

Divisibility and Prime Numbers

- 1 Write 360 as a product of prime factors, and hence find the number of positive divisors of 360. [3]
- 2 Without using a calculator, determine whether 7293 is divisible by (i) 3, (ii) 9, (iii) 11. [3]
- 3 Show that 391 is not a prime number. [2]
- 4 List all the prime numbers between 40 and 60. [2]
- 5 By writing 84 and 126 as products of prime factors, find their highest common factor and lowest common multiple. [3]
- 6 Prove that the sum of any three consecutive integers is a multiple of 3. [2]
- 7 Show that $n^2 + n$ is even for every integer n . [3]
- 8 Prove that the square of any odd integer can be written in the form $4k + 1$, where k is an integer. [3]
- 9 The number $N = 2^4 \times 3^2 \times 7$.
Find the number of positive divisors of N , and the sum of all the positive divisors of N . [4]
- 10 Find the smallest positive integer n such that $1080n$ is a perfect square. [3]
- 11 Given that the integer a divides both b and c , prove that a divides $3b - 5c$. [3]
- 12 Find the number of zeros at the end of $100!$ when it is written out as an integer. Explain your method. [3]
- 13 The four-digit number $64d8$ is divisible by 11, where d is a single digit. Find d . [3]
- 14 Prove that the product of any three consecutive integers is divisible by 6. [4]
- 15 Prove that the product of four consecutive integers, plus 1, is always a perfect square. [5]
- 16 Given that n is an odd integer, prove that $n^4 - 1$ is divisible by 16. [4]
- 17 Use a suitable test to show that 523 is a prime number. State clearly which primes you need to check and why. [4]
- 18 Prove by contradiction that $\sqrt{3}$ is irrational. [5]
- 19 A positive integer n has exactly 6 positive divisors. Show that n is of the form p^5 or p^2q , where p and q are distinct primes, and hence find all such integers n less than 30. [5]
- 20 Prove, without using induction, that $7^n - 1$ is divisible by 6 for every positive integer n . [4]
- 21 Prove that if p is a prime number greater than 3, then $p^2 - 1$ is divisible by 24. [6]
- 22 Prove that there are infinitely many prime numbers. [6]
- 23 Find all prime numbers p such that p , $p + 2$ and $p + 4$ are all prime. Justify your answer fully. [6]
- 24 Find all pairs of positive integers (a, b) such that $a^2 - b^2 = 105$. [6]

- 25** A student claims that $n^2 + n + 41$ is prime for every positive integer n , because it is prime when $n = 1, 2, 3, 4$ and 5 .
Show that the claim is false, and explain why the student's reasoning is not a valid proof. [6]
- 26** Prove that a positive integer has exactly three positive divisors if and only if it is the square of a prime number. [6]
- 27** Prove that $n^5 - n$ is divisible by 30 for every integer n . [8]
- 28** Let $n > 1$ be an integer. A Mersenne number is a number of the form $2^n - 1$.
(a) Prove that if $2^n - 1$ is prime then n is prime. (Hint: prove the contrapositive.) [6]
(b) Show by a counterexample that the converse of the statement in part (a) is false. [2]
- 29** Find all positive integers n for which $n^4 + 4$ is prime. [9]
- 30** In this question all letters represent integers.
(a) Prove that no number of the form $4k + 3$ can be written as the sum of two squares. [5]
(b) Use part (a) to show that 2023 cannot be written as the sum of two squares. Find integers a and b such that $a^2 + b^2 = 2029$. [4]

Euclidean Algorithm

- 1** Use Euclid's algorithm to find the highest common factor of 252 and 105 . [3]
- 2** Use Euclid's algorithm to find the highest common factor of 221 and 119 . [3]
- 3** Find the quotient and the remainder when 1000 is divided by 37 . [2]
- 4** Use Euclid's algorithm to determine whether 91 and 144 are coprime. [3]
- 5** The highest common factor of 18 and 24 is 6 . Use this to find their lowest common multiple. [2]
- 6** The highest common factor of 48 and n is 12 , where $50 < n < 70$. Find n . [2]
- 7** Use Euclid's algorithm to find the highest common factor of 2415 and 1449 . [3]
- 8** Find the highest common factor of 5593 and 2431 . [4]
- 9** Use Euclid's algorithm to show that 35 and 12 are coprime, and find integers x and y such that $35x + 12y = 1$. [4]
- 10** Find integers x and y such that $91x + 35y = 7$. [4]
- 11** Find the highest common factor and the lowest common multiple of 1989 and 1547 . [4]
- 12** Prove that any two consecutive integers are coprime. [3]
- 13** When a positive integer N is divided by 13 the quotient is twice the remainder. Given that $40 < N < 60$, find N . [3]
- 14** Use Euclid's algorithm to find the highest common factor h of 341 and 154 , and hence find integers x and y such that $341x + 154y = h$. [5]

