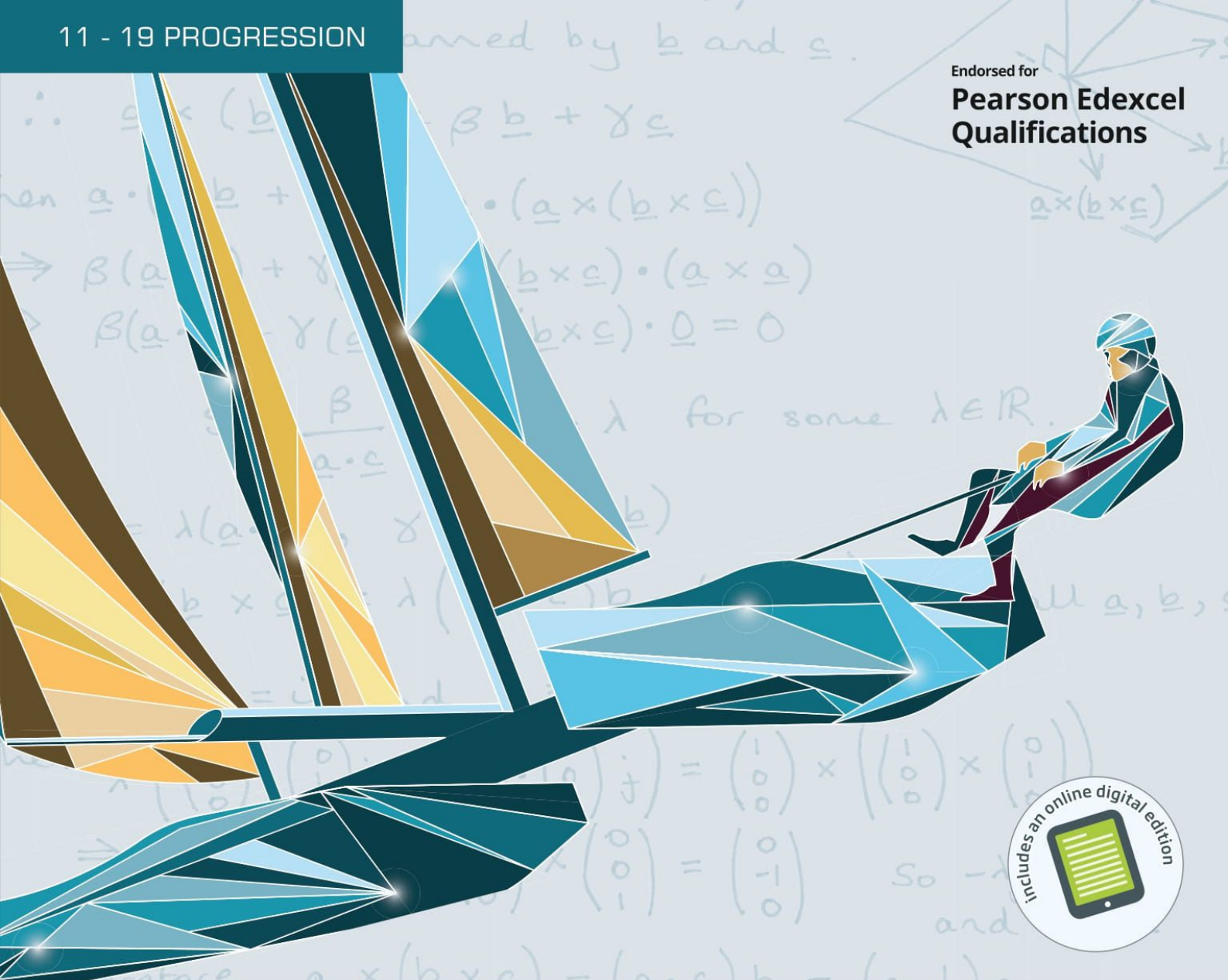




Edexcel AS and A level Further Mathematics

Further Pure Mathematics 2

FP2

Contents

● = A level only

Overarching themes	iv	4 Recurrence relations	120
Extra online content	vi	4.1 Forming recurrence relations	121
1 Number theory	1	4.2 Solving first-order recurrence relations	125
1.1 The division algorithm	2	● 4.3 Solving second-order recurrence relations	134
1.2 The Euclidean algorithm	5	4.4 Proving closed forms	142
1.3 Modular arithmetic	10	Mixed exercise 4	145
1.4 Divisibility tests	16	5 Matrix algebra	152
● 1.5 Solving congruence equations	20	5.1 Eigenvalues and eigenvectors	153
● 1.6 Fermat's little theorem	26	5.2 Reducing matrices to diagonal form	166
● 1.7 Combinatorics	28	5.3 The Cayley–Hamilton theorem	179
Mixed exercise 1	38	Mixed exercise 5	183
2 Groups	44	● 6 Integration techniques	188
2.1 The axioms for a group	45	● 6.1 Reduction formulae	189
2.2 Cayley tables and finite groups	51	● 6.2 Arc length	197
2.3 Order and subgroups	64	● 6.3 Area of a surface of revolution	206
● 2.4 Isomorphism	72	Mixed exercise 6	213
Mixed exercise 2	80	Review exercise 2	217
3 Complex numbers	86	Exam-style practice: AS	225
3.1 Loci in an Argand diagram	87	● Exam-style practice: A level	227
3.2 Regions in an Argand diagram	96	Answers	230
● 3.3 Transformations of the complex plane	100	Index	264
Mixed exercise 3	109		
