \, dx = x^n e^x - \int nx^{n-1} e^x \, dx \\ &= x^n e^x - n \int x^{n-1} e^x \, dx \\ I_n &= x^n e^x - nI_{n-1} \end{aligned}$$

b $\int x^4 e^x \, dx = I_4$

$$\begin{aligned} I_4 &= x^4 e^x - 4I_3 \\ &= x^4 e^x - 4(x^3 e^x - 3I_2) \\ &= x^4 e^x - 4x^3 e^x + 12(x^2 e^x - 2I_1) \\ &= x^4 e^x - 4x^3 e^x + 12x^2 e^x - 24(xe^x - I_0) \\ &= x^4 e^x - 4x^3 e^x + 12x^2 e^x - 24xe^x + 24 \int e^x \, dx \\ &= x^4 e^x - 4x^3 e^x + 12x^2 e^x - 24xe^x + 24e^x + c \end{aligned}$$

Substitute $I_0 = \int e^x \, dx$

Apply the integration by parts formula. x^n reduces in power by 1 when it is differentiated, so choose x^n for u and e^x for $\frac{dv}{dx}$

This is the reduction formula for I_n . Note how the general integral I_n is written in terms of the same integral but with n reduced by 1. Since the formula reduces n by 1 each time it is applied, after applying the reduction formula a sufficient number of times it is possible to eventually express I_n in terms of I_0 , which is $\int e^x \, dx$, a standard integral that can be found directly.

Apply the reduction formula from part **a**.

Use $I_n = x^n e^x - nI_{n-1}$ with $n = 3$.

Use $I_n = x^n e^x - nI_{n-1}$ with $n = 2$.

Use $I_n = x^n e^x - nI_{n-1}$ with $n = 1$.

Example 2

- A** a Show that, if $I_n = \int \sin^n x \, dx$, then $I_n = -\frac{1}{n} \sin^{n-1} x \cos x + \frac{n-1}{n} I_{n-2}$
 b Apply the reduction formula found in part a to find $\int \sin^4 x \, dx$.

a Let $u = \sin^{n-1} x$ and $\frac{dv}{dx} = \sin x$
 So $\frac{du}{dx} = (n-1) \sin^{n-2} x \cos x$ and $v = -\cos x$
 Then $I_n = \int \sin^n x \, dx$

$$= -\sin^{n-1} x \cos x + \int (n-1) \sin^{n-2} x \cos^2 x \, dx$$

$$= -\sin^{n-1} x \cos x + (n-1) \int \sin^{n-2} x (1 - \sin^2 x) \, dx$$

$$= -\sin^{n-1} x \cos x + (n-1) \int \sin^{n-2} x \, dx - (n-1) \int \sin^n x \, dx$$

$$= -\sin^{n-1} x \cos x + (n-1) I_{n-2} - (n-1) I_n$$

$$\Rightarrow I_n + (n-1) I_n = -\sin^{n-1} x \cos x + (n-1) I_{n-2}$$

$$n I_n = -\sin^{n-1} x \cos x + (n-1) I_{n-2}$$

$$I_n = -\frac{1}{n} \sin^{n-1} x \cos x + \frac{n-1}{n} I_{n-2} \text{ as required}$$

b $\int \sin^4 x \, dx = -\frac{1}{4} \sin^3 x \cos x + \frac{3}{4} \int \sin^2 x \, dx$

$$= -\frac{1}{4} \sin^3 x \cos x + \frac{3}{4} \int \frac{1}{2} (1 - \cos 2x) \, dx$$

$$= -\frac{1}{4} \sin^3 x \cos x + \frac{3}{8} \int dx - \frac{3}{8} \int \cos 2x \, dx$$

$$= -\frac{1}{4} \sin^3 x \cos x + \frac{3}{8} x - \frac{3}{16} \sin 2x + c$$

Problem-solving

To use integration by parts, it's necessary to express the integrand $\sin^n x$ as a product. Do this by writing $\sin^n x$ as $\sin^{n-1} x \sin x$.

Differentiate $\sin^{n-1} x$ using the chain rule. Be careful with negative signs when carrying out integration by parts.

Substitute $\cos^2 x = 1 - \sin^2 x$ to express the integral as powers of $\sin x$ only

Substitute I_{n-2} for $\int \sin^{n-2} x \, dx$, and I_n for $\int \sin^n x \, dx$.

Collect terms with I_n on the left side of the equation.

Substitute $n = 4$ into the reduction formula $I_n = -\frac{1}{n} \sin^{n-1} x \cos x + \frac{n-1}{n} I_{n-2}$

Substitute $\frac{1}{2}(1 - \cos 2x) = \sin^2 x$

Sometimes, after using integration by parts, you may need to use an algebraic or trigonometric identity to produce the reduction formula.

Example 3

Show that, if $I_n = \int_0^1 x^n \sqrt{1-x} \, dx$, then $I_n = \frac{2n}{2n+3} I_{n-1}$, $n \geq 1$.

Let $u = x^n$ $\frac{dv}{dx} = \sqrt{1-x}$
 So $\frac{du}{dx} = nx^{n-1}$ $v = -\frac{2}{3}(1-x)^{\frac{3}{2}}$
 Then, integrating by parts,

$$I_n = \left[-\frac{2}{3} x^n (1-x)^{\frac{3}{2}} \right]_0^1 + \int_0^1 \frac{2}{3} nx^{n-1} (1-x)^{\frac{3}{2}} \, dx$$

$$= [0 - 0] + \int_0^1 \frac{2}{3} nx^{n-1} (1-x)^{\frac{3}{2}} \, dx$$

Watch out

This is a **definite integral**. When you use integration by parts to evaluate a definite integral you have to evaluate uv between the given limits.

If $n \geq 1$, $[\dots]_0^1 = 0$.

You need to write this so that the term $\sqrt{1-x}$ appears.

A

$$\begin{aligned}
 I_n &= \frac{2n}{3} \int_0^1 x^{n-1} (1-x) \sqrt{1-x} \, dx \\
 &= \frac{2n}{3} \int_0^1 x^{n-1} \sqrt{1-x} \, dx - \frac{2n}{3} \int_0^1 x^n \sqrt{1-x} \, dx \\
 &= \frac{2n}{3} I_{n-1} - \frac{2n}{3} I_n \\
 \text{So } (3 + 2n)I_n &= 2nI_{n-1} \\
 I_n &= \frac{2n}{2n+3} I_{n-1}
 \end{aligned}$$

Use the identity $(1-x)^{\frac{3}{2}} \equiv (1-x)\sqrt{1-x}$ Collect together terms in I_n .**Example 4** $I_n = \int \tan^n x \, dx$, where n is a positive integer.By writing $\tan^n x$ as $\tan^{n-2} x \tan^2 x$, and using $1 + \tan^2 x \equiv \sec^2 x$, establish the reduction formula

$$I_n = \frac{1}{n-1} \tan^{n-1} x - I_{n-2}, \quad n \geq 2$$

$$\begin{aligned}
 I_n &= \int \tan^{n-2} x \tan^2 x \, dx = \int \tan^{n-2} x (\sec^2 x - 1) \, dx \\
 &= \int \tan^{n-2} x \sec^2 x \, dx - \int \tan^{n-2} x \, dx
 \end{aligned}$$

$$\text{So } I_n = \frac{1}{n-1} \tan^{n-1} x - I_{n-2}$$

Use $\int (f(x))^n f'(x) \, dx = \frac{f(x)^{n+1}}{n+1} + c$ **Example 5**Consider the general definite integral $I_n = \int_0^{\frac{\pi}{2}} \sin^n x \, dx$.**a** Prove that, for $n \geq 2$, $nI_n = (n-1)I_{n-2}$ **b** Find the values of **i** $\int_0^{\frac{\pi}{2}} \sin^5 x \, dx$ **ii** $\int_0^{\frac{\pi}{2}} \sin^6 x \, dx$ **a** From Example 2, part **a**, we know that

$$\begin{aligned}
 I_n &= [-\sin^{n-1} x \cos x]_0^{\frac{\pi}{2}} + (n-1) \int_0^{\frac{\pi}{2}} \sin^{n-2} x \, dx - (n-1) \int_0^{\frac{\pi}{2}} \sin^n x \, dx \\
 &= [0 - 0] + (n-1) \int_0^{\frac{\pi}{2}} \sin^{n-2} x \, dx - (n-1) \int_0^{\frac{\pi}{2}} \sin^n x \, dx \\
 &= (n-1) \int_0^{\frac{\pi}{2}} \sin^{n-2} x \, dx - (n-1) \int_0^{\frac{\pi}{2}} \sin^n x \, dx
 \end{aligned}$$

$$I_n = (n-1)I_{n-2} - (n-1)I_n$$

$$\Rightarrow I_n + (n-1)I_n = (n-1)I_{n-2}$$

So $nI_n = (n-1)I_{n-2}$, $n \geq 2$ as required.**b** As $I_{n-2} = \left(\frac{n-3}{n-2}\right)I_{n-4}$, $n \geq 4$,

$$I_n = \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)I_{n-4} = \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\left(\frac{n-5}{n-4}\right)I_{n-6}$$

and so on.

Watch out These are definite integrals, so your answers will be numerical values, and not functions of x .The same working from Example 2, part **a**, can be applied here to arrive at the definite integral to be evaluated from $x = 0$ to $x = \frac{\pi}{2}$ Collect terms in I_n and I_{n-2} .

A

If n is odd,

$$\begin{aligned}
 I_n &= \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\cdots\left(\frac{2}{3}\right)I_1 \\
 &= \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\cdots\left(\frac{2}{3}\right)\int_0^{\frac{\pi}{2}} \sin x \, dx \\
 &= \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\cdots\left(\frac{2}{3}\right)(1) \quad (1)
 \end{aligned}$$

If n is even,

$$\begin{aligned}
 I_n &= \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\cdots\left(\frac{3}{4}\right)\left(\frac{1}{2}\right)I_0 \\
 &= \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\cdots\left(\frac{3}{4}\right)\left(\frac{1}{2}\right)\int_0^{\frac{\pi}{2}} 1 \, dx \\
 &= \left(\frac{n-1}{n}\right)\left(\frac{n-3}{n-2}\right)\cdots\left(\frac{3}{4}\right)\left(\frac{1}{2}\right)\left(\frac{\pi}{2}\right) \quad (2)
 \end{aligned}$$

$$\text{i } \int_0^{\frac{\pi}{2}} \sin^5 x \, dx = I_5$$

$$= \left(\frac{4}{5}\right)\left(\frac{2}{3}\right)(1) = \frac{8}{15}$$

Use (1) with $n = 5$.

$$\text{ii } \int_0^{\frac{\pi}{2}} \sin^6 x \, dx = I_6$$

$$= \left(\frac{5}{6}\right)\left(\frac{3}{4}\right)\left(\frac{1}{2}\right)\left(\frac{\pi}{2}\right) = \frac{5\pi}{32}$$

Use (2) with $n = 6$.**Example 6**Given $I_n = \int_0^{\ln 2} \tanh^n x \, dx$, $n \geq 1$

$$\text{a Show that } I_n = I_{n-2} - \frac{1}{n-1} \left(\frac{3}{5}\right)^{n-1}, \quad n \geq 2$$

$$\text{b Hence, show that } \sum_{r=1}^{\infty} \frac{1}{2^r} \left(\frac{3}{5}\right)^{2r} = \ln\left(\frac{5}{4}\right)$$