- 15** The Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, ... where each term is the sum of the previous two.
 (a) Use Euclid's algorithm to find the highest common factor of the consecutive Fibonacci numbers 144 and 233. [3]
 (b) Prove that any two consecutive Fibonacci numbers are coprime. [2]
- 16** Let $a = bq + r$, where a , b , q and r are integers. Prove that $\text{hcf}(a, b) = \text{hcf}(b, r)$. [4]
- 17** Find all positive integers x less than 100 such that the highest common factor of x and 84 is 12. [5]
- 18** Use Euclid's algorithm to find an integer x with $0 < x < 43$ such that $17x$ leaves a remainder of 1 when divided by 43. [5]
- 19** Find the highest common factor of 360, 504 and 1260. [4]
- 20** Show that $15n + 4$ and $10n + 3$ are coprime for every integer n . [4]
- 21** The integers a and b are coprime. Prove that the highest common factor of $a + b$ and $a - b$ is either 1 or 2. [6]
- 22** The integers a , b and c are such that $\text{hcf}(a, b) = 1$ and a divides bc . Prove that a divides c . [6]
- 23** The highest common factor of 143 and 221 is h .
 (a) Use Euclid's algorithm to find h . [2]
 (b) Find integers x and y such that $143x + 221y = 13$. [3]
 (c) Hence find integers p and q such that $143p + 221q = 39$. [2]
- 24** Use Euclid's algorithm to find the highest common factor of $2^{12} - 1$ and $2^{18} - 1$, and show that your answer equals $2^h - 1$ where h is the highest common factor of 12 and 18. [6]
- 25** Find all the possible values of the highest common factor of $n^2 + 1$ and $n + 1$, as n varies over the positive integers, and state for which n each value occurs. [6]
- 26** A student uses Euclid's algorithm to find the highest common factor of 1241 and 533.
 $1241 = 2 \times 533 + 175$, $533 = 3 \times 175 + 8$, $175 = 21 \times 8 + 7$, $8 = 1 \times 7 + 1$, $7 = 7 \times 1 + 0$.
 The student concludes that the highest common factor is 7.
 (a) Explain the student's error. [1]
 (b) State the correct highest common factor. [1]
 (c) Hence find integers x and y such that $1241x + 533y = 1$. [4]
- 27** Prove that, for positive integers a and b , $\text{hcf}(a, b) \times \text{lcm}(a, b) = ab$. [8]
- 28** Let a and b be positive integers with $a > b$. Prove that $\text{hcf}(2^a - 1, 2^b - 1) = \text{hcf}(2^{a-b} - 1, 2^b - 1)$, and hence that $\text{hcf}(2^a - 1, 2^b - 1) = 2^{\text{hcf}(a, b)} - 1$. [9]
- 29** The highest common factor of two positive integers a and b is 6 and their lowest common multiple is 180. Given that $a < b$, find all possible pairs (a, b) . [8]
- 30** Prove that, for every positive integer n , the numbers $n! + 1$ and $(n + 1)! + 1$ are coprime. [8]

Modular Arithmetic

- 1** Find the smallest non-negative integer x such that $x \equiv 123 \pmod{7}$. [2]
- 2** Without calculating 47×58 , find its remainder when divided by 9. [3]

- | | | |
|----|---|-------------------|
| 3 | List all integers x such that $x \equiv 3 \pmod{5}$ and $10 < x < 30$. | [2] |
| 4 | Show that $2^{10} \equiv 1 \pmod{11}$. | [2] |
| 5 | Working in arithmetic modulo 11, find the values of $8 + 9$ and 8×9 . | [2] |
| 6 | Solve $x + 7 \equiv 3 \pmod{11}$, giving x as an integer with $0 \leq x < 11$. | [2] |
| 7 | Solve $5x \equiv 3 \pmod{8}$. | [3] |
| 8 | Find the remainder when 3^{100} is divided by 7. | [3] |
| 9 | Find the last digit of 7^{2023} . | [3] |
| 10 | Prove that the square of an integer is never of the form $3k + 2$. | [3] |
| 11 | Find the multiplicative inverse of 7 modulo 26, and hence solve $7x \equiv 5 \pmod{26}$. | [4] |
| 12 | Show that $10^n \equiv 1 \pmod{9}$ for every positive integer n , and hence prove that a positive integer is divisible by 9 if and only if its digit sum is divisible by 9. | [4] |
| 13 | Find all integers x with $0 \leq x < 7$ such that $x^2 \equiv 2 \pmod{7}$. | [3] |
| 14 | Find all solutions of $14x \equiv 21 \pmod{35}$ with $0 \leq x < 35$. | [5] |
| 15 | State Fermat's little theorem. Use it to find the remainder when 2^{100} is divided by 13. | [4] |
| 16 | Find the smallest positive integer N such that $N \equiv 2 \pmod{3}$, $N \equiv 3 \pmod{5}$ and $N \equiv 2 \pmod{7}$. | [5] |
| 17 | Find the last two digits of 7^{2024} . | [4] |
| 18 | Show that $2^{50} + 3^{50}$ is divisible by 13. | [5] |
| 19 | Solve the simultaneous congruences $3x + 2y \equiv 1 \pmod{7}$ and $x + 4y \equiv 3 \pmod{7}$, giving x and y in the range 0 to 6. | [5] |
| 20 | Integers x and y are such that $x^2 + y^2$ is divisible by 3. Prove that both x and y are divisible by 3. | [5] |
| 21 | Wilson's theorem states that if p is prime then $(p - 1)! \equiv -1 \pmod{p}$.
(a) Verify the theorem for $p = 7$.
(b) Use the theorem with $p = 23$ to find the remainder when $20!$ is divided by 23. | [2]
[4] |
| 22 | The order of a non-zero residue a modulo a prime p is the smallest positive integer k with $a^k \equiv 1 \pmod{p}$.
(a) Find the order of 3 modulo 7.
(b) Find the order of 2 modulo 7.
(c) Hence show that every non-zero residue modulo 7 is congruent to a power of 3, but not every one is congruent to a power of 2. | [2]
[2]
[2] |
| 23 | Prove that no integer of the form $8k + 7$ can be written as the sum of three squares of integers. | [6] |
| 24 | Find all integers x with $0 \leq x < 13$ such that $x^2 + x + 1 \equiv 0 \pmod{13}$. Show that the congruence $x^2 + x + 1 \equiv 0$ has no solutions modulo 11. | [6] |