Review exercise 1	113		

Overarching themes

The following three overarching themes have been fully integrated throughout the Pearson Edexcel AS and A level Mathematics series, so they can be applied alongside your learning and practice.

1. Mathematical argument, language and proof

- Rigorous and consistent approach throughout
- Notation boxes explain key mathematical language and symbols
- Dedicated sections on mathematical proof explain key principles and strategies
- Opportunities to critique arguments and justify methods

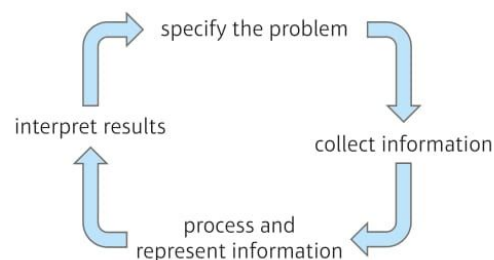
2. Mathematical problem solving

- Hundreds of problem-solving questions, fully integrated into the main exercises
- Problem-solving boxes provide tips and strategies
- Structured and unstructured questions to build confidence
- Challenge boxes provide extra stretch

3. Mathematical modelling

- Dedicated modelling sections in relevant topics provide plenty of practice where you need it
- Examples and exercises include qualitative questions that allow you to interpret answers in the context of the model
- Dedicated chapter in Statistics & Mechanics Year 1/AS explains the principles of modelling in mechanics

The Mathematical Problem-solving cycle



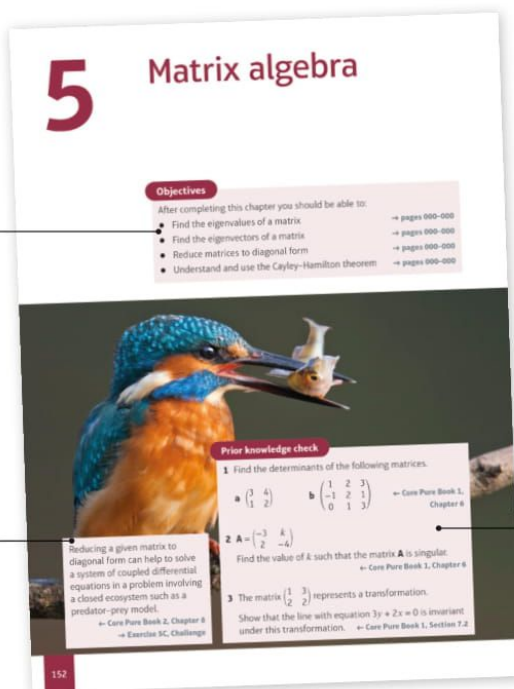
Finding your way around the book

Access an online digital edition using the code at the front of the book.