You may assume that $\lim_{n \rightarrow \infty} \int_0^{\ln 2} \tanh^n x \, dx = 0$.**Problem-solving**

To answer part **a**, you need to recognize that starting with the same approach used in Example 4 for the derivation of a reduction formula for $\int \tan^n x \, dx$ will be useful. In this case, you can substitute $1 - \operatorname{sech}^2 x$ for $\tanh^2 x$ after rewriting the integrand to include a factor of $\tanh^2 x$.

$$\begin{aligned}
 \text{a } I_n &= \int_0^{\ln 2} \tanh^n x \, dx \\
 &= \int_0^{\ln 2} \tanh^{n-2} x \tanh^2 x \, dx \\
 &= \int_0^{\ln 2} \tanh^{n-2} x (1 - \operatorname{sech}^2 x) \, dx \\
 &= \int_0^{\ln 2} \tanh^{n-2} x \, dx - \int_0^{\ln 2} \tanh^{n-2} x \operatorname{sech}^2 x \, dx \\
 &= I_{n-2} - \frac{1}{n-1} [\tanh^{n-1} x]_0^{\ln 2} \\
 &= I_{n-2} - \frac{1}{n-1} (\tanh(\ln 2))^{n-1} \\
 &= I_{n-2} - \frac{1}{n-1} \left(\frac{e^{2\ln 2} - 1}{e^{2\ln 2} + 1} \right)^{n-1} \\
 I_n &= I_{n-2} - \frac{1}{n-1} \left(\frac{4-1}{4+1} \right)^{n-1} = I_{n-2} - \frac{1}{n-1} \left(\frac{3}{5} \right)^{n-1} \text{ as required}
 \end{aligned}$$

$$\begin{aligned}
 &\text{Using } \int (f(x))^n f'(x) \, dx \\
 &= \frac{1}{n+1} f(x)^{n+1}, \text{ gives} \\
 &\int \tanh^{n-2} x \operatorname{sech}^2 x \, dx \\
 &= \frac{1}{n-1} \tanh^{n-1} x
 \end{aligned}$$

$$\text{Use the definition, } \tanh x = \frac{e^{2x} - 1}{e^{2x} + 1}$$

A

$$b \quad \frac{1}{2r} \left(\frac{3}{5}\right)^{2r} = I_{2r-1} - I_{2r+1}$$

$$\sum_{r=1}^k \frac{1}{2r} \left(\frac{3}{5}\right)^{2r} = \sum_{r=1}^k I_{2r-1} - I_{2r+1}$$

$$\text{Put } r=1 \quad I_1 - \cancel{I_3}$$

$$r=2 \quad \cancel{I_3} - \cancel{I_5}$$

$$r=3 \quad \cancel{I_5} - \cancel{I_7}$$

$$\vdots$$

$$r=k \quad \cancel{I_{2k-1}} - I_{2k+1}$$

$$\text{So } \sum_{r=1}^k \frac{1}{2r} \left(\frac{3}{5}\right)^{2r} = I_1 - I_{2k+1}$$

$$\text{Thus } \sum_{r=1}^{\infty} \frac{1}{2r} \left(\frac{3}{5}\right)^{2r} = I_1 - \lim_{k \rightarrow \infty} I_{2k+1}$$

$$= I_1$$

$$\text{So } \sum_{r=1}^{\infty} \frac{1}{2r} \left(\frac{3}{5}\right)^{2r} = \int_0^{\ln 2} \tanh x \, dx$$

$$= [\ln \cosh x]_0^{\ln 2}$$

$$= \ln(\cosh(\ln 2)) - \ln(\cosh(0))$$

$$= \ln\left(\frac{e^{\ln 2} + e^{-\ln 2}}{2}\right) - \ln(1)$$

$$= \ln\left(\frac{2 + \frac{1}{2}}{2}\right) - 0$$

$$= \ln\left(\frac{5}{4}\right) \text{ as required.}$$

Substitute $n = 2r + 1$ into the reduction formula and write $\frac{1}{2r} \left(\frac{3}{5}\right)^{2r}$ in terms of I_{2r-1} and I_{2r+1} .

Problem-solving

Use the **method of differences** to simplify the finite series. ← **Core Pure Book 2, Section 2.1**

Find an expression for the infinite series.

As $\lim_{n \rightarrow \infty} \int_0^{\ln 2} \tanh^n x \, dx = 0$, then $\lim_{k \rightarrow \infty} I_{2k+1} = 0$.

The derivation of some reduction formulae will require clever substitutions and/or algebraic manipulations. Often, in such cases, the question will guide you to a successful strategy.

Example 7

A general indefinite integral is defined as $I_n = \int \frac{\sin nx}{\sin x} \, dx$, $n \geq 1$

a By considering $I_{n+2} - I_n$, show that $I_{n+2} = \frac{2 \sin((n+1)x)}{n+1} + I_n$

b Hence, show that $\int_{\frac{\pi}{4}}^{\frac{\pi}{3}} \frac{\sin 6x}{\sin x} \, dx = \frac{1}{15}(12\sqrt{3} - 17\sqrt{2})$

$$\begin{aligned} a \quad I_{n+2} - I_n &= \int \frac{\sin((n+2)x)}{\sin x} \, dx - \int \frac{\sin nx}{\sin x} \, dx \\ &= \int \frac{\sin((n+2)x) - \sin nx}{\sin x} \, dx \\ &= \int \frac{2 \cos\left(\frac{(n+2)x + nx}{2}\right) \sin\left(\frac{(n+2)x - nx}{2}\right)}{\sin x} \, dx \\ &= \int \frac{2 \cos((n+1)x) \sin x}{\sin x} \, dx \\ &= \int 2 \cos((n+1)x) \, dx \\ &= \frac{2}{n+1} \sin((n+1)x) \\ \text{So } I_{n+2} &= \frac{2 \sin((n+1)x)}{n+1} + I_n \text{ as required} \end{aligned}$$

Problem-solving

Use $\sin A - \sin B = 2 \cos\left(\frac{A+B}{2}\right) \sin\left(\frac{A-B}{2}\right)$ with $A = (n+2)x$ and $B = nx$. This can be found in the formula booklet.

A

$$\begin{aligned}
 \text{b } I_6 &= \int \frac{\sin 6x}{\sin x} dx \\
 I_6 &= I_{4+2} = \frac{2 \sin 5x}{5} + I_4 \\
 &= \frac{2 \sin 5x}{5} + I_{2+2} \\
 &= \frac{2 \sin 5x}{5} + \frac{2 \sin 3x}{3} + I_2 \\
 &= \frac{2 \sin 5x}{5} + \frac{2 \sin 3x}{3} + I_{0+2} \\
 &= \frac{2 \sin 5x}{5} + \frac{2 \sin 3x}{3} + \frac{2 \sin x}{1} + I_0 \\
 &= \frac{2 \sin 5x}{5} + \frac{2 \sin 3x}{3} + 2 \sin x + \int \frac{\sin 0}{\sin x} dx \\
 &= \frac{2 \sin 5x}{5} + \frac{2 \sin 3x}{3} + 2 \sin x + 0
 \end{aligned}$$

$$\begin{aligned}
 \text{Thus, } \int_{\frac{\pi}{4}}^{\frac{5\pi}{3}} \frac{\sin 6x}{\sin x} dx &= \left[\frac{2 \sin 5x}{5} + \frac{2 \sin 3x}{3} + 2 \sin x \right]_{\frac{\pi}{4}}^{\frac{5\pi}{3}} \\
 &= \left(\frac{2 \sin\left(\frac{5\pi}{3}\right)}{5} + \frac{2 \sin \pi}{3} + 2 \sin \frac{\pi}{3} \right) - \\
 &\quad \left(\frac{2 \sin\left(\frac{5\pi}{4}\right)}{5} + \frac{2 \sin\left(\frac{3\pi}{4}\right)}{3} + 2 \sin \frac{\pi}{4} \right) \\
 &= \left(\frac{2\left(-\frac{\sqrt{3}}{2}\right)}{5} + \frac{2(0)}{3} + 2\left(\frac{\sqrt{3}}{2}\right) \right) - \\
 &\quad \left(\frac{2\left(-\frac{\sqrt{2}}{2}\right)}{5} + \frac{2\left(\frac{\sqrt{2}}{2}\right)}{3} + 2\left(\frac{\sqrt{2}}{2}\right) \right) \\
 &= \left(-\frac{\sqrt{3}}{5} + \sqrt{3} \right) - \left(-\frac{\sqrt{2}}{5} + \frac{\sqrt{2}}{3} + \sqrt{2} \right) \\
 &= \frac{4\sqrt{3}}{5} - \frac{17\sqrt{2}}{15} = \frac{1}{15}(12\sqrt{3} - 17\sqrt{2}) \text{ as required}
 \end{aligned}$$

Since the reduction formula is for I_{n+2} , apply the formula with $n = 4$; and then apply the reduction formula again.

Repeatedly apply the reduction formula until I_0 appears, which is an integral that can be easily evaluated.

Now the result for the indefinite integral I_6 can be used to evaluate the given indefinite integral.

Exercise 6A

1 Given that $I_n = \int x^n e^{\frac{x}{2}} dx$,

a show that $I_n = 2x^n e^{\frac{x}{2}} - 2nI_{n-1}$, $n \geq 1$

b Hence find $\int x^3 e^{\frac{x}{2}} dx$.

2 Given that $I_n = \int_1^e x (\ln x)^n dx$, $n \in \mathbb{N}$,

a show that $I_n = \frac{e^2}{2} - \frac{n}{2} I_{n-1}$, $n \in \mathbb{N}$

b Hence, show that $\int_1^e x (\ln x)^4 dx = \frac{e^2 - 3}{4}$.

3 In Example 3, you saw that, if $I_n = \int_0^1 x^n \sqrt{1-x} dx$, then $I_n = \frac{2n}{2n+3} I_{n-1}$, $n \geq 1$.

Use this reduction formula to evaluate $\int_0^1 (x+1)(x+2)\sqrt{1-x} dx$.