- 25** A student solves $6x \equiv 9 \pmod{15}$ as follows.
Divide by 3: $2x \equiv 3 \pmod{15}$. Multiply by 8 (since $2 \times 8 = 16 \equiv 1$): $x \equiv 24 \equiv 9 \pmod{15}$. So $x = 9$.
The student's answer is incomplete.
(a) Explain what the student has done wrong. [2]
(b) Find all solutions of $6x \equiv 9 \pmod{15}$ with $0 \leq x < 15$. [4]
- 26** Today is a Thursday.
(a) On what day of the week will it be in 3^{50} days' time? [3]
(b) Find all positive integers n such that it will again be a Thursday in 3^n days' time. [3]
- 27** Let p be a prime and a an integer not divisible by p . Prove Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p}$. [8]
- 28** Find the smallest positive integer that leaves remainder 2 when divided by 5, remainder 3 when divided by 7, and remainder 4 when divided by 9. Show clearly that your answer is the smallest. [8]
- 29** Find all positive integers n for which $2^n + 3^n$ is divisible by 7. [8]
- 30** Let p be a prime of the form $4k + 3$. Given that p divides $a^2 + b^2$, where a and b are integers, prove that p divides both a and b . (You may use Fermat's little theorem.) [9]

Diophantine Equations

- 1** Find one pair of integers x and y that satisfy $3x + 5y = 1$. [2]
- 2** Explain why $6x + 9y = 20$ has no integer solutions. [2]
- 3** Show that $4x + 6y = 10$ has integer solutions, and write down one. [2]
- 4** Find all positive integer solutions of $x + 3y = 10$. [2]
- 5** Given that $x = 3$ and $y = -2$ is a solution of $5x + 7y = 1$, write down the general integer solution of $5x + 7y = 1$. [2]
- 6** Show that $2x + 4y = 7$ has no integer solutions. [2]
- 7** Find the general integer solution of $3x + 4y = 5$. [3]
- 8** Use Euclid's algorithm to find the general integer solution of $17x + 13y = 1$. [4]
- 9** A post office has only 5p and 8p stamps. Find all the ways of making exactly 53p using these stamps. [4]
- 10** Find all the positive integer solutions of $12x + 18y = 30$. [3]
- 11** Determine whether each equation has integer solutions: (i) $14x + 21y = 100$, (ii) $14x + 21y = 105$. Find the general solution where one exists. [4]
- 12** Find the number of ways of making exactly £2.30 using only 20p coins and 50p coins, and state each way. [4]
- 13** Find all pairs of positive integers (x, y) such that $x^2 - y^2 = 21$. [3]

- 14** Find the general integer solution of $23x + 37y = 1$, and write down the solution in which x is the smallest positive value. [5]
- 15** Find the general integer solution of $15x + 21y = 9$, and hence find the solution with $0 < y < 5$. [5]
- 16** A machine accepts only 3p and 5p coins. Show that it is impossible to pay exactly 7p, but that every whole number of pence from 8p upwards can be paid exactly. [5]
- 17** Find all pairs of positive integers (x, y) such that $x^2 + y^2 = 125$. [4]
- 18** Prove that the equation $x^2 - 5y^2 = 3$ has no integer solutions. [4]
- 19** Find all the positive integer solutions of the simultaneous equations $x + y + z = 10$ and $2x + 3y + 5z = 28$. [5]
- 20** Find all the non-negative integer solutions of $13x + 8y = 300$. [5]
- 21** Every primitive Pythagorean triple (a, b, c) , with $a^2 + b^2 = c^2$ and no common factor, can be written as $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ (or with a and b swapped), where $m > n$ are coprime positive integers of opposite parity. Use this to find all the primitive Pythagorean triples with hypotenuse 65. [6]
- 22** Consider the equation $x^2 - 2y^2 = 1$ where x and y are positive integers.
 (a) Find the solution with the smallest value of y . [1]
 (b) Expand $(3 + 2\sqrt{2})^2$ and hence find a second solution. [3]
 (c) By considering $(3 + 2\sqrt{2})(17 + 12\sqrt{2})$, find a third solution. [2]
- 23** Prove that an integer of the form $4k + 2$ cannot be written as a difference of two squares of integers. Hence show that 2018 cannot be written as $x^2 - y^2$. [6]
- 24** A merchant buys exactly 100 animals for exactly £100. Cows cost £10 each, sheep cost £3 each and hens cost 50p each. He buys at least one animal of each type. Find the number of each animal he buys. [7]
- 25** A student considers the equation $12x + 18y = c$ and writes: "hcf(12, 18) = 6, and 6 is smaller than 15, so there will be integer solutions when $c = 15$."
 (a) Explain the student's error. [2]
 (b) List the values of c between 1 and 30 inclusive for which the equation has integer solutions, and find a solution when $c = 30$. [4]
- 26** Find the number of positive integer solutions of the equation $7x + 11y = 1000$, and give the solution with the smallest x and the solution with the largest x . [6]
- 27** A shop sells sweets only in bags of 5 and bags of 7.
 (a) Show that it is impossible to buy exactly 23 sweets. [3]
 (b) Prove that every number of sweets $n \geq 24$ can be bought exactly. [5]
- 28** Let (a, b, c) be a Pythagorean triple of positive integers, so $a^2 + b^2 = c^2$.
 (a) Prove that at least one of a and b is divisible by 3. [4]
 (b) Prove that at least one of a and b is divisible by 4. [6]
- 29** Find all pairs of positive integers (x, y) such that $x^2 - y^2 = 2024$. [8]
- 30** Prove that the only integer solution of $x^2 + y^2 = 3z^2$ is $x = y = z = 0$. [9]

Binary Operations

- 1** The binary operation $*$ is defined on the real numbers by $a * b = a + 2b$. Evaluate $3 * 4$ and $4 * 3$, and state whether $*$ is commutative. [3]

- 2** Determine whether subtraction is a closed operation on (a) the positive integers, (b) the integers. Justify each answer. [2]

- 3** The table shows a binary operation $\circ$ on the set $\{1, 2, 3\}$. Explain why the set is not closed under $\circ$.