Each chapter starts with a list of objectives

The real world applications of the maths you are about to learn are highlighted at the start of the chapter with links to relevant questions in the chapter



The *Prior knowledge check* helps make sure you are ready to start the chapter

Exercise questions are carefully graded so they increase in difficulty and gradually bring you up to exam standard

Exercises are packed with exam-style questions to ensure you are ready for the exams

Challenge boxes give you a chance to tackle some more difficult questions

A level content is clearly flagged

Exam-style questions are flagged with **(E)**
Problem-solving questions are flagged with **(P)**

Chapter 3 Complex numbers

Exercise 3.1

5 a Sketch on the same Argand diagram:

- the locus of points representing $|z - 2| = |z - 8|$
- the locus of points representing $\arg(z - 4 - 2i) = \frac{\pi}{2}$
- the locus of points representing $\arg(z - 4 - 2i) = \frac{\pi}{4}$

The region R is defined by the inequalities $|z - 2| \leq |z - 8|$ and $0 \leq \arg(z - 4 - 2i) \leq \frac{\pi}{2}$.

b On your sketch from part a, identify, by shading, the region R .

6 On separate Argand diagrams, shade the regions, R , defined by the sets of points:

- $\{z \in \mathbb{C} : -\frac{\pi}{2} \leq \arg(z + 1 + i) \leq -\frac{\pi}{4}\} \cap \{z \in \mathbb{C} : |z + 1 + 2i| \leq 1\}$ (4 marks)
- $\{z \in \mathbb{C} : 2i - 6i \leq |z - 3i| \leq 7\} \cap \{z \in \mathbb{C} : \operatorname{Re}(z) \leq 7\}$ (4 marks)

7 a Shade on an Argand diagram the region defined by $|z + 6i| \leq 3$. (2 marks)
b The complex number z satisfies $|z + 6i| \leq 3$. Find the range of possible values of $\arg z$. (4 marks)

8 a Indicate on an Argand diagram the region consisting of the set of points satisfying both $\frac{\pi}{2} \leq \arg z \leq \pi$ and $\operatorname{Im}(z) \leq \operatorname{Re}(z)$. (3 marks)
b Find the exact area of this region. (3 marks)

9 a Shade on an Argand diagram the region R defined by $|z \in \mathbb{C} : |z - 3 + 2i| \geq \sqrt{2}|z - 1i| \cap \{z \in \mathbb{C} : 0 \leq \arg(z + 1 + 2i) \leq \frac{\pi}{3}\}$. (4 marks)
b Find the exact area of region R . (5 marks)
c The complex number z lies in region R . Find the maximum value of $\operatorname{Im}(z)$. (5 marks)

Challenge
On an Argand diagram, shade the set of points $\{z \in \mathbb{C} : 6 \leq \operatorname{Re}(z - 3i) \leq 12\} \cap \{z \in \mathbb{C} : \operatorname{Re}(z \operatorname{Im}(z)) \geq 0\}$

3.3 Transformations of the complex plane

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 $w = u + iv$.

It is helpful to be able to recognise the type of transformation - translation, enlargement, or rotation - from the formula for some simple transformations.

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.

Example 6

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:

- $T_1: w = z - 2 + 4i$
- $T_2: w = 3z$
- $T_3: w = \frac{1}{2}z + i$

The locus of P in the z -plane is a circle with centre O , 0 and radius 2 . This is the locus of P in the z -plane before any transformations have been applied.

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 $|z + i| = |z|/|z|$.
Use $|z| = 2$.