- A** 4 Given that $I_n = \int x^n e^{-x} dx$, where n is a positive integer,
- E** a show that $I_n = -x^n e^{-x} + n I_{n-1}$, $n \geq 1$ (7 marks)
- b Find $\int x^3 e^{-x} dx$ (4 marks)
- c Evaluate $\int_0^1 x^4 e^{-x} dx$, giving your answer in terms of e . (4 marks)
- E** 5 $I_n = \int \tanh^n x dx$
- a By writing $\tanh^n x = \tanh^{n-2} x \tanh^2 x$ show that, for $n \geq 2$,
- $$I_n = I_{n-2} - \frac{1}{n-1} \tanh^{n-1} x. \quad (6 \text{ marks})$$
- b Find $\int \tanh^5 x dx$ (3 marks)
- c Show that $\int_0^{\ln 2} \tanh^4 x dx = \ln 2 - \frac{84}{125}$ (4 marks)
- E** 6 Given that $\int \tan^n x dx = \frac{1}{n-1} \tan^{n-1} x - \int \tan^{n-2} x dx$,
- a find $\int \tan^4 x dx$ (4 marks)
- b Evaluate $\int_0^{\frac{\pi}{4}} \tan^5 x dx$ (3 marks)
- c Show that $\int_0^{\frac{\pi}{3}} \tan^6 x dx = \frac{9\sqrt{3}}{5} - \frac{\pi}{3}$ (4 marks)
- E/P** 7 Given that $I_n = \int_1^a (\ln x)^n dx$ where $a > 1$ is a constant,
- a show that, for $n \geq 1$, $I_n = a(\ln a)^n - n I_{n-1}$ (8 marks)
- b find the exact value of $\int_1^2 (\ln x)^3 dx$ (4 marks)
- c show that $\int_1^e (\ln x)^6 dx = 5(53e - 144)$ (4 marks)
- 8 Using the results given in Example 5, evaluate:
- a $\int_0^{\frac{\pi}{2}} \sin^7 x dx$ b $\int_0^{\frac{\pi}{2}} \sin^2 x \cos^4 x dx$
- c $\int_0^1 x^5 \sqrt{1-x^2} dx$, using the substitution $x = \sin \theta$
- d $\int_0^{\frac{\pi}{6}} \sin^8 3t dt$, using a suitable substitution.
- E** 9 Given that $I_n = \int \frac{\sin^{2n} x}{\cos x} dx$,
- a write down a similar expression for I_{n+1} and hence show that $I_n - I_{n+1} = \frac{\sin^{2n+1} x}{2n+1}$. (6 marks)
- b Find $\int \frac{\sin^4 x}{\cos x} dx$ and hence show that $\int_0^{\frac{\pi}{4}} \frac{\sin^4 x}{\cos x} dx = \ln(1 + \sqrt{2}) - \frac{7\sqrt{2}}{12}$. (6 marks)
- E** 10 a Given that $I_n = \int_0^1 x(1-x^3)^n dx$, show that $I_n = \frac{3n}{3n+2} I_{n-1}$. (6 marks)
- b Use your reduction formula to evaluate I_4 . (4 marks)
- E/P** 11 Given that $I_n = \int_0^a (a^2 - x^2)^n dx$, where a is a positive constant,
- a show that, for $n > 0$, $I_n = \frac{2na^2}{2n+1} I_{n-1}$. (9 marks)
- b Use the reduction formula to evaluate:
- i $\int_0^1 (1-x^2)^4 dx$ ii $\int_0^3 (9-x^2)^3 dx$ iii $\int_0^2 \sqrt{4-x^2} dx$. (9 marks)
- c Check your answer to part biii by using another method. (7 marks)

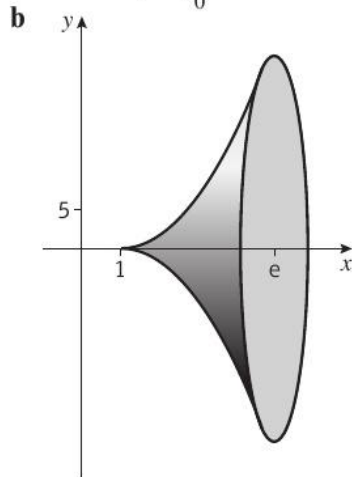
Hint This result was derived in example 4.

Hint After integrating by parts, write x^4 as $x(1 - (1-x^3))$.

- A** 12 Given that $I_n = \int_0^4 x^n \sqrt{4-x} \, dx$,
- E** a establish the reduction formula $I_n = \frac{8n}{2n+3} I_{n-1}$, $n \geq 1$. (8 marks)
- b Evaluate $\int_0^4 x^3 \sqrt{4-x} \, dx$, giving your answer correct to 3 significant figures. (3 marks)
- E/P** 13 Given that $I_n = \int \cos^n x \, dx$,
- a establish, for $n \geq 2$, the reduction formula $n I_n = \cos^{n-1} x \sin x + (n-1) I_{n-2}$. (8 marks)
- Defining $J_n = \int_0^{2\pi} \cos^n x \, dx$,
- b write down a reduction formula relating J_n and J_{n-2} , for $n \geq 2$. (4 marks)
- c Hence evaluate i J_4 ii J_8 . (4 marks)
- d Show that if n is odd, J_n is always equal to zero. (4 marks)
- E/P** 14 Given that $I_n = \int_0^1 x^n \sqrt{1-x^2} \, dx$, $n \geq 0$,
- a show that $(n+2)I_n = (n-1)I_{n-2}$, $n \geq 2$. (6 marks)
- b Hence evaluate $\int_0^1 x^7 \sqrt{1-x^2} \, dx$. (4 marks)
- Hint** Write $x^n \sqrt{1-x^2}$ as $x^{n-1}(x\sqrt{1-x^2})$ before integrating by parts.
- E/P** 15 Given that $I_n = \int x^n \cosh x \, dx$,
- a show that for $n \geq 2$, $I_n = x^n \sinh x - n x^{n-1} \cosh x + n(n-1) I_{n-2}$. (8 marks)
- b find $\int x^4 \cosh x \, dx$ (4 marks)
- c evaluate $\int_0^1 x^3 \cosh x \, dx$, giving your answer in terms of e . (4 marks)
- E/P** 16 Given that $I_n = \int \frac{\sin nx}{\sin x} \, dx$, $n > 0$,
- a write down a similar expression for I_{n-2} , and hence show that
- $$I_n - I_{n-2} = \frac{2 \sin((n-1)x)}{n-1}. \quad (7 \text{ marks})$$
- b Find:
- i $\int \frac{\sin 4x}{\sin x} \, dx$ ii the exact value of $\int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \frac{\sin 5x}{\sin x} \, dx$ (6 marks)
- E/P** 17 Given that $I_n = \int \sinh^n x \, dx$, $n \in \mathbb{N}$,
- a derive the reduction formula $n I_n = \sinh^{n-1} x \cosh x - (n-1) I_{n-2}$, $n \geq 2$. (9 marks)
- b Hence:
- i evaluate $\int_0^{\ln 3} \sinh^5 x \, dx$
- ii show that $\int_0^{\operatorname{arsinh} 1} \sinh^4 x \, dx = \frac{1}{8} \{3 \ln(1+\sqrt{2}) - \sqrt{2}\}$. (7 marks)
- E/P** 18 Consider the definite integral $I_n = \int_0^{\ln \sqrt{3}} \tanh^n x \, dx$, $n \geq 1$.
- a By rewriting $\tanh^n x$ as $\tanh^{n-2} x \tanh^2 x$ and using the identity $\tanh^2 x = 1 - \operatorname{sech}^2 x$, show that $I_n = I_{n-2} - \frac{1}{n-1} \left(\frac{1}{2}\right)^{n-1}$, $n \geq 2$. (6 marks)
- b Hence, show that $\sum_{r=1}^{\infty} \frac{1}{2^r} \left(\frac{1}{2}\right)^{2r} = \ln \frac{2}{\sqrt{3}}$. (9 marks)
- (You may assume that $\lim_{n \rightarrow \infty} \int_0^{\ln \sqrt{3}} \tanh^n x \, dx = 0$.)

- A** 19 a Given $I_n = \int_0^e x^2 (\ln x)^n dx$, $n \geq 0$, prove that, for $n \geq 1$, $I_n = \frac{e^3}{3} - \frac{n}{3} I_{n-1}$. (6 marks)

E/P



A company has designed a spinning top (shown above) using 3D graphing software. The design consists of a solid created by rotating the portion of the curve $y = 3x(\ln x)^2$ from $x = 1$ to $x = e$. Find the exact volume of the top. (7 marks)

Challenge

- a Derive a reduction formula for $I_n = \int x^a (\ln x)^n dx$ where a is a rational number such that $a \neq -1$ and n is an integer such that $n \geq 1$.
- b Hence, find $\int \sqrt{x} (\ln x)^3 dx$. by $-ab = 0$.

6.2 Arc length

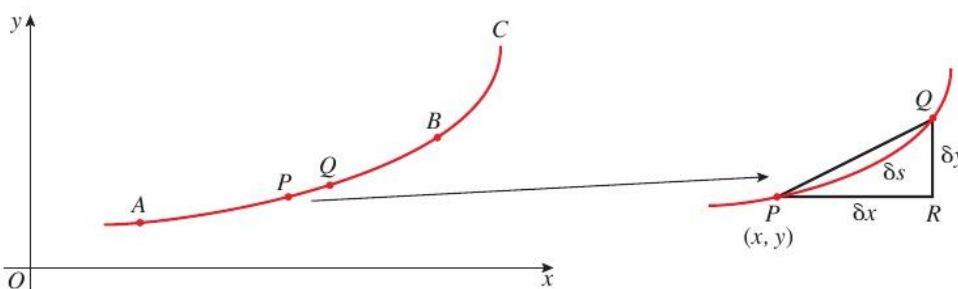
You can use integration to find the length of a curve between two points on the curve. This length is usually referred to as the **arc length**.

Consider the graph of a curve C whose equation is $y = f(x)$. Suppose $P(x, y)$ is any point on the curve C and that $Q(x + \delta x, y + \delta y)$ is another point on C that is close to P .

Let s represent the length of the arc on C between any two points $A(x_A, y_A)$ and $B(x_B, y_B)$, and let δs be the small portion of this arc between points P and Q .

Watch out You have previously used 'arc length' to refer to the length of an arc of a circle. In this chapter, 'arc length' is used to refer to the length of **any** continuous section of a curve measured from one point on the curve to another.

Notation δx and δy ('delta x ' and 'delta y ') represent, respectively, a small change in x and a small change in y . Similarly, δs represents a small change in the length, s , of an arc.



A Since P and Q are close to each other, the small arc length between them, δs , can be approximated by the line segment PQ .

$$\text{Thus, } (\delta s)^2 \approx (\delta x)^2 + (\delta y)^2$$

$$\text{Dividing through by } (\delta x)^2 \text{ gives } \left(\frac{\delta s}{\delta x}\right)^2 \approx 1 + \left(\frac{\delta y}{\delta x}\right)^2$$

$$\text{As } Q \text{ moves closer to } P, \delta x \rightarrow 0, \frac{\delta s}{\delta x} \rightarrow \frac{ds}{dx} \text{ and } \frac{\delta y}{\delta x} \rightarrow \frac{dy}{dx}$$

$$\text{Thus, as } \delta x \rightarrow 0, \left(\frac{\delta s}{\delta x}\right)^2 \approx 1 + \left(\frac{\delta y}{\delta x}\right)^2 \Rightarrow \left(\frac{ds}{dx}\right)^2 = 1 + \left(\frac{dy}{dx}\right)^2$$

$$\text{and } \frac{ds}{dx} = \sqrt{1 + \left(\frac{dy}{dx}\right)^2}$$

Integrating this with respect to x gives an expression for the arc length, s .

Similarly, dividing $(\delta s)^2 \approx (\delta x)^2 + (\delta y)^2$ through by $(\delta y)^2$ and taking the limit as $\delta y \rightarrow 0$ gives

$$\frac{ds}{dy} = \sqrt{1 + \left(\frac{dx}{dy}\right)^2}, \text{ and then integrating with respect to } y \text{ gives an alternative expression for } s.$$

You can use either of these approaches to find an arc length of a curve given in **Cartesian form**.

- If s is the length of the arc between $A(x_A, y_A)$ and $B(x_B, y_B)$ on the graph with Cartesian equation $y = f(x)$, then:

$$\bullet s = \int_{x_A}^{x_B} \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$$

If the equation of the curve is given parametrically, that is, in the form

$x = f(t), y = g(t)$, then dividing

$$(\delta s)^2 \approx (\delta x)^2 + (\delta y)^2$$

through by $(\delta t)^2$ and proceeding to the limit, gives $\frac{ds}{dt} = \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}$. If the parameters at points A and B on the curve are t_A and t_B respectively, then integrating with respect to t gives an expression for the arc length, s .

