

Divisibility and Prime Numbers

1 (3 marks)

$$360 = 2^3 \times 3^2 \times 5$$

M1 A1

$$\text{Number of divisors} = (3 + 1)(2 + 1)(1 + 1) = 24$$

B1

Answer: $2^3 \times 3^2 \times 5$; 24 divisors

3 marks

2 (3 marks)

Digit sum $7 + 2 + 9 + 3 = 21$: divisible by 3 but not by 9

M1 A1

Alternating sum $7 - 2 + 9 - 3 = 11$, so divisible by 11

B1

Answer: 3: yes; 9: no; 11: yes

3 marks

3 (2 marks)

$$391 = 17 \times 23 \quad (17 \times 23 = 340 + 51)$$

M1 A1

Answer: $391 = 17 \times 23$

2 marks

4 (2 marks)

41, 43, 47, 53, 59

B1 B1

Answer: 41, 43, 47, 53, 59

2 marks

5 (3 marks)

$$84 = 2^2 \times 3 \times 7 \text{ and } 126 = 2 \times 3^2 \times 7$$

B1

$$\text{HCF} = 2 \times 3 \times 7 = 42$$

M1

$$\text{LCM} = 2^2 \times 3^2 \times 7 = 252$$

A1

Answer: HCF 42, LCM 252

3 marks

6 (2 marks)

$$n + (n + 1) + (n + 2) = 3n + 3$$

M1

$$= 3(n + 1), \text{ a multiple of 3}$$

A1

Answer: $3(n + 1)$

2 marks

7 (3 marks)

$$n^2 + n = n(n + 1)$$

M1

One of n and $n + 1$ is even

E1

So the product is even

A1

Answer: $n(n + 1)$ is even

3 marks

8 (3 marks)

$$\text{Odd integer} = 2m + 1$$

M1

$$(2m + 1)^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1$$

M1

$$k = m^2 + m \text{ is an integer}$$

A1

Answer: $4(m^2 + m) + 1$

3 marks

9 (4 marks)

$$\text{Number of divisors} = 5 \times 3 \times 2 = 30$$

M1 A1

$$\text{Sum} = (1 + 2 + 4 + 8 + 16)(1 + 3 + 9)(1 + 7)$$

M1

$$= 31 \times 13 \times 8 = 3224$$

A1

Answer: 30 divisors; sum 3224

4 marks

10 (3 marks)

$$1080 = 2^3 \times 3^3 \times 5$$

M1

Each prime must have an even power, so n must contain $2 \times 3 \times 5$

M1

$$n = 30 \text{ (giving } 32400 = 180^2)$$

A1

Answer: 30

3 marks

11 (3 marks)

$b = ap$ and $c = aq$ for integers p, q

M1

$$3b - 5c = 3ap - 5aq = a(3p - 5q)$$

M1

$3p - 5q$ is an integer, so a divides $3b - 5c$

A1

Answer: $a(3p - 5q)$

3 marks

12 (3 marks)

Each zero comes from a factor $10 = 2 \times 5$, and there are far more factors 2 than 5

E1

$$\text{Number of factors 5: } \lfloor 100/5 \rfloor + \lfloor 100/25 \rfloor = 20 + 4$$

M1

$= 24$ zeros

A1

Answer: 24

3 marks

13 (3 marks)

Alternating digit sum: $6 - 4 + d - 8 = d - 6$

M1

$d - 6$ must be a multiple of 11, and $0 \leq d \leq 9$

M1

$$d = 6 \quad (6468 = 11 \times 588)$$

A1

Answer: $d = 6$

3 marks

14 (4 marks)

Let the integers be $n, n + 1, n + 2$

B1

At least one of them is even, so the product is divisible by 2

E1

Exactly one of them is a multiple of 3, so the product is divisible by 3

E1

2 and 3 are coprime, so the product is divisible by 6

E1

Answer: Divisible by 2 and 3, hence by 6

4 marks

15 (5 marks)

$$n(n + 1)(n + 2)(n + 3) + 1$$

B1

$$\text{Pair the factors: } [n(n + 3)][(n + 1)(n + 2)] = (n^2 + 3n)(n^2 + 3n + 2)$$