Each section begins with explanation and key learning points

Each chapter ends with a *Mixed exercise* and a *Summary of key points*

Step-by-step worked examples focus on the key types of questions you'll need to tackle

Problem-solving boxes provide hints, tips and strategies, and *Watch out* boxes highlight areas where students often lose marks in their exams

Every few chapters a *Review exercise* helps you consolidate your learning with lots of exam-style questions

Review exercise 2

1 a Find the general solution of the recurrence relation $u_n = 4u_{n-1} + 1, n \geq 1$. (4)
b Find the particular solution of the recurrence relation given that $u_0 = 7$. (2)

2 The diagram shows the first four pentagonal numbers.

a Find p_1 and p_2 . (1)
b Find, in terms of p_{n-1} , a recurrence relation for p_n . (2)
c Solve the recurrence relation to find a closed form for the n th pentagonal number. (3)
d Find p_{100} . (1)

3 Solve the recurrence relation $u_n = 2u_{n-1} + 3n + 1$, for $n \geq 0$, where $u_0 = 11$. (4)

4 A sequence is defined by the recurrence relation $u_{n+1} = 3u_n - 10$, with $u_1 = 7$.

a Find u_5 . (1)
b i Solve the recurrence relation. (2)
ii Find the smallest value of n for which u_n is greater than 1 million. (4)

5 A hospital patient receives 100 mg of a drug every 4 hours. Once administered, 20% of the drug remaining in the patient's body is lost every hour. Initially, the drug is not present in the patient's body. Let u_n represent the amount of the drug in the patient's body immediately after the n th dose.

a Find, in terms of u_{n-1} , a recurrence relation for u_n . (2)
b Solve the recurrence relation for u_n . (3)
c The amount of the drug present in the patient's body must not exceed 160 mg. What is the maximum number of doses that can be administered in this way? (3)

6 A finance company loans a customer, Heather, £3000 to help her buy a car. The company charges a fixed rate of interest of 1.8% per month for this loan which is added on the last day of each month. Heather agrees to make repayments of £300 on the first day of each month, starting with the second month. Heather needs to form a recurrence relation which defines the amount still owed, u_n , after n repayments.

a Define a correct recurrence relation which Heather can use. (2)
b Heather's final repayment to settle the loan will be less than £300. Use your recurrence relation to calculate the value of the final repayment Heather will need to make. (3)

Exam-style practice
Further Mathematics
AS Level
Further Pure 2

Time: 50 minutes
You must have: Mathematical Formulae and Statistical Tables, Calculator

1 a Using a suitable algorithm, and without performing any division explain why 1485 is divisible by 11. (1)
b Use the Euclidean algorithm to find integers p and q such that $1485p + 143q = 11$. (4)
c Hence find integers a and b such that $1485a + 143b = 22$. (1)

2 The set $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under the operation of multiplication modulo 20.

a Complete the Cayley table below for this group.

$\times$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3								
7								
9								
11								
13								
17								
19								

b Explain why $(G, \times_{20})$ cannot contain a subgroup of order 3. (4)
c Find three different subgroups of $(G, \times_{20})$ of order 2. (2)

3 L is the locus of points on an Argand diagram satisfied by $|z - 1| = \sqrt{2}|z + 9|$.

a Sketch clearly the locus L . (4)
On the same Argand diagram a finite region R is bounded by L and the condition $0 \leq \arg(z + 2i) \leq \frac{\pi}{6}$.
b i Show this region on your sketch. (1)
ii Find the exact area of region R . (3)

AS and A level practice papers at the back of the book help you prepare for the real thing.

Extra online content

Whenever you see an *Online* box, it means that there is extra online content available to support you.



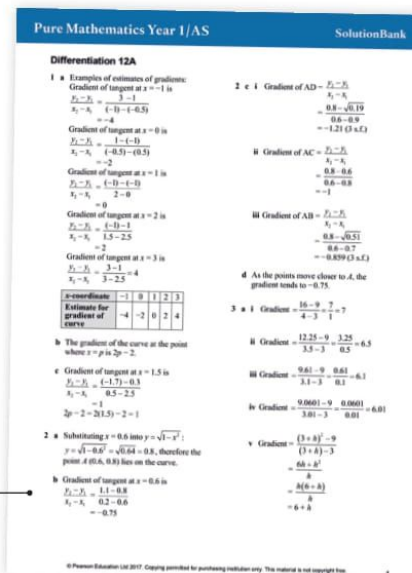
SolutionBank

SolutionBank provides a full worked solution for every question in the book.