- If s is the length of the arc between the points $A(f(t_A), g(t_A))$ and $B(f(t_B), g(t_B))$ on the curve with parametric equations $x = f(t), y = g(t)$, then

$$s = \int_{t_A}^{t_B} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$$

You also need to know how to find the length of an arc along a curve that is given in polar form.

Note This use of Pythagoras' theorem is key to deriving all of the arc length formulae.

Note This formula for $\frac{ds}{dx}$ will be used in the next section to develop the formula for the area of a surface of revolution. The positive square is taken so that s increases as x increases.

Note In order to use this formula, it is necessary to be able to find $\frac{dy}{dx}$ or $\frac{dx}{dy}$ at all points on the arc.

$$\bullet s = \int_{y_A}^{y_B} \sqrt{1 + \left(\frac{dx}{dy}\right)^2} dy$$

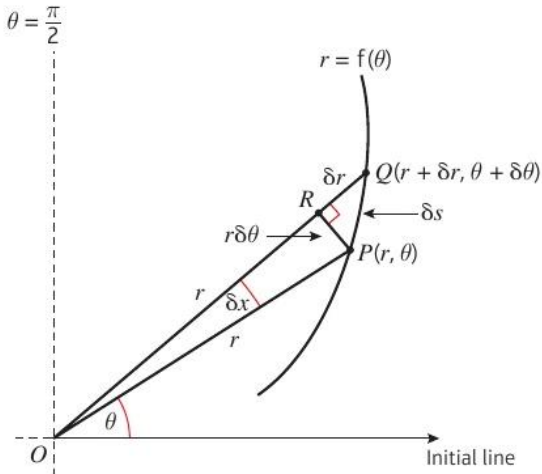
Note You can use either version of the formula, depending on which is most convenient.

Links A curve in polar form is defined by an equation of the form $r = f(\theta)$, where r is the distance from the origin and θ is the angle measure anticlockwise from the positive x -axis.

← Core Book Pure 2, Chapter 5

- A** The diagram below shows the curve with polar equation $r = f(\theta)$. P is the point (r, θ) , and Q is the nearby point $(r + \delta r, \theta + \delta \theta)$. The length of the arc between P and Q is δs . As $\delta \theta \rightarrow 0$, PQ can be approximated as the arc of a circle with radius r , giving PR to be $r\delta\theta$.

The formula for the arc length l of a circle with radius r that is subtended by central angle θ is $l = r\theta$.



Thus, PQR approximates a right triangle, so $(\delta s)^2 \approx (r\delta\theta)^2 + (\delta r)^2$.

Dividing through by $(\delta\theta)^2$ gives $\left(\frac{\delta s}{\delta\theta}\right)^2 \approx r^2 + \left(\frac{\delta r}{\delta\theta}\right)^2$

Then taking the limit as $\delta\theta \rightarrow 0$ gives $\frac{ds}{d\theta} = \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2}$

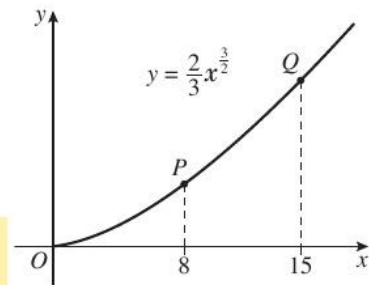
Integrating this with respect to θ gives an expression for the arc length, s , subtended by two angles (or half-lines).

- If s is the length of the arc between the half-lines $\theta = \alpha$ and $\theta = \beta$ on the curve with polar equation $r = f(\theta)$, then

$$s = \int_{\alpha}^{\beta} \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} d\theta$$

Example 8

Find the length of the arc PQ on the curve with equation $y = \frac{2}{3}x^{\frac{3}{2}}$, where the x -coordinates of P and Q are 8 and 15 respectively.



$$y = \frac{2}{3}x^{\frac{3}{2}} \Rightarrow \frac{dy}{dx} = \frac{2}{3} \times \frac{3}{2}x^{\frac{1}{2}} = \sqrt{x}$$

$$s = \int_{x_A}^{x_B} \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$$

Start by finding $\frac{dy}{dx}$

Choose the appropriate arc length formula. For this example, the curve's equation is given in Cartesian form. Since it's easier to find $\frac{dy}{dx}$ rather than $\frac{dx}{dy}$, use the formula that involves integrating with respect to x .

A

$$\begin{aligned}
 \text{Length of arc } PQ &= \int_8^{15} \sqrt{1 + (\sqrt{x})^2} dx \\
 &= \int_8^{15} (1+x)^{\frac{1}{2}} dx \\
 &= \left[\frac{2}{3} (1+x)^{\frac{3}{2}} \right]_8^{15} \\
 &= \frac{2}{3} (16^{\frac{3}{2}} - 9^{\frac{3}{2}}) = \frac{2}{3} (64 - 27) \\
 &= \frac{74}{3}
 \end{aligned}$$

Problem-solving

In this example, the straight-line distance from P to Q should be close to the length along the curve from P to Q . P and Q have y -coordinates 15.085 and 38.730 respectively, so the distance formula gives

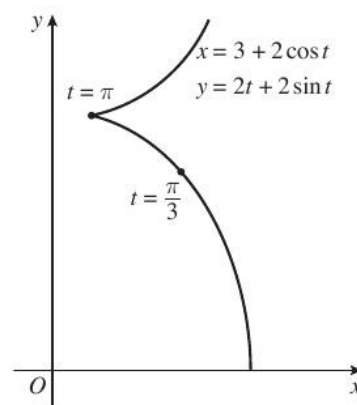
$$PQ = \sqrt{(15-8)^2 + (38.73-15.085)^2} = 24.66... \approx \frac{74}{3}$$

So, the answer looks correct. This check is only appropriate if the curve is approximately straight between the two given points.

Example 9

A curve is defined by the parametric equations $x = 3 + 2 \cos t$, $y = 2t + 2 \sin t$, $t \in \mathbb{R}$.

- Show that $\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 = 16 \cos^2\left(\frac{t}{2}\right)$
- Find the exact length of this curve between the points where $t = \frac{\pi}{3}$ and $t = \pi$.



$$\begin{aligned}
 \text{a } x &= 3 + 2 \cos t \Rightarrow \frac{dx}{dt} = -2 \sin t \\
 y &= 2t + 2 \sin t \Rightarrow \frac{dy}{dt} = 2 + 2 \cos t \\
 \text{So } \left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 &= (-2 \sin t)^2 + (2 + 2 \cos t)^2 \\
 &= 4 \sin^2 t + 4 \cos^2 t + 8 \cos t + 4 \\
 &= 4(\sin^2 t + \cos^2 t) + 8 \cos t + 4 \\
 &= 8 \cos t + 8 \\
 &= 8 \left(\cos^2 \frac{t}{2} - \sin^2 \frac{t}{2} \right) + 8 \\
 &= 8 \cos^2 \frac{t}{2} + 8 - 8 \sin^2 \frac{t}{2} \\
 &= 8 \cos^2 \frac{t}{2} + 8 \left(1 - \sin^2 \frac{t}{2} \right) \\
 &= 16 \cos^2 \frac{t}{2} \text{ as required}
 \end{aligned}$$

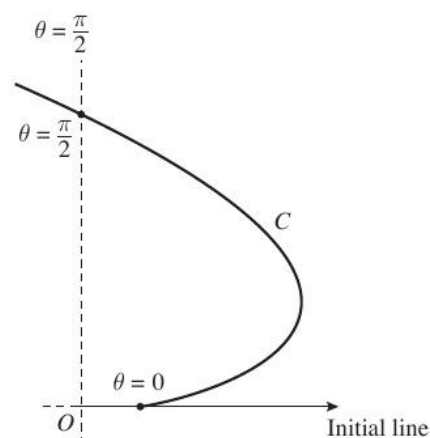
Use the identity
 $\cos 2A \equiv \cos^2 A - \sin^2 A$.

$$\begin{aligned}
 \text{b Arc length} &= \int_{\pi/3}^{\pi} \sqrt{16 \cos^2 \frac{t}{2}} dt \\
 &= 4 \int_{\pi/3}^{\pi} \cos \frac{t}{2} dt \\
 &= 4 \left[2 \sin \frac{t}{2} \right]_{\pi/3}^{\pi} \\
 &= 8 \left(\sin \frac{\pi}{2} - \sin \frac{\pi}{6} \right) \\
 &= 8 \left(1 - \frac{1}{2} \right) \\
 &= 4
 \end{aligned}$$

Use the formula
 $s = \int_{t_A}^{t_B} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

Example 10

- A The curve C shown in the diagram has polar equation $r = 5e^{2\theta}$. Find the length of the arc of C between the points on the curve with $\theta = 0$ and $\theta = \frac{\pi}{2}$.



$$r = 5e^{2\theta} \Rightarrow \frac{dr}{d\theta} = 10e^{2\theta}$$

$$\begin{aligned} \text{Arc length} &= \int_0^{\frac{\pi}{2}} \sqrt{(5e^{2\theta})^2 + (10e^{2\theta})^2} d\theta \\ &= \int_0^{\frac{\pi}{2}} \sqrt{125e^{4\theta}} d\theta \\ &= 5\sqrt{5} \int_0^{\frac{\pi}{2}} e^{2\theta} d\theta \\ &= 5\sqrt{5} \left[\frac{1}{2} e^{2\theta} \right]_0^{\frac{\pi}{2}} \\ &= \frac{5\sqrt{5}}{2} (e^{\pi} - 1) \end{aligned}$$

Use the formula $s = \int_{\alpha}^{\beta} \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} d\theta$

Example 11

Find the exact length of the arc on the parabola with equation $y = \frac{1}{2}x^2$, from the origin to the point $P(4, 8)$.

$$y = \frac{1}{2}x^2 \Rightarrow \frac{dy}{dx} = x$$

Using $s = \int_{x_A}^{x_B} \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$,

Length of arc $OP = \int_0^4 \sqrt{1 + x^2} dx$

Using the substitution $x = \sinh u$, so that $dx = \cosh u du$,

$$\text{Arc length} = \int_0^{\text{arsinh } 4} \sqrt{1 + \sinh^2 u} \cosh u du$$

$$= \int_0^{\text{arsinh } 4} \cosh^2 u du$$

$$= \int_0^{\text{arsinh } 4} \frac{(1 + \cosh 2u)}{2} du$$

$$= \frac{1}{2} \left[u + \frac{1}{2} \sinh 2u \right]_0^{\text{arsinh } 4}$$

$$= \frac{1}{2} [u + \sinh u \cosh u]_0^{\text{arsinh } 4}$$

$$= \frac{1}{2} \text{arsinh } 4 + \frac{1}{2} 4\sqrt{1 + 16} - \frac{1}{2}(0 + 0)$$

$$= \frac{1}{2} \text{arsinh } 4 + 2\sqrt{17}$$

$$= \frac{1}{2} (\ln 4 + \sqrt{17}) + 2\sqrt{17}$$

Start by finding $\frac{dy}{dx}$

Choose the appropriate formula.

$x_A = 0$ and $x_B = 4$.

Problem-solving

You need to use a hyperbolic substitution to find $\int \sqrt{1 + x^2} dx$. ← Core Pure Book 2, Section 6.5

Choose the appropriate method of integration.

Use $\cosh u = \sqrt{1 + \sinh^2 u}$ and $\sinh u = 4$.