$\circ$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	4

[2]

- 4** A binary operation $*$ is defined on the real numbers by $a * b = ab + 1$. Evaluate $(2 * 3) * 4$ and $2 * (3 * 4)$. What do your answers show about the operation? [3]

- 5** The operation $*$ on the real numbers is defined by $a * b = a + b - 3$. Find the identity element. [2]

- 6** A commutative binary operation $\circ$ on the set $\{p, q, r\}$ satisfies $p \circ q = q$, $p \circ r = r$ and $q \circ r = p$, and p is its identity element. Write down the value of $r \circ q$ and of $r \circ p$. [2]

- 7** The binary operation $*$ is defined on the real numbers by $a * b = a + b + ab$. Prove that $*$ is commutative and associative. [4]

- 8** The binary operation $*$ is defined on the real numbers by $a * b = a + b + 2$. Find the identity element and the inverse of a general element a . [4]

- 9** The operation $*$ on the integers is defined by $a * b = |a - b|$. Determine whether $*$ is (i) commutative, (ii) associative. [4]

- 10** Multiplication modulo 6 is a binary operation on the set $\{0, 1, 2, 3, 4, 5\}$. State the identity element, and find which elements have an inverse. [4]

- 11** The operation $\circ$ on the integers is defined by $a \circ b = \max(a, b)$. Show that $\circ$ is closed, commutative and associative, but that there is no identity element on the set of all integers. [4]

- 12** Show, by a counterexample, that addition does not distribute over multiplication on the real numbers, i.e. that $a + (b \times c)$ is not always equal to $(a + b) \times (a + c)$. [3]

- 13** The table shows multiplication modulo 5 on the set $\{1, 2, 3, 4\}$. State the identity element and the inverse of each element.

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

[4]

- 14** The binary operation $*$ is defined on the set $S = \{x \in \mathbb{R} : x \neq 1\}$ by $a * b = a + b - ab$.
- (a) Show that S is closed under $*$. [2]
- (b) Find the identity element. [1]
- (c) Find the inverse of a general element a in S . [2]
-
- 15** Let G be the set of ordered pairs (a, b) of real numbers with $a \neq 0$, and define $(a, b) * (c, d) = (ac, ad + b)$.
- (a) Prove that $*$ is associative. [3]
- (b) Find the identity element and the inverse of (a, b) . [3]
-
- 16** The operation $\circ$ on the set $\{0, 1, 2, 3\}$ is defined by $a \circ b = (a + 2b) \bmod 4$. Draw up the operation table, and determine whether $\circ$ is commutative and whether it has an identity element. [5]
-
- 17** Let H be the set of matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ where x is a real number, under matrix multiplication. Show that H is closed, that multiplication is commutative on H , and that H contains an identity element and an inverse for each of its elements. [5]
-
- 18** The operation $*$ on the real numbers is defined by $a * b = a^2 + b^2$. Show that $*$ is commutative but not associative, and that there is no identity element. [5]
-
- 19** The operation $*$ on the positive integers is defined by $a * b = a^b$. Determine whether $*$ is commutative, whether it is associative, and whether it has an identity element. [5]
-
- 20** The operation $*$ on the subsets of $\{1, 2, 3\}$ is defined by $A * B = (A \cup B) - (A \cap B)$, where $-$ denotes set difference, so $A * B$ is the set of elements in exactly one of A and B . Find $\{1, 2\} * \{2, 3\}$, and show that the empty set is the identity element and that every subset is its own inverse. [5]
-
- 21** The binary operation $*$ is defined on the real numbers by $a * b = a + b + kab$, where k is a non-zero constant.
- (a) Show that $*$ is associative for every value of k . [3]
- (b) Find the identity element. [1]
- (c) Find the inverse of a , stating the value of a for which no inverse exists. [3]
-
- 22** The binary operation $*$ on a set S is associative and has an identity element e .
- (a) Prove that the identity element is unique. [2]
- (b) Prove that, if an element a has an inverse, then the inverse is unique. [4]
-
- 23** Count the binary operations that can be defined on the set $\{0, 1\}$.
- (a) How many binary operations are there on $\{0, 1\}$? Explain your answer. [2]
- (b) How many of these are commutative? [2]
- (c) How many have an identity element? [2]
-
- 24** A student claims that the operation $a * b = \frac{(a + b)}{2}$ on the real numbers is associative "because it is commutative".
- (a) Explain why the student's reasoning is invalid. [1]
- (b) Evaluate $(1 * 2) * 3$ and $1 * (2 * 3)$ to show that $*$ is not associative. [2]
- (c) Show that $(a * b) * c = a * (b * c)$ holds only when $a = c$. [3]

- 25** The table shows a binary operation $\circ$ on the set $\{e, a, b, c\}$.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	b	c
b	b	b	c	e
c	c	c	e	b

- (a) Show that e is the identity element and that every element has an inverse. [3]
 (b) By evaluating $(a \circ b) \circ c$ and $a \circ (b \circ c)$, show that $\circ$ is not associative. [3]

- 26** The operation $*$ is defined on the positive real numbers by $a * b = \frac{ab}{(a+b)}$. Prove that $*$ is associative, and show that there is no identity element. [6]

- 27** The binary operation $*$ on a set S is associative and has an identity element e . Given that $a * a = e$ for every element a of S , prove that $*$ is commutative. [8]

- 28** The binary operation $*$ is defined on the real numbers by $a * b = pa + qb + r$, where p , q and r are constants. Find all the triples (p, q, r) for which $*$ is associative. [9]