M1

$$\text{Let } m = n^2 + 3n: \text{ expression} = m(m + 2) + 1$$

M1

$$= m^2 + 2m + 1 = (m + 1)^2$$

M1

$$= (n^2 + 3n + 1)^2, \text{ a perfect square}$$

A1

Answer: $(n^2 + 3n + 1)^2$

5 marks

16 (4 marks)

$$n^4 - 1 = (n^2 - 1)(n^2 + 1)$$

M1

$$n = 2m + 1: n^2 - 1 = 4m(m + 1), \text{ and } m(m + 1) \text{ is even, so } n^2 - 1 = 8k$$

M1 A1

$$n^2 + 1 \text{ is even (odd} + 1), \text{ so the product is divisible by } 8 \times 2 = 16$$

A1

Answer: Divisible by 16

4 marks

17 (4 marks)

$$22^2 = 484 < 523 < 23^2 = 529, \text{ so } \sqrt{523} < 23$$

M1

If 523 were composite it would have a prime factor ≤ 22 : check 2, 3, 5, 7, 11, 13, 17, 19

M1

$523 \div 2, 3, 5$ fail (odd, digit sum 10, ends in 3); remainders on 7, 11, 13, 17, 19 are 5, 6, 3, 13, 10

A1

None divides 523, so 523 is prime

E1

Answer: 523 is prime

4 marks

18 (5 marks)

Assume $\sqrt{3} = \frac{a}{b}$ with a, b integers with no common factor

M1

$$3b^2 = a^2, \text{ so } a^2 \text{ is a multiple of 3}$$

M1

Hence a is a multiple of 3 (as 3 is prime): $a = 3c$

A1

$$3b^2 = 9c^2, \text{ so } b^2 = 3c^2 \text{ and } b \text{ is a multiple of 3}$$

M1

a and b have a common factor 3, a contradiction, so $\sqrt{3}$ is irrational

E1

Answer: Contradiction

5 marks

19 (5 marks)

If $n = p_1^a p_2^b \dots$ the number of divisors is $(a + 1)(b + 1) \dots$

M1

$6 = 6 \times 1$ or 3×2 , so $n = p^5$ or $n = p^2 q$

A1

$p^5 \geq 32 > 30$, so none from this form

B1

$p = 2$: $4q < 30$ gives $q = 3, 5, 7$ so 12, 20, 28; $p = 3$: $9q < 30$ gives $q = 2$ so 18

M1

$p \geq 5$ gives $25q > 30$. So $n = 12, 18, 20, 28$

A1

Answer: 12, 18, 20, 28

5 marks

20 (4 marks)

$7^n - 1 = (7 - 1)(7^{n-1} + 7^{n-2} + \dots + 7 + 1)$

M1 A1

$= 6 \times (\text{an integer})$

M1

Hence divisible by 6

A1

Answer: $6(7^{n-1} + \dots + 1)$

4 marks

21 (6 marks)

$p^2 - 1 = (p - 1)(p + 1)$

M1

p is odd, so $p - 1$ and $p + 1$ are consecutive even numbers, one of which is a multiple of 4:

M1 A1

product divisible by 8

p is not a multiple of 3, so $p - 1$ or $p + 1$ is a multiple of 3 ($p - 1, p, p + 1$ are consecutive)

M1 A1

8 and 3 coprime, so divisible by 24

A1

Answer: Divisible by 24

6 marks

22 (6 marks)

Assume there are finitely many primes $p_1, p_2, \dots, p_k$

M1

Let $N = p_1 p_2 \dots p_k + 1$

M1

N leaves remainder 1 when divided by each p_i , so no p_i divides N

A1

$N > 1$ has a prime factor (or is prime)

M1

That prime is not in the list, a contradiction

A1

Hence there are infinitely many primes

E1

Answer: Contradiction

6 marks

23 (6 marks)

Consider p modulo 3: $p = 3k, 3k + 1$ or $3k + 2$

M1

If $p = 3k + 1$ then $p + 2 = 3k + 3$ is a multiple of 3 (and greater than 3)

M1 A1

If $p = 3k + 2$ then $p + 4 = 3k + 6$ is a multiple of 3 (and greater than 3)