Use $\text{arsinh } x = \ln(x + \sqrt{1 + x^2})$

Exercise 6B

A

- Find the length of the arc of the curve with equation $y = \frac{1}{3}x^{\frac{3}{2}}$, from the origin to the point with x -coordinate 12.
- The curve C has equation $x = \ln \cos y$. Find the length of the arc of C between the points with y -coordinates 0 and $\frac{\pi}{3}$.
- Find the length of the arc on the catenary with equation $y = 2 \cosh\left(\frac{x}{2}\right)$, between the points with x -coordinates 0 and $\ln 4$.
- Find the length of the arc of the curve with equation $y^2 = \frac{4}{9}x^3$, between the points with y -coordinates 0 and $2\sqrt{3}$.
- The curve C has equation $y = \frac{1}{2} \sinh^2 2x$. Find the length of the arc on C from the origin to the point whose x -coordinate is 1, giving your answer to 3 significant figures.

E

- Points A and B , with x -coordinates 1 and 2 respectively, lie on the curve

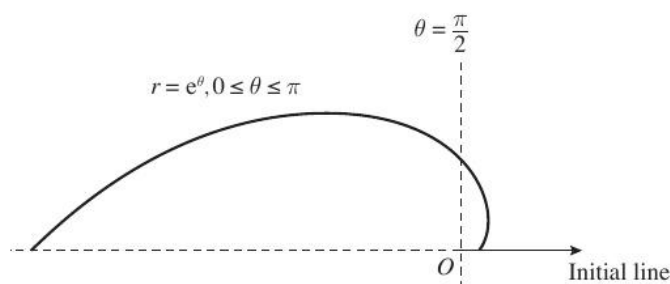
$$y = \frac{1}{4}(2x^2 - \ln x), \quad x > 0$$

Show that the length of the arc from A to B is $\frac{1}{4}(6 + \ln 2)$.

(5 marks)

E

- The diagram shows the curve with polar equation $r = e^\theta$ between the points where $\theta = 0$ and $\theta = \pi$.

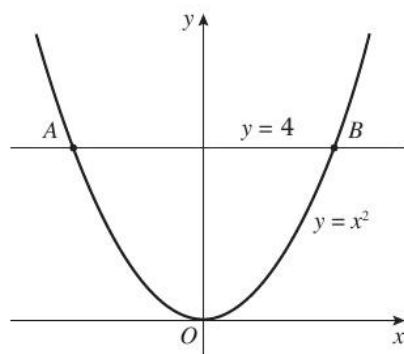


Find the exact length of the curve.

(6 marks)

E

- The line $y = 4$ intersects the parabola with equation $y = x^2$ at the points A and B .

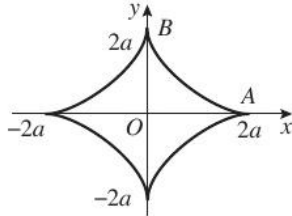


Find the length of the arc of the parabola from A to B .

(6 marks)

- A** 9 The circle C has parametric equations $x = r \cos \theta$, $y = r \sin \theta$. Use the formula for arc length to show that the length of the circumference is $2\pi r$. **(6 marks)**

- E** 10 The diagram shows the astroid with parametric equations
 $x = 2a \cos^3 t$, $y = 2a \sin^3 t$, $0 \leq t \leq 2\pi$



Find the length of the arc of the curve AB , and hence find the total length of the curve. **(7 marks)**

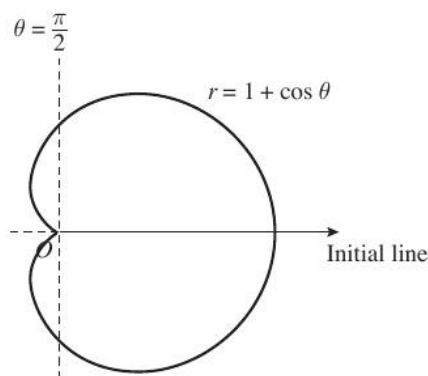
- E** 11 Calculate the length of the arc on the curve with parametric equations $x = \tanh u$, $y = \operatorname{sech} u$, between the points with parameters $u = 0$ and $u = 1$. **(5 marks)**

- E** 12 The cycloid has parametric equations $x = a(\theta + \sin \theta)$, $y = a(1 - \cos \theta)$. Find the length of the arc from $\theta = 0$ to $\theta = \pi$. **(5 marks)**

- E** 13 Show that the length of the arc, between the points with parameters $t = 0$ and $t = \frac{\pi}{3}$ on the curve defined by the equations $x = t + \sin t$, $y = 1 - \cos t$, is 2. **(5 marks)**

- E** 14 Find the length of the arc on the curve given by the equations $x = e^t \cos t$, $y = e^t \sin t$, between the points with parameters $t = 0$ and $t = \frac{\pi}{4}$. **(5 marks)**

- E** 15 The diagram shows the cardioid with polar equation $r = 1 + \cos \theta$.



Find the total length of the cardioid. **(5 marks)**

- E** 16 The curve C has equation $y = \ln(\cos x)$, $0 \leq x < \frac{\pi}{2}$

a Show that $\sqrt{1 + \left(\frac{dy}{dx}\right)^2} = \sec x$ **(4 marks)**

b The length of the arc on C from the origin to the point with x -coordinate $\frac{\pi}{6}$ is $\ln k$. Find the exact value of k . **(5 marks)**

- A** 17 Consider the curve which is the portion of the graph of $y = \ln(1 - x^2)$ from $x = -\frac{1}{2}$ to $x = \frac{1}{2}$. The length of this curve is s .

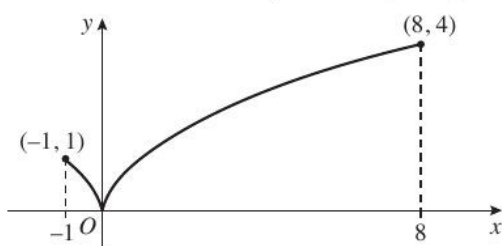
a Show that $s = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{1+x^2}{1-x^2} dx$

(4 marks)

b Find the exact length of s .

(6 marks)

- E/P** 18 A graphic designer has created a symbol (shown in the diagram) that is modelled by the two curves, $x = -y^{\frac{3}{2}}$ from $(-1, 1)$ to $(0, 0)$, and $x = y^{\frac{3}{2}}$ from $(0, 0)$ to $(8, 4)$.



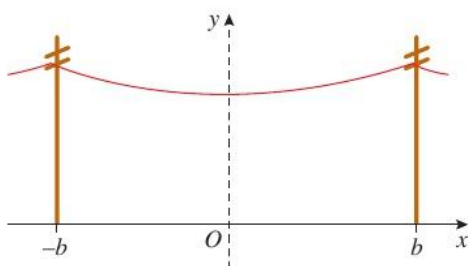
Hint The equations are given in the form $x = f(y)$ so it will be easier to use the formula for arc length that involves integrating with respect to y . Integrating with respect to x is not possible for the whole length of the given arc since $\frac{dy}{dx}$ is not defined at $(0, 0)$.

The scale for the graph above is 1 cm per unit.

Find the length of the curve to the nearest tenth of a centimetre.

(8 marks)

- E/P** 19 The diagram below shows an electricity wire that hangs between two poles located at $x = -b$ and $x = b$.



The shape of the curve is called a catenary, and its equation is $y = c + a \cosh\left(\frac{x}{a}\right)$.

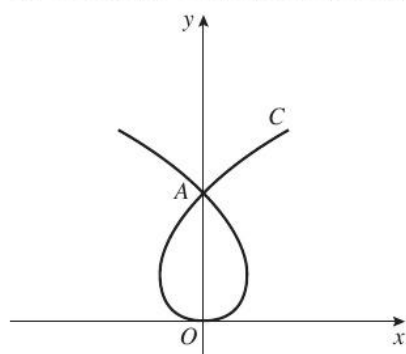
a Show that the length of the wire is $2a \sinh\left(\frac{b}{a}\right)$.

(5 marks)

- b** Two electricity poles are 50 metres apart and the length of the wire between the poles is 51 metres. If the lowest point of the wire is 20 metres above the ground, then how high up on each pole should the wire be attached?

(7 marks)

- A 20** A jewellery designer is making a brooch from silver wire. The wire is bent into a shape modelled by the curve C shown in the diagram, with parametric equations $x = 3t^3 - t$, $y = 3t^2$, $-k \leq t \leq k$

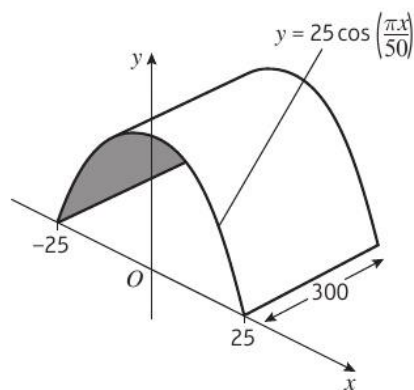


All units are in cm.

The design requires the wire to cross itself at the point marked A.

- a** Find:
- the range of possible values of k
 - the minimum length of wire needed to make the brooch. (8 marks)
- b** Given that $k = \frac{3}{4}$, find the length of wire needed to make the brooch in centimetres. Give your answer in centimetres, correct to 3 significant figures. (2 marks)

- E/P 21** An engineering company is submitting a bid to construct the tunnel shown in the diagram (not to scale).



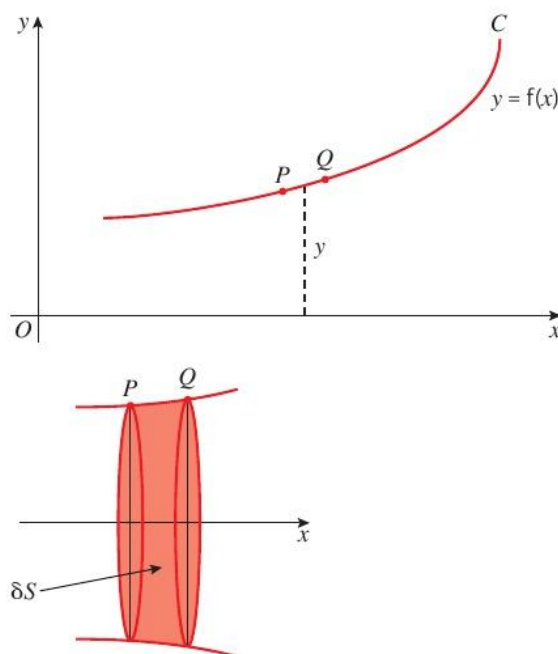
The tunnel is 300 metres long and 50 metres wide at the base. The tunnel's cross section has the shape of one arch of the curve $y = 25 \cos\left(\frac{\pi x}{50}\right)$. The inside surface of the tunnel (not including the road surface) will be waterproofed with a sealer that costs £17 per square metre to apply. Find the cost of applying the sealer. (7 marks)

Challenge

Find the exact length of the curve $y = \int_1^x \sqrt{t^3 - 1} dt$, $1 \leq x \leq 4$.

6.3 Area of a surface of revolution

- A** The curve C with equation $y = f(x)$ (shown below) is rotated through 2π radians about the x -axis generating a surface (called a **surface of revolution**). Consider a small arc PQ of length δs that is a distance y from the x -axis. When arc PQ is rotated about the x -axis it generates a very narrow cylinder with radius y and surface area δS – a small portion of the total area of the surface of revolution created by rotating C .



Notation The lower-case letter s represents the length of an arc; whereas capital S represents the area of a surface. Correspondingly, δs is a small change, or small length, of an arc; and δS is a small change, or small area, of a surface.

Using the formula for the surface area of a cylinder gives $\delta S = 2\pi y \delta s$.