- 29** The operation $*$ is defined on the open interval $S = (-1, 1)$ by $a * b = \frac{(a+b)}{(1+ab)}$.
 (a) Show that S is closed under $*$. [3]
 (b) Prove that $*$ is associative. [4]
 (c) Find the identity element and the inverse of a . [2]

- 30** The binary operation $*$ is defined on the real numbers by $a * b = a|b|$.
 (a) Prove that $*$ is associative. [3]
 (b) Show that $*$ is not commutative. [2]
 (c) Find all the elements e such that $a * e = a$ for all a (right identities), and show that there is no element f with $f * a = a$ for all a (left identity). [3]

Groups

- 1** Show that the integers under addition, $(\mathbb{Z}, +)$, satisfy the identity and inverse axioms of a group. [3]
2 Explain why the set of non-negative integers $\{0, 1, 2, 3, \dots\}$ under addition is not a group. [2]
3 The set $\{1, -1, i, -i\}$ is a group under multiplication of complex numbers. State the order of the group and the inverse of i . [2]
4 Explain why the real numbers under multiplication, $(\mathbb{R}, \times)$, do not form a group. [2]
5 Consider the integers modulo 6 under addition, $\{0, 1, 2, 3, 4, 5\}$. State the identity, the inverse of 4, and the order of the group. [3]
6 In a group, $a * b = a * c$. Show that $b = c$. [2]
7 State the four axioms that a set G with a binary operation $*$ must satisfy for $(G, *)$ to be a group. [4]

- 8** The table shows multiplication modulo 7 on the set $\{1, 2, 4\}$. Show that this set is a group under this operation.

$\times$	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

[4]

- 9** Show that the set $\{0, 1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6. [3]

- 10** Let $\omega = e^{2\pi i/3}$, so that $\omega^3 = 1$ and $1 + \omega + \omega^2 = 0$. Show that $\{1, \omega, \omega^2\}$ is a group under multiplication. [4]

- 11** Let a and b be elements of a group G . Prove that $(ab)^{-1} = b^{-1}a^{-1}$. [3]

- 12** The group $(\mathbb{Z}_8, +)$ consists of the integers 0 to 7 under addition modulo 8. Find the order of each non-zero element. [4]

- 13** Consider the group of non-zero residues modulo 11 under multiplication.
 (a) Find the inverse of 7. [2]
 (b) Find the order of 3. [2]

- 14** Show that the set $\{1, 3, 5, 7\}$ is a group under multiplication modulo 8. State, with a reason, whether every element is its own inverse. [5]

- 15** In the group S_3 of permutations of $\{1, 2, 3\}$, let $p = (1\ 2\ 3)$ and $q = (1\ 2)$. Products are composed right to left, so pq means "apply q first, then p ".
 (a) Find pq and qp , and state whether S_3 is abelian. [3]
 (b) Find p^{-1} and the order of p . [2]

- 16** Find the order of every element of the group of non-zero residues modulo 7 under multiplication. [5]

- 17** Prove that the set of matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with a, b, d real and $ad \neq 0$ forms a group under matrix multiplication. [6]

- 18** G is a group in which $(ab)^2 = a^2b^2$ for all $a, b \in G$. Prove that G is abelian. [4]

- 19** The functions $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$ and $f_4(x) = -\frac{1}{x}$ are defined for $x \in \mathbb{R}$, $x \neq 0$. Show that $\{f_1, f_2, f_3, f_4\}$ is a group under composition of functions, where $(f \circ g)(x) = f(g(x))$. [5]

- 20** Prove that the set $U = \{z \in \mathbb{C} : |z| = 1\}$ forms a group under multiplication. [5]

- 21** Let a and b be elements of a group G . Prove that ab and ba have the same order. [6]

- 22** The six functions $f_1(x) = x$, $f_2(x) = 1 - x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = \frac{1}{(1-x)}$, $f_5(x) = \frac{(x-1)}{x}$ and $f_6(x) = \frac{x}{(x-1)}$ form a group under composition of functions, $(f \circ g)(x) = f(g(x))$.
 (a) Show that $f_2 \circ f_3 = f_5$ and $f_3 \circ f_2 = f_4$, and hence that the group is not abelian. [3]
 (b) Find $f_4 \circ f_5$ and hence write down the inverse of f_4 . [3]
 (c) Find the order of f_4 . [1]

- 23** The non-zero residues modulo 13 form a group of order 12 under multiplication.
 (a) Show that the element 2 has order 12. [3]
 (b) Hence find the order of 5 and of 4, giving your reasoning. [3]
-
- 24** A student writes: "The set of odd integers under addition is a group, because the inverse of an odd number a is $-a$, which is also odd."
 (a) Identify two of the group axioms that the set of odd integers fails to satisfy. [3]
 (b) Show that the set of even integers under addition is a group. [3]
-
- 25** A group G has four elements e, a, b, c , with e the identity, $a^2 = b^2 = c^2 = e$ and $ab \neq e$. Show that $ab = c$ and that G is abelian, and write down the complete group table. [6]
-
- 26** G is a group of order 3 with identity e and other elements a and b . Show that $ab = e$, and complete the group table by finding a^2 , b^2 and ba . [6]
-
- 27** Let S be a finite non-empty set with an associative binary operation under which S is closed, and suppose both cancellation laws hold: $xa = xb$ implies $a = b$, and $ax = bx$ implies $a = b$. Prove that S is a group. [9]
-
- 28** Elements a and b of a group G have orders m and n respectively, where m and n are coprime, and $ab = ba$. Prove that ab has order mn . [9]
-
- 29** Let G be a finite group of even order. Prove that G contains an odd number of elements of order 2. [8]
-
- 30** Let G be the set of 2×2 matrices whose entries are 0 or 1 and whose determinant is odd (non-zero modulo 2). Matrix multiplication is carried out with all entries reduced modulo 2; you may assume that G is a group under this operation.
 (a) Show that G has exactly 6 elements, and list them. [3]
 (b) Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Find AB and BA , and deduce that G is not abelian. [3]
 (c) Show that AB has order 3, and explain why G has no element of order 6. [2]