Online Full worked solutions are available in SolutionBank.



Download all the solutions as a PDF or quickly find the solution you need online



Use of technology

Explore topics in more detail, visualise problems and consolidate your understanding using pre-made GeoGebra activities.

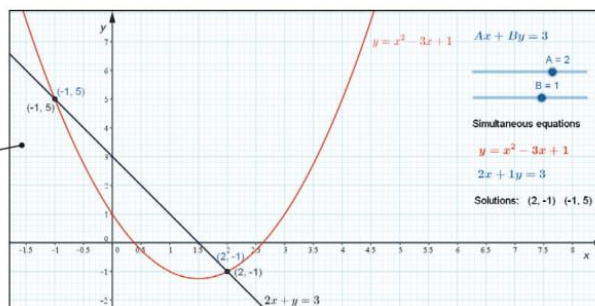
Online Find the point of intersection graphically using technology.



GeoGebra

GeoGebra-powered interactives

Interact with the maths you are learning using GeoGebra's easy-to-use tools



Access all the extra online content for free at:

www.pearsonschools.co.uk/fp2maths

You can also access the extra online content by scanning this QR code:



Number theory

1

Objectives

After completing this chapter you should be able to:

- Use the division algorithm and the Euclidean algorithm → pages 2–7
- Use the Euclidean algorithm to illustrate Bezout's identity → pages 8–10
- Understand and use modular arithmetic and congruences → pages 10–15
- Apply tests for divisibility by 2, 3, 4, 5, 6, 9, 10 and 11 → pages 16–20
- Solve simple congruence equations → pages 20–25
- Use Fermat's little theorem to find least positive residues → pages 26–27
- Solve counting problems → pages 28–37

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

'Check' digits in bar codes and book identification numbers help to identify and correct scanning errors. They are generated using modular arithmetic.

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 $|a| > |b| > 0$, 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 $m, n \in \mathbb{Z}$.

$$\begin{aligned} b &= ja \text{ for some } j \in \mathbb{Z} \\ c &= ka \text{ for some } k \in \mathbb{Z} \\ bn + cm &= (ja)n + (ka)m \\ &= (jn + km)a \end{aligned}$$

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 $b = 13$

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 $0 \leq r < b$.

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

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 can be written in the form $4q + r$ where $r = 0, 1, 2$ or 3 . 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 Given that $n \in \mathbb{Z}$ 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 $k \in \mathbb{Z}$.

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

Problem-solving

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 any 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 of 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 $90 = 2 \times 3^2 \times 5$ $84 = 2^2 \times 3 \times 7$
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:

$$\begin{aligned} a &= q_1b + r_1 \\ b &= q_2r_1 + r_2 \\ r_1 &= q_3r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_nr_{n-1} + r_n \\ r_{n-1} &= q_{n+1}r_n + 0 \end{aligned}$$

Online Implement the Euclidean algorithm using GeoGebra.



The last non-zero remainder in this process, r_n , is the greatest common divisor (or highest common factor) of a and b .

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.

A 24 Paulo has the five letter cards **M A T H S**

- E/P** 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 **H A T**
 - ii the letters in the word **H A 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)

26 Five adults and five children take it in turns to serve themselves from a buffet.

E/P Find the number of possible orders of people if:

- 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 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 , 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 $0 \leq r < b$.
 - Begin with values of a and b .
 - Set q equal to the greatest integer that is less than or equal to $\frac{a}{b}$
 - 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 $a \geq b$:
 - 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 $\gcd(a, b) = b$.
 - 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 $\gcd(a, b) = r_1$.
 - 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 .