Thus, $\frac{\delta S}{\delta x} = 2\pi y \frac{\delta s}{\delta x}$. Taking the limit as $\delta x \rightarrow 0$, $\frac{\delta S}{\delta x} \rightarrow \frac{dS}{dx}$ and $\frac{\delta s}{\delta x} \rightarrow \frac{ds}{dx}$.

Hence, using the formula for $\frac{ds}{dx}$ from the previous section,

$$\frac{dS}{dx} = 2\pi y \frac{ds}{dx} = 2\pi y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} \quad \text{---} \quad \frac{ds}{dx} = \sqrt{1 + \left(\frac{dy}{dx}\right)^2}$$

Integrating this with respect to x gives a formula for the surface area S .

- If the curve with Cartesian equation $y = f(x)$ between the points (x_A, y_A) and (x_B, y_B) is rotated through 2π radians about the x -axis, then the area of the resulting surface of revolution is given by

$$S = 2\pi \int_{x_A}^{x_B} y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$$

- If the curve with Cartesian equation $x = f(y)$ between the points (x_A, y_A) and (x_B, y_B) is rotated through 2π radians about the y -axis, then the area of the resulting surface of revolution is given by

$$S = 2\pi \int_{y_A}^{y_B} x \sqrt{1 + \left(\frac{dx}{dy}\right)^2} dy \quad \text{or} \quad S = 2\pi \int_{x_A}^{x_B} x \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$$

Using results derived in the previous section on arc length, the formulae for the areas of surfaces of revolution formed from curves defined by parametric equations or polar equations can also be found.

Note When rotating a curve given in the form $y = f(x)$ about the **y -axis**, it is often easiest to use the second formula given here.

- A** ■ If the curve with parametric equations $x = f(t)$ and $y = g(t)$ between the points (x_A, y_A) and (x_B, y_B) is rotated through 2π radians about the coordinate axes, then the areas of the resulting surfaces of revolution are given by:

• Rotation about the x -axis: $S = 2\pi \int_{t_A}^{t_B} y \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

• Rotation about the y -axis: $S = 2\pi \int_{t_A}^{t_B} x \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

- If the curve with polar equation $r = f(\theta)$ between the points where $\theta = \alpha$ and $\theta = \beta$ is rotated about the given lines, then the areas of the resulting surfaces of revolution are given by:

• Rotation about the initial line, $\theta = 0$: $S = 2\pi \int_{\alpha}^{\beta} r \sin \theta \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} d\theta$

• Rotation about the line $\theta = \pm \frac{\pi}{2}$: $S = 2\pi \int_{\alpha}^{\beta} r \cos \theta \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} d\theta$

Links The line $\theta = \pm \frac{\pi}{2}$ is the vertical line through the origins.

← Core Book Pure 2, Section 5.1

Example 12

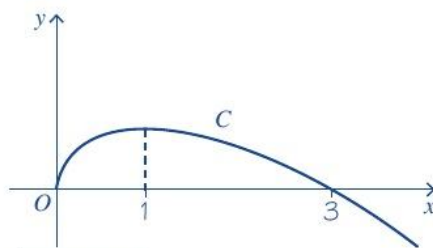
The curve C has equation $y = \frac{1}{3}\sqrt{x}(3-x)$. The arc of the curve between the points with x -coordinates 1 and 3 is completely rotated about the x -axis. Find the area of the surface generated.

Choose the appropriate formula. Given that the equation for the curve is in Cartesian form, and it is being rotated about the x -axis, use the formula

$S = 2\pi \int_{x_A}^{x_B} y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$. This means that you need to start by finding $\frac{dy}{dx}$

$$y = x^{\frac{1}{2}} - \frac{1}{3}x^{\frac{3}{2}} \Rightarrow \frac{dy}{dx} = \frac{1}{2}(x^{-\frac{1}{2}} - x^{\frac{1}{2}})$$

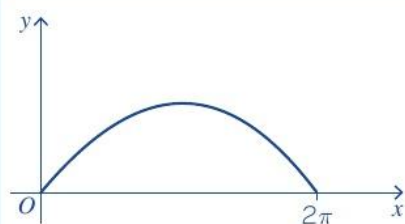
$$\begin{aligned} \text{So } 1 + \left(\frac{dy}{dx}\right)^2 &= 1 + \frac{1}{4}x^{-1} - \frac{1}{2} + \frac{1}{4}x \\ &= \frac{1}{4}x^{-1} + \frac{1}{2} + \frac{1}{4}x \\ &= \frac{1}{4}(x^{-\frac{1}{2}} + x^{\frac{1}{2}})^2 \end{aligned}$$



$$\begin{aligned} \text{Area of the surface generated} &= 2\pi \int_1^3 y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx \\ &= 2\pi \int_1^3 \left(x^{\frac{1}{2}} - \frac{1}{3}x^{\frac{3}{2}}\right) \frac{1}{2}(x^{-\frac{1}{2}} + x^{\frac{1}{2}}) dx \\ &= \pi \int_1^3 \left(1 + \frac{2}{3}x - \frac{1}{3}x^2\right) dx \\ &= \pi \left[x + \frac{1}{3}x^2 - \frac{1}{9}x^3\right]_1^3 \\ &= 3\pi - \frac{11}{9}\pi \\ &= \frac{16}{9}\pi \end{aligned}$$

Example 13

A The curve with parametric equations $x = t - \sin t$, $y = 1 - \cos t$, from $t = 0$ to $t = 2\pi$, is rotated through 360° about the x -axis. Find the area of the surface generated.



$$\frac{dx}{dt} = 1 - \cos t, \quad \frac{dy}{dt} = \sin t$$

$$\begin{aligned} \text{So } \left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 &= (1 - \cos t)^2 + \sin^2 t \\ &= 2 - 2 \cos t \\ &= 2(1 - \cos t) \\ &= 4 \sin^2 \frac{t}{2} \end{aligned}$$

$$\begin{aligned} \text{Area of the surface generated} &= \int_0^{2\pi} 2\pi y \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt \\ &= 2\pi \int_0^{2\pi} (1 - \cos t) 2 \sin \frac{t}{2} dt \\ &= 2\pi \int_0^{2\pi} 4 \sin^3 \frac{t}{2} dt \\ &= 8\pi \int_0^{2\pi} \sin^2 \frac{t}{2} \sin \frac{t}{2} dt \\ &= 8\pi \int_0^{2\pi} \left(1 - \cos^2 \frac{t}{2}\right) \sin \frac{t}{2} dt \\ &= -16\pi \int_1^{-1} (1 - u^2) du \\ &= -16\pi \left[u + \frac{1}{3}u^3\right]_1^{-1} \\ &= -16\pi \left(\left(1 - \frac{1}{3}\right) - \left(-1 + \frac{1}{3}\right)\right) \\ &= \frac{64}{3}\pi \end{aligned}$$

Choose the appropriate formula. Given that the equations for the curve are in parametric form, and it is being rotated about the x -axis, use the

$$\text{formula } S = 2\pi \int_{t_A}^{t_B} y \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt.$$

Start by finding $\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2$.

Problem-solving

You need to take the square root of $\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2$, so let $2A = t$ and use the identity $\cos 2A \equiv 1 - 2\sin^2 A$ to write it in a more convenient form.

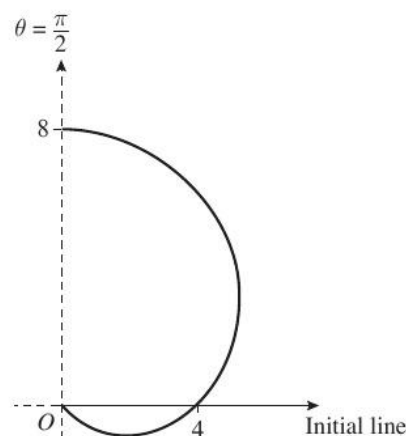
Problem-solving

$$\begin{aligned} \text{Use the identity } \cos 2A &= \cos^2 A - \sin^2 A \text{ to write } \cos t \\ \text{as } \cos^2 \frac{t}{2} - \sin^2 \frac{t}{2} \\ 1 - \cos t &= 1 - \left(\cos^2 \frac{t}{2} - \sin^2 \frac{t}{2}\right) \\ &= 1 - \cos^2 \frac{t}{2} + \sin^2 \frac{t}{2} \\ &= \sin^2 \frac{t}{2} + \sin^2 \frac{t}{2} \\ &= 2 \sin^2 \frac{t}{2} \end{aligned}$$

Use the substitution
 $u = \cos \frac{t}{2}$

Example 14

- A** The graph of the polar equation $r = 4 + 4 \sin \theta$ from $\theta = -\frac{\pi}{2}$ to $\theta = \frac{\pi}{2}$ is shown below. The curve is rotated through 2π radians about the vertical line $\theta = \pm \frac{\pi}{2}$, forming a surface of revolution. Find the exact area of the surface



Choose the appropriate formula. Given that the equation for the curve is in polar form and it is being rotated about the vertical line $\theta = \pm \frac{\pi}{2}$, use the formula

$$S = 2\pi \int_{\alpha}^{\beta} r \cos \theta \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} d\theta.$$

$$r = 4 + 4 \sin \theta \Rightarrow \frac{dr}{d\theta} = 4 \cos \theta$$

$$S = 2\pi \int_{-\pi/2}^{\pi/2} (4 + 4 \sin \theta) \cos \theta \sqrt{(4 + 4 \sin \theta)^2 + (4 \cos \theta)^2} d\theta$$

$$= 8\pi \int_{-\pi/2}^{\pi/2} (1 + \sin \theta) \cos \theta \sqrt{4^2(1 + \sin \theta)^2 + 4^2(\cos \theta)^2} d\theta$$

$$= 32\pi \int_{-\pi/2}^{\pi/2} (1 + \sin \theta) \cos \theta \sqrt{1 + \sin \theta)^2 + (\cos \theta)^2} d\theta$$

$$= 32\pi \int_{-\pi/2}^{\pi/2} (1 + \sin \theta) \cos \theta \sqrt{1 + 2 \sin \theta + \sin^2 \theta + \cos^2 \theta} d\theta$$

$$= 32\pi \int_{-\pi/2}^{\pi/2} (1 + \sin \theta) \cos \theta \sqrt{2 + 2 \sin \theta} d\theta$$

$$= 16\pi \int_{-\pi/2}^{\pi/2} (2 + 2 \sin \theta) \cos \theta \sqrt{2 + 2 \sin \theta} d\theta$$

$$\text{Let } u = 2 + 2 \sin \theta \Rightarrow du = 2 \cos \theta d\theta$$

Substituting gives

$$S = 8\pi \int_0^4 u \sqrt{u} du = 8\pi \int_0^4 u^{3/2} du$$

$$= 8\pi \left[\frac{2}{5} u^{5/2} \right]_0^4$$

$$= \frac{16\pi}{5} (4^{5/2} - 0)$$

$$= \frac{16\pi}{5} (2^5) = \frac{512\pi}{5}$$

Problem-solving

Look at the integrand to try and determine a successful strategy to integrate it. The derivative of $2 + 2 \sin \theta$ is $2 \cos \theta$, so a substitution of $u = 2 + 2 \sin \theta$ will simplify the integral.