Subgroups

- 1** Show that $\{0, 2, 4\}$ is a subgroup of the group $(\mathbb{Z}_6, +)$. [2]
-
- 2** Show that $\{0, 1, 2\}$ is not a subgroup of the group $(\mathbb{Z}_6, +)$. [2]
-
- 3** State Lagrange's theorem. Hence explain why a group of order 12 cannot have a subgroup of order 5. [2]
-
- 4** A group has order 15. List all the possible orders of its subgroups. [2]
-
- 5** Write down the subgroup of $(\mathbb{Z}_{12}, +)$ generated by 3. [2]
-
- 6** Write down two subgroups that every group G has. [2]
-
- 7** Show that $\{1, -1\}$ is a subgroup of the group $\{1, -1, i, -i\}$ under multiplication. [3]
-
- 8** Find all the subgroups of $(\mathbb{Z}_6, +)$. [4]
-
- 9** In the group of non-zero residues modulo 7 under multiplication, find the subgroup generated by 2 and the subgroup generated by 3. [3]

- 10** $H = \{0, 4, 8\}$ is a subgroup of $(\mathbb{Z}_{12}, +)$. List all the distinct cosets of H . [3]
- 11** Let H be a subgroup of a group G with identity e . Prove that the identity element of H is e . [3]
- 12** In the group S_3 , find the subgroup generated by $(1\ 2\ 3)$ and the subgroup generated by $(1\ 2)$. [3]
- 13** G is a group of order 7. Prove that G has no subgroups other than $\{e\}$ and G , and that every non-identity element has order 7. [3]
- 14** Use a subgroup test to prove that $H = \{2^k : k \in \mathbb{Z}\}$ is a subgroup of the group of positive rational numbers under multiplication. [4]
- 15** The set $k\mathbb{Z}$ consists of all integer multiples of the integer k . Prove that $3\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$, and that $3\mathbb{Z} \cap 5\mathbb{Z} = 15\mathbb{Z}$. [5]
- 16** $H = \{0, 2, 4\}$ and $K = \{0, 3\}$ are subgroups of $(\mathbb{Z}_6, +)$.
(a) Find $H \cap K$ and show that it is a subgroup. [2]
(b) Show that $H \cup K$ is not a subgroup. [3]
- 17** A group G has order 10.
(a) List the possible orders of elements of G . [2]
(b) Given that G has no element of order 10, explain why every non-identity element has order 2 or 5. [2]
- 18** The centre of a group G is $Z(G) = \{z \in G : zx = xz \text{ for all } x \in G\}$. Prove that $Z(G)$ is a subgroup of G . [5]
- 19** In S_3 , with composition right to left, let $H = \{e, (1\ 2)\}$. Find the three distinct left cosets pH of H and verify that they partition S_3 . [5]
- 20** Let a be an element of a group G . Prove that $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G . [4]
- 21** Find all the subgroups of the group $(\mathbb{Z}_{12}, +)$, and show that there is exactly one subgroup of each possible order. [6]
- 22** List all the subgroups of S_3 , and explain why there are no others. [6]
- 23** H and K are subgroups of a finite group G , where $|H|$ and $|K|$ are coprime. Prove that $H \cap K = \{e\}$. Hence give the intersection of subgroups of orders 4 and 9 of a group of order 36. [6]
- 24** A student claims that $\{0, 1, 2, 3\}$ is a subgroup of $(\mathbb{Z}_8, +)$ "because it has 4 elements and 4 divides 8, as Lagrange's theorem requires".
(a) Explain why this reasoning is wrong and show that the set is not a subgroup. [3]
(b) Find the subgroup of order 4 of $(\mathbb{Z}_8, +)$ and justify that it is the only one. [3]
- 25** In the group $(\mathbb{Z}_{20}, +)$, H is the subgroup generated by 8.
(a) List the elements of H . [2]
(b) Write down all the distinct cosets of H . [2]
(c) Determine whether $7 + H = 19 + H$. [2]
- 26** G is an abelian group. Prove that $H = \{g \in G : g^2 = e\}$ is a subgroup of G . Find H when $G = (\mathbb{Z}_{12}, +)$, where the identity is 0. [6]
- 27** Prove Lagrange's theorem: if H is a subgroup of a finite group G then $|H|$ divides $|G|$. [9]

- 28** Let G be a group whose only subgroups are $\{e\}$ and G itself, where $G \neq \{e\}$. Prove that G is cyclic and of prime order. [9]
- 29** H and K are finite subgroups of a group G . Prove that the set $HK = \{hk : h \in H, k \in K\}$ contains exactly $\frac{|H||K|}{|H \cap K|}$ distinct elements. [8]
- 30** U is the set of positive integers less than 15 that are coprime to 15, under multiplication modulo 15. You may assume that U is a group.
- (a) List the elements of U and state its order. [2]
- (b) Use Lagrange's theorem to prove that $a^8 \equiv 1 \pmod{15}$ for every a in U . [3]
- (c) Hence find the remainder when 7^{222} is divided by 15. [3]