Example 15

The arc of the curve with equation $y = \cosh x$, from the point $(0, 1)$ to $(\ln 2, \frac{5}{4})$, is rotated completely about the y -axis. Find the area of the surface generated.



$$y = \cosh x \Rightarrow \frac{dy}{dx} = \sinh x$$

Choose the appropriate formula. Although you are rotating about the **y-axis**, the curve is given in the form $y = f(x)$, so use the alternative formula:

$$S = 2\pi \int_{x_A}^{x_B} x \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$$

A

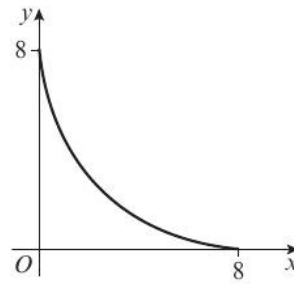
$$\begin{aligned}
 S &= \int_{x_A}^{x_B} 2\pi x \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx \\
 &= 2\pi \int_0^{\ln 2} x \sqrt{1 + \sinh^2 x} dx \\
 &= 2\pi \int_0^{\ln 2} x \cosh x dx \\
 &= 2\pi \left([x \sinh x]_0^{\ln 2} - \int_0^{\ln 2} \sinh x dx \right) \\
 &= 2\pi [x \sinh x - \cosh x]_0^{\ln 2} \\
 &= 2\pi (\ln 2 \sinh(\ln 2) - \cosh(\ln 2) + 1) \\
 &= 2\pi \left[\frac{3}{4} \ln 2 - \frac{5}{4} + 1 \right] \\
 &= \frac{\pi}{2} (3 \ln 2 - 1)
 \end{aligned}$$

Use integration by parts with $u = x$ and $\frac{dv}{dx} = \cosh x$.

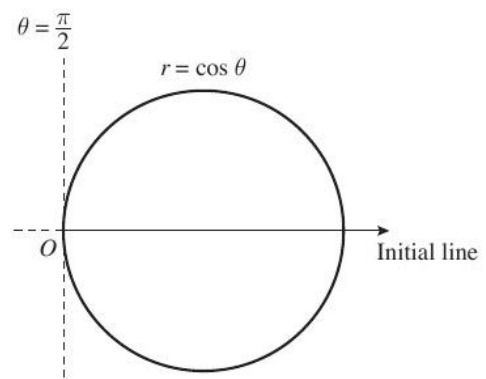
Exercise 6C

- 1 a The section of the line $y = \frac{3}{4}x$ between points with x -coordinates 4 and 8 is rotated completely about the x -axis. Use integration to find the area of the surface generated.
 b The same section of line is rotated completely about the y -axis. Show that the area of the surface generated is 60π .
- 2 The arc of the curve $y = x^3$, between the origin and the point $(1, 1)$, is rotated through 4 right-angles about the x -axis. Find the area of the surface generated.
- 3 The arc of the curve $y = \frac{1}{2}x^2$, between the origin and the point $(2, 2)$, is rotated through 4 right-angles about the y -axis. Find the area of the surface generated.
- E** 4 The curve with parametric equations $x = \sin^2 t$, $y = \cos^2 t$, $0 \leq t \leq \frac{\pi}{2}$, is rotated through 2π radians about the y -axis to form a surface of revolution. Find the exact area of the surface. (5 marks)
- 5 The curve C has equation $y = \cosh x$. The arc s , on C , has end points $(0, 1)$ and $(1, \cosh 1)$.
 a Find the area of the surface generated when s is rotated completely about the x -axis.
 b Show that the area of the surface generated when s is rotated completely about the y -axis is $2\pi \left(\frac{e-1}{e} \right)$.
- E** 6 The curve C has equation $y = \frac{1}{2x} + \frac{x^3}{6}$
 a Show that $\sqrt{1 + \left(\frac{dy}{dx}\right)^2} = \frac{1}{2} \left(x^2 + \frac{1}{x^2} \right)$. (3 marks)
 The arc of the curve between points with x -coordinates 1 and 3 is rotated completely about the x -axis.
 b Find the area of the surface generated. (5 marks)

- A** 7 The diagram shows part of the curve with equation $x^{\frac{2}{3}} + y^{\frac{2}{3}} = 4$. Find the area of the surface generated when this arc is rotated completely about the y -axis. (6 marks)



- E/P** 8 The graph with polar equation $r = \cos \theta$ from $\theta = 0$ to $\theta = \pi$ is a circle. Find the exact area of the surface generated by rotating the circle completely about the line $\theta = \pm \frac{\pi}{2}$ (6 marks)



- E** 9 The finite arc of the parabola with parametric equations $x = at^2$, $y = 2at$, where a is a positive constant, cut off by the line $x = 4a$, is rotated through 180° about the x -axis. Show that the area of the surface generated is $\frac{8a^2\pi}{3}(5\sqrt{5} - 1)$. (6 marks)

- E** 10 The arc, in the first quadrant, of the curve with parametric equations $x = \operatorname{sech} t$, $y = \tanh t$, between the points where $t = 0$ and $t = \ln 2$, is rotated completely about the x -axis. Show that the area of the surface generated is $\frac{2\pi}{5}$. (6 marks)

- E/P** 11 The arc of the curve given by $x = 3t^2$, $y = 2t^3$, from $t = 0$ and $t = 2$, is completely rotated about the y -axis.
a Show that the area of the surface generated can be expressed as $36\pi \int_0^2 t^3 \sqrt{1+t^2} dt$. (3 marks)
b Find the exact value of the surface area. (4 marks)

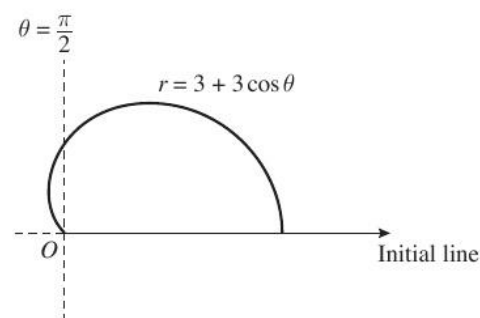
- E** 12 The arc of the curve with parametric equations $x = t^2$, $y = t - \frac{1}{3}t^3$, between the points where $t = 0$ and $t = 1$, is rotated through 2π radians about the x -axis. Calculate the area of the surface generated. (6 marks)

- E** 13 The astroid C has parametric equations $x = a \cos^3 t$, $y = a \sin^3 t$, where a is a positive constant. The arc of C , between $t = \frac{\pi}{6}$ and $t = \frac{\pi}{2}$, is rotated through 2π radians about the x -axis. Find the area of the surface of revolution formed. (6 marks)

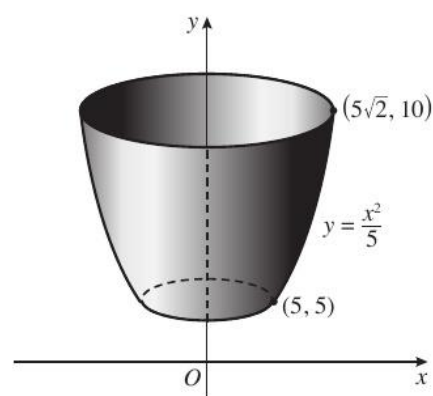
- E** 14 The part of the curve $y = e^x$, between $(0, 1)$ and $(\ln 2, 2)$, is rotated completely about the x -axis. Show that the area of the surface generated is $\pi(\operatorname{arsinh} 2 - \operatorname{arsinh} 1 + 2\sqrt{5} - \sqrt{2})$. (5 marks)

- A** 15 The graph of the polar equation $r = e^\theta$, between where $\theta = 0$ and $\theta = \frac{\pi}{2}$, is rotated completely about the vertical line $\theta = \pm \frac{\pi}{2}$, forming a surface of revolution. Find the exact area of this surface. (6 marks)

- E** 16 A mathematics student is working on a project to measure the surface area of an apple. She decides to model the surface of the apple with the polar equation $r = 3 + 3 \cos \theta$ from $\theta = 0$ to $\theta = \pi$ that is rotated 360° about the horizontal line $\theta = 0$. If each unit on the graph of $r = 3 + 3 \cos \theta$ represents 1 centimetre, then find the approximate surface area of the apple to the nearest one-tenth of a square centimetre. (7 marks)

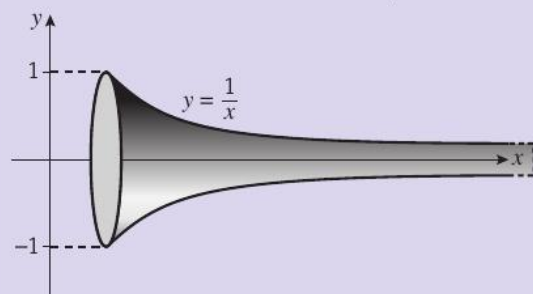


- E/P** 17 A company manufactures small bowls. A model of the bowl is shown in the diagram. This model is created by rotating the portion of the parabola $y = \frac{x^2}{5}$ from $(5, 5)$ to $(5\sqrt{2}, 10)$ about the y -axis. The company applies a special ceramic coating to the outside surface of each bowl (including the circular base). The cost of the ceramic coating is £0.02 per square centimetre. If each unit in the model represents 1 cm, then find the cost for applying the ceramic coating to one bowl. (8 marks)



Challenge

The solid formed by rotating the curve $y = \frac{1}{x}$, $x > 1$ by 2π about the x -axis is sometimes called Torricelli's Trumpet.



- Find the volume generated by the solid.
- Show that the area of the surface of revolution generated is $2\pi \int_1^\infty \frac{1}{x} \sqrt{1 + \frac{1}{x^4}} dx$
- Explain why $2\pi \int_1^a \frac{1}{x} \sqrt{1 + \frac{1}{x^4}} dx > 2\pi \int_1^a \frac{1}{x} dx$ for all $x > 0$.
- Hence explain why Torricelli's trumpet has infinite surface area.

Mixed exercise 6

A 1 a Given that $I_n = \int (\ln x)^n dx$ for $n \geq 1$, show that $I_n = x(\ln x)^n - nI_{n-1}$. (4 marks)

E b Hence, find the exact value of $\int_1^2 (\ln x)^3 dx$. (3 marks)

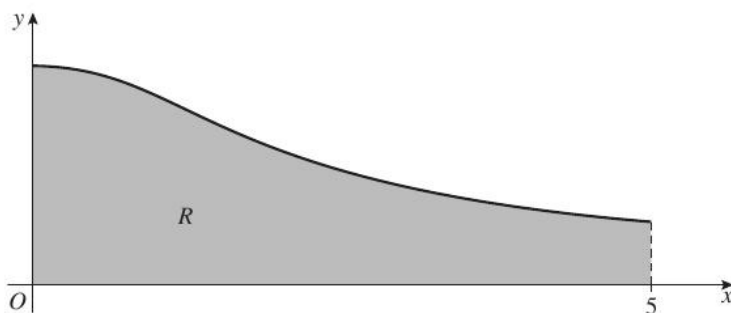
E 2 Find the exact arc length of the curve $y = 3x^{\frac{3}{2}} - 1$ between the points $(0, 0)$ and $(1, 2)$. (5 marks)

3 The arc of the curve $y = \cos x$ from the point $(0, 1)$ and $(\frac{\pi}{2}, 0)$ is rotated 2π radians about the x -axis, forming a surface of revolution. Find the exact area of the surface.

E 4 The diagram shows the cross-section R of an artificial ski slope. The slope is modelled by the curve with equation

$$y = \frac{10}{\sqrt{4x^2 + 9}}, 0 \leq x \leq 5.$$

Given that 1 unit on each axis represents 10 metres, use integration to calculate the distance travelled by the skier from the top to the bottom of the slope.



Show your method clearly and give your answer to 2 significant figures. (8 marks)

5 a Given that $I_n = \int_0^{\pi/2} e^{2x} \sin^n x dx$, $n > 1$, show that $(n^2 + 4)I_n = n(n-1)I_{n-2} + 2e^\pi$.

b Hence, find the exact value of $\int_0^{\pi/2} e^{2x} \sin^3 x dx$.

6 A rope is hung from two points on the same horizontal level. The curve formed by the rope is modelled by the equation

$$y = 4 \cosh\left(\frac{x}{4}\right), -20 \leq x \leq 20$$

Find the length of the rope, giving your answer to 3 significant figures.

7 A curve is defined by the parametric equations $x = t^3$, $y = 3t^2$. An arc of the curve from $t = 0$ to $t = 2$ is rotated completely about the x -axis. Find the exact area of the surface that is generated.

8 Given that $I_n = \int_0^{\pi/2} x^n \cos x dx$,

a find the values of: i I_0 ii I_1 ,

b show, by using integration by parts twice, that $I_n = \left(\frac{\pi}{2}\right)^n - n(n-1)I_{n-2}$, $n \geq 2$.

c Hence show that $\int_0^{\pi/2} x^3 \cos x dx = \frac{1}{8}(\pi^3 - 24\pi + 48)$.

d Evaluate $\int_0^{\pi/2} x^4 \cos x dx$, leaving your answer in terms of π .

9 A curve C is defined by the parametric equations $x = r(\cos \theta + \theta \sin \theta)$ and $y = r(\sin \theta - \theta \cos \theta)$. Find, in terms of r , the length of an arc of the curve from where $\theta = 0$ to $\theta = \pi$.

A 10 Given that $I_n = \int_0^1 x^n (1-x)^{\frac{1}{3}} dx$, $n \geq 0$,

a show that $I_n = \frac{3n}{3n+4} I_{n-1}$, $n \geq 1$

b Hence find the exact value of $\int_0^1 (1+x)(1-x)^{\frac{4}{3}} dx$.

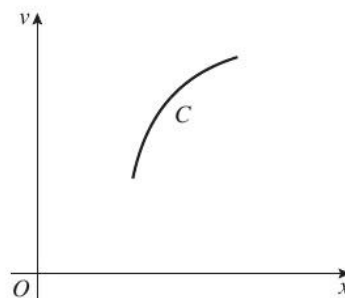
E 11 The curve C has parametric equations

$$x = t - \ln t, y = 4\sqrt{t}, 1 \leq t \leq 4$$

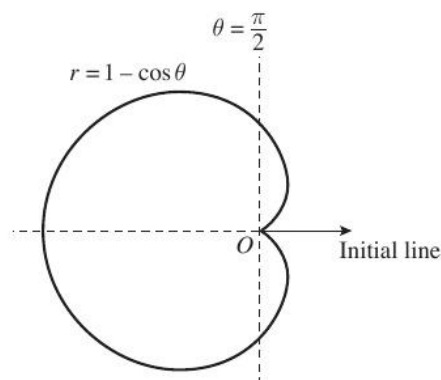
a Show that the length of C is $3 + \ln 4$. **(3 marks)**

The curve is rotated through 2π radians about the x -axis.

b Find the exact area of the curved surface generated. **(4 marks)**



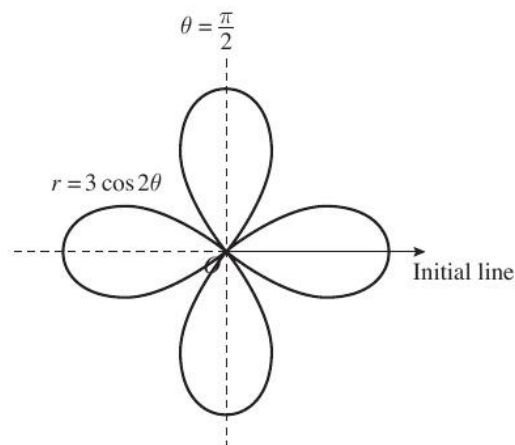
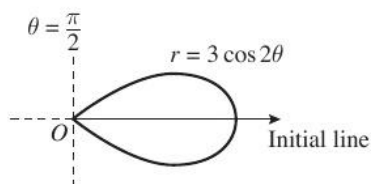
E 12 Josh is creating a frame out of wire in the shape of a cardioid with equation $r = 1 - \cos \theta$, shown in the figure below. If each unit represents 10 cm, then find the length of wire that Josh needs to make his frame.



(5 marks)

E/P 13 An art student has designed a piece of jewellery with four equal lobes symmetrically attached around a centre point. The design is defined by the polar equation $r = 3 \cos 2\theta$ shown below. Each unit represents one centimetre.

In order to apply silver plating to the piece of jewellery, the student needs to determine the total surface area. The diagram below shows one lobe.



a Show that the surface area of this one lobe is given by the following definite integral

$$4\pi \int_{\alpha}^{\beta} \cos \theta d\theta, \text{ where } \alpha \text{ and } \beta \text{ are angles in radians.}$$

(4 marks)

b Find the values for α and β .

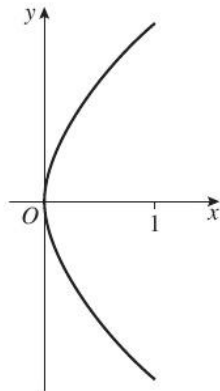
(4 marks)

c Find the total surface of the piece of jewellery to the nearest tenth of a square centimetre.

(3 marks)

- A** 14 The curve C shown in the diagram has equation $y^2 = 4x$, $0 < x < 1$.

E



The part of the curve in the first quadrant is rotated through 2π radians about the x -axis.

- a** Show that the surface area of the solid generated is given by

$$4\pi \int_0^1 \sqrt{1+x} \, dx \quad (3 \text{ marks})$$

- b** Find the exact value of this surface area.

- c** Show also that the length of the curve C , between the points $(1, -2)$ and $(1, 2)$, is

$$\text{given by } 2 \int_0^1 \sqrt{\frac{x+1}{x}} \, dx \quad (3 \text{ marks})$$

- d** Use the substitution $x = \sinh^2 \theta$ to show that the exact value of this length is

$$2(\sqrt{2} + \ln(1 + \sqrt{2})) \quad (4 \text{ marks})$$

- 15 The curve C has parametric equations $x = \cos \theta$, $y = \ln(\sec \theta + \tan \theta) - \sin \theta$.

An arc of the curve from $\theta = 0$ to $\theta = \frac{\pi}{3}$ has length L . Show that $L = \ln 2$.

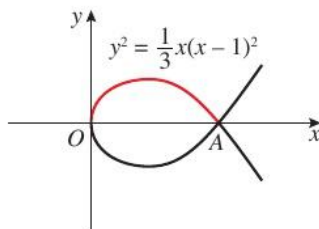
- 16 Given that $I_n = \int \frac{\sin(2n+1)x}{\sin x} \, dx$,

- a** show that $I_n - I_{n-1} = \frac{\sin 2nx}{n}$

- b** Hence find I_5 .

- c** Show that, for all positive integers n , $\int_0^{\frac{\pi}{2}} \frac{\sin(2n+1)x}{\sin x} \, dx$ always has the same value, which should be found.

- 17 The diagram shows part of the graph of the curve with equation $y^2 = \frac{1}{3}x(x-1)^2$.



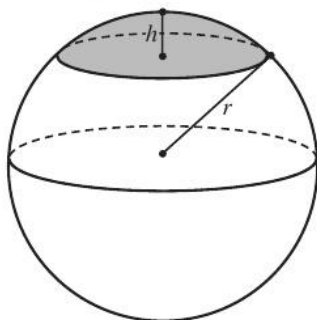
- a** Show that the length of the loop is $\frac{4\sqrt{3}}{3}$

The arc OA (in red) is rotated completely about the x -axis.

- b** Find the area of the surface generated.

- A** 18 The figure below shows a spherical cap of height h for a sphere of radius r .

E/P



Hint Rotate an appropriate portion of the circle about the y -axis.

Show that the surface area of the cap is $S = 2\pi rh$.

(5 marks)

- 19 Given that $I_n = \int \sec^n x \, dx$,

a by writing $\sec^n x = \sec^{n-2} x \sec^2 x$, show that, for $n \geq 2$,

$$(n-1)I_n = \sec^{n-2} x \tan x + (n-2)I_{n-2}.$$

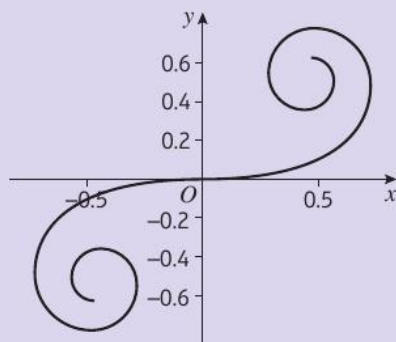
b Find I_5 .

c Hence show that $\int_0^{\frac{\pi}{4}} \sec^5 x \, dx = \frac{1}{8}(7\sqrt{2} + 3\ln(1 + \sqrt{2}))$.

Challenge

The diagram shows a **Cornu spiral**, which has parametric equations

$$x = \int_0^t \cos\left(\frac{\pi u^2}{2}\right) du, \quad y = \int_0^t \sin\left(\frac{\pi u^2}{2}\right) du, \quad 0 \leq t \leq a$$



Find the length of the Cornu spiral.

Summary of key points

A

1 A reduction formula allows you to write a recurrence relation for an integral $I_n = \int f(x, n) dx$ in terms of related integrals I_{n-1} , I_{n-2} , etc.

2 The length, s , of an arc on the curve C , between points $A(x_A, y_A)$ and $B(x_B, y_B)$ is given by

$$s = \int_{x_A}^{x_B} \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx \text{ or } s = \int_{y_A}^{y_B} \sqrt{1 + \left(\frac{dx}{dy}\right)^2} dy$$

If the equation is given parametrically, with the parameters at A and B being t_A and t_B

respectively, then the arc length is given by $s = \int_{t_A}^{t_B} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

- If the equation is given in polar form, $r = f(\theta)$, and the length of the arc is between the half-lines $\theta = \alpha$ and $\theta = \beta$, then

- $s = \int_{\alpha}^{\beta} \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} d\theta$

3 The area, S , of the surface generated when the arc AB on the curve C is rotated completely about the x -axis is $2\pi \int y ds$, and about the y -axis is $2\pi \int x ds$.

These can be used to give the following results:

i about the x -axis: $S = 2\pi \int_{x_A}^{x_B} y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$

ii about the y -axis: $S = 2\pi \int_{y_A}^{y_B} x \sqrt{1 + \left(\frac{dx}{dy}\right)^2} dy$ or $S = 2\pi \int_{x_A}^{x_B} x \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$

If C is given in parametric form, the results are

i about the x -axis: $S = 2\pi \int_{t_A}^{t_B} y \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

ii about the y -axis: $S = 2\pi \int_{t_A}^{t_B} x \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt$

If C is given in polar form, the results are

i about the initial line, $\theta = 0$: $S = 2\pi \int_{\alpha}^{\beta} r \sin \theta \sqrt{r^2 + \left(\frac{d\theta}{dr}\right)^2} d\theta$

ii about the line $\theta = \pm \frac{\pi}{2}$: $S = 2\pi \int_{\alpha}^{\beta} r \cos \theta \sqrt{r^2 + \left(\frac{d\theta}{dr}\right)^2} d\theta$