Cyclic Groups

- 1** Explain why every non-zero element of $(\mathbb{Z}_5, +)$ is a generator of the group. [2]
- 2** Show that $(\mathbb{Z}_7, +)$ is cyclic, with 3 as a generator. [2]
- 3** Let $G = \langle a \rangle$ be a cyclic group of order 6. List the elements of G , and state the order of a^2 . [3]
- 4** Show that the group $\{1, i, -1, -i\}$ under multiplication is cyclic, and write down a generator. [2]
- 5** Find the order of the element 4 in the group $(\mathbb{Z}_{10}, +)$. [2]
- 6** Prove that every cyclic group is abelian. [2]
- 7** Find all the generators of the group $(\mathbb{Z}_{12}, +)$. [3]
- 8** The element a generates a cyclic group of order 12. Find the orders of a^2, a^3, a^4, a^5 and a^6 . [4]
- 9** Show that the group $\{1, 3, 5, 7\}$ under multiplication modulo 8 is not cyclic. [3]
- 10** Show that the group of non-zero residues modulo 7 under multiplication is cyclic. [3]
- 11** The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ consists of ordered pairs (a, b) with $a \in \mathbb{Z}_2, b \in \mathbb{Z}_3$, added componentwise. Show that it is cyclic by finding a generator. [4]
- 12** Let $\omega = e^{i\pi/3}$. Show that the sixth roots of unity form a cyclic group under multiplication, generated by ω , and list its elements in the form ω^k . Name another generator. [4]
- 13** List the generators of $(\mathbb{Z}_{20}, +)$ and state how many there are. [3]
- 14** G is a cyclic group of order 18 generated by a . Find all subgroups of G , giving a generator for each. [5]
- 15** Let $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$ be groups of ordered pairs under componentwise addition. Show that neither group is cyclic. [5]
- 16** The element a of a group has order n . Prove that a^k has order $\frac{n}{\text{hcf}(n, k)}$. [5]
- 17** The units modulo 9, $U = \{1, 2, 4, 5, 7, 8\}$, form a group under multiplication modulo 9. Show that U is cyclic and find all its generators. [5]

- 18** $G = \langle a \rangle$ is a cyclic group of order 15. Find the elements of G of order 5 and the elements of G of order 3. [5]
- 19** Find the number of solutions of $x^2 = e$ in (a) a cyclic group of order 8 and (b) a cyclic group of order 9. [5]
- 20** Let $z = e^{2\pi i/5}$. The fifth roots of unity form a cyclic group of order 5 under multiplication. Show that z^2 is also a generator, and express z^3 as a power of z^2 . [5]
- 21** Prove that every subgroup of the group of integers under addition, $(\mathbb{Z}, +)$, has the form $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for some non-negative integer n . [6]
- 22** A primitive root modulo a prime p is an element which generates the group of non-zero residues modulo p under multiplication. Show that 2 is a primitive root modulo 11, and find all the primitive roots modulo 11. [6]
- 23** In a group, if a has order m and b has order n then the element (a, b) of the product group has order $\text{lcm}(m, n)$.
(a) Use this to show that $\mathbb{Z}_4 \times \mathbb{Z}_6$ (componentwise addition) is not cyclic. [3]
(b) Show that $\mathbb{Z}_4 \times \mathbb{Z}_9$ is cyclic. [3]
- 24** A student studying the group $(\mathbb{Z}_{12}, +)$ writes: "8 is a generator because $8 = 8 \times 1$, so its order is 8, and in fact every odd number is a generator."
(a) Find the order of 8 in $(\mathbb{Z}_{12}, +)$ and state whether 8 is a generator. [2]
(b) Give a counterexample to the claim that every odd number is a generator. [2]
(c) State the correct rule for the generators of $(\mathbb{Z}_n, +)$. [2]
- 25** A circular combination lock has 15 positions numbered 0 to 14. Each time the lock is turned the dial advances k positions (modulo 15) from its current position, starting at 0.
(a) Find the positions visited when $k = 6$ and the number of turns before the dial first returns to 0. [2]
(b) Find all the values of k , $1 \leq k \leq 14$, for which every position is eventually visited. [3]
(c) Explain why the number of turns before returning to 0 is always a factor of 15. [1]
- 26** $G = \langle a \rangle$ is a cyclic group of order n . Prove that for each positive divisor d of n , G has exactly one subgroup of order d . [6]
- 27** $G = \langle a \rangle$ is a cyclic group of order n . Use the fact that G has exactly one subgroup of order d for each divisor d of n to prove that the number of elements of order d is $\varphi(d)$, where $\varphi(d)$ is the number of integers between 1 and d coprime to d , and hence that the sum of $\varphi(d)$ over all divisors d of n equals n . Verify the result for $n = 12$. [8]
- 28** Prove that every group of order 4 is either cyclic or has every non-identity element of order 2, and in the second case that the group is abelian. [8]
- 29** Let g be a primitive root modulo a prime p . Prove that g^k is a primitive root if and only if $\text{hcf}(k, p - 1) = 1$. Hence find all the primitive roots modulo 13, given that 2 is one. [8]
- 30** The group U_{2^k} consists of the residues modulo 2^k that are odd, under multiplication modulo 2^k , for $k \geq 3$.
(a) Prove that a cyclic group has at most two elements x with $x^2 = e$. [4]
(b) Show that $1, 2^{k-1} - 1, 2^{k-1} + 1$ and $2^k - 1$ are four different elements of U_{2^k} that each square to 1, and deduce that U_{2^k} is not cyclic. [5]

Group Isomorphisms

- 1 State the two conditions that a function $\varphi : G \rightarrow H$ between groups must satisfy to be an isomorphism. [2]
- 2 Explain why a group of order 6 cannot be isomorphic to a group of order 8. [2]
- 3 The function φ maps the group $(\mathbb{Z}_4, +)$ to the group $\{1, i, -1, -i\}$ under multiplication by $\varphi(k) = i^k$. Find $\varphi(0)$, $\varphi(1)$, $\varphi(2)$ and $\varphi(3)$, and verify that $\varphi(1 + 3) = \varphi(1)\varphi(3)$. [3]
- 4 Explain why an abelian group cannot be isomorphic to a non-abelian group. [2]
- 5 Show that $\varphi(x) = 2x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, +)$. [2]
- 6 Show that $f(x) = x + 1$ is not a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, +)$. [2]
- 7 Show that the function $\varphi(x) = e^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$, where $\mathbb{R}^+$ is the set of positive real numbers. [4]
- 8 Prove that $\varphi(k) = i^k$ defines an isomorphism from $(\mathbb{Z}_4, +)$ to the group $\{1, i, -1, -i\}$ under multiplication. [4]
- 9 Explain why the group $\{1, 3, 5, 7\}$ under multiplication modulo 8 is not isomorphic to $(\mathbb{Z}_4, +)$. [3]
- 10 Explain why $(\mathbb{Z}_6, +)$ and the group S_3 of permutations of $\{1, 2, 3\}$ are not isomorphic. [3]
- 11 Let $\varphi : G \rightarrow H$ be a homomorphism between groups, with identities e_G and e_H . Prove that $\varphi(e_G) = e_H$ and that $\varphi(a^{-1}) = (\varphi(a))^{-1}$. [4]
- 12 List the orders of the elements of $(\mathbb{Z}_8, +)$ and of $(\mathbb{Z}_2 \times \mathbb{Z}_4, +)$. Hence explain why these groups are not isomorphic. [4]
- 13 The table shows a group $G = \{e, a, b\}$ under $\circ$. Show that G is isomorphic to $(\mathbb{Z}_3, +)$ by giving an isomorphism φ and explaining why it works.

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

 [4]
- 14 Prove that $\varphi(k) = 2^k \pmod{5}$ defines an isomorphism from $(\mathbb{Z}_4, +)$ to the group of non-zero residues modulo 5 under multiplication. [5]
- 15 Show that the function $\varphi(k) = (k \pmod{2}, k \pmod{3})$ is an isomorphism from $(\mathbb{Z}_6, +)$ to $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$. [5]
- 16 Show that the group $\{1, 3, 5, 7\}$ under multiplication modulo 8 is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, by defining a suitable isomorphism and checking it. [5]
- 17 Let $\varphi : G \rightarrow H$ be an isomorphism and let $a \in G$ have order n . Prove that $\varphi(a)$ has order n . [5]

- 18** Show that the group of non-zero real numbers under multiplication is not isomorphic to the group $(\mathbb{R}, +)$. [5]
- 19** Show that the group of matrices $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $x \in \mathbb{R}$, under matrix multiplication is isomorphic to $(\mathbb{R}, +)$. [4]
- 20** $G = \langle a \rangle$ and $H = \langle b \rangle$ are cyclic groups, both of order n . Prove that G and H are isomorphic. [5]
- 21** Each of the following four groups has order 4: $A = \{1, i, -1, -i\}$ under multiplication; $B = \{1, 3, 5, 7\}$ under multiplication modulo 8; $C =$ the non-zero residues modulo 5 under multiplication; $D = \{1, 5, 7, 11\}$ under multiplication modulo 12. Decide which of the groups are isomorphic to $(\mathbb{Z}_4, +)$ and which to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, giving reasons. [6]
- 22** The function $\varphi : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_4$ is defined by $\varphi(x) = x \bmod 4$.
 (a) Show that φ is a homomorphism from $(\mathbb{Z}_{12}, +)$ to $(\mathbb{Z}_4, +)$. [2]
 (b) Find the kernel of φ , the set of elements mapped to the identity, and the image of φ . [2]
 (c) Explain why φ is not an isomorphism. [2]
- 23** Count the elements of each order in $(\mathbb{Z}_8, +)$ and in $(\mathbb{Z}_2 \times \mathbb{Z}_4, +)$, and hence prove that the two groups are not isomorphic. [6]
- 24** A student writes: "The groups $(\mathbb{Z}_4, +)$ and $\{1, 3, 5, 7\}$ under multiplication modulo 8 both have order 4 and both are abelian, so they must be isomorphic."
 (a) Explain why the student's reasoning is not valid. [2]
 (b) Prove that the two groups are not isomorphic. [2]
 (c) Name the group of order 4 that $\{1, 3, 5, 7\}$ is isomorphic to. [2]
- 25** Let G be a group. Prove that the function $\varphi : G \rightarrow G$ defined by $\varphi(x) = x^{-1}$ is a homomorphism if and only if G is abelian. [6]
- 26** The six functions $f_1(x) = x$, $f_2(x) = 1 - x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = \frac{1}{(1-x)}$, $f_5(x) = \frac{(x-1)}{x}$ and $f_6(x) = \frac{x}{(x-1)}$ form a group G under composition. Each function maps the set $\{2, -1, \frac{1}{2}\}$ into itself. By considering how each function permutes these three values, show that G is isomorphic to S_3 . [6]
- 27** Prove that every cyclic group of infinite order is isomorphic to $(\mathbb{Z}, +)$, and that every cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$. [8]
- 28** Let m and n be coprime positive integers. Prove that $(\mathbb{Z}_{mn}, +)$ is isomorphic to $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$, and deduce that $\mathbb{Z}_{15}$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_5$. [8]
- 29** Prove that every abelian group of order 6 is cyclic, and hence isomorphic to $(\mathbb{Z}_6, +)$. You may use the result that a finite group of even order contains an element of order 2, and the result that if commuting elements a, b have coprime orders m, n then ab has order mn . [9]
- 30** An automorphism of a group G is an isomorphism from G to itself. Prove that the automorphisms of $(\mathbb{Z}_n, +)$ are exactly the functions $\varphi_k(x) = kx \pmod{n}$ with $\text{hcf}(k, n) = 1$. Hence write down all the automorphisms of $\mathbb{Z}_{12}$. [8]