M1 A1

So $p = 3k, p = 3$: 3, 5, 7 are all prime. Only $p = 3$

A1

Answer: $p = 3$

6 marks

24 (6 marks)

$(a - b)(a + b) = 105 = 3 \times 5 \times 7$

M1

$a - b < a + b$, so factor pairs (1,105), (3,35), (5,21), (7,15)

M1 A1

$a = \frac{(F + G)}{2}, b = \frac{(G - F)}{2}$ where F, G are the factors

M1

All factor pairs are odd, so a, b are integers

A1

$(a, b) = (53, 52), (19, 16), (13, 8), (11, 4)$

A1

Answer: (53,52), (19,16), (13,8), (11,4)

6 marks

25 (6 marks)

$n = 1$ to 5 give 43, 47, 53, 61, 71, all prime

B1

Take $n = 40$: $40^2 + 40 + 41 = 1681$

M1 A1

$1681 = 41^2$, which is not prime, so the claim is false

A1

Checking a finite number of cases cannot prove a statement for all n

E1

One counterexample is enough to disprove a general claim

E1

Answer: $n = 40$ gives 41^2

6 marks

26 (6 marks)

If $n = p^2$ the divisors are 1, p , p^2 : exactly three

B1

Conversely, let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

M1

Number of divisors $= (a_1 + 1)(a_2 + 1) \dots (a_k + 1) = 3$

M1

3 is prime, so exactly one factor is 3 and the rest are 1 (no other primes appear)

A1

So $k = 1$ and $a_1 + 1 = 3$, giving $a_1 = 2$

M1

$n = p^2$ with p prime

A1

Answer: $n = p^2$

6 marks

27 (8 marks)

$n^5 - n = n(n^2 - 1)(n^2 + 1) = (n - 1)n(n + 1)(n^2 + 1)$

M1 A1

Three consecutive integers: divisible by 2 and by 3, hence by 6

M1 A1

Divisibility by 5: consider $n = 5k$, $5k \pm 1$, $5k \pm 2$

M1

$n = 5k$, $5k + 1$, $5k - 1$: n , $n - 1$ or $n + 1$ is a multiple of 5

A1

$n = 5k \pm 2$: $n^2 = 25k^2 \pm 20k + 4$, so $n^2 + 1 = 5(\dots)$ is a multiple of 5

M1

5 and 6 coprime, so divisible by 30

A1

Answer: Divisible by 30

8 marks

28 (8 marks)

(a) Suppose n is not prime: $n = ab$ with $a, b > 1$

M1

$2^n - 1 = (2^a)^b - 1$

M1

Let $x = 2^a$: $x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \dots + 1)$

M1 A1

$x - 1 = 2^a - 1 > 1$ as $a > 1$, and the other factor > 1 as $b > 1$

M1

So $2^n - 1$ is composite; hence if $2^n - 1$ is prime then n is prime

A1

Answer: Proved

6 marks

(b) $2^{11} - 1 = 2047$

M1

$2047 = 23 \times 89$, so it is composite

A1

Answer: $2047 = 23 \times 89$

2 marks

29 (9 marks)

Try to factorise: $n^4 + 4 = (n^2 + 2)^2 - 4n^2$

M1 A1

$= (n^2 + 2 - 2n)(n^2 + 2 + 2n)$

M1 A1

$= (n^2 - 2n + 2)(n^2 + 2n + 2)$

A1

Second factor $n^2 + 2n + 2 > 1$ for all $n \geq 1$

B1

For a prime, the first factor must equal 1: $n^2 - 2n + 1 = 0$

M1

$(n - 1)^2 = 0$, so $n = 1$

A1

Check: $1 + 4 = 5$, which is prime. Only $n = 1$

A1

Answer: $n = 1$ only

9 marks

30 (9 marks)

(a) Squares are 0 or 1 modulo 4: $(2m)^2 = 4m^2$, $(2m + 1)^2 = 4(m^2 + m) + 1$

M1 A1

Sum of two squares is therefore 0 + 0, 0 + 1 or 1 + 1, i.e. 0, 1 or 2 modulo 4

M1 A1

Never 3 modulo 4, so $4k + 3$ is not a sum of two squares

E1

Answer: Squares are 0 or 1 mod 4

5 marks

(b) $2023 = 4 \times 505 + 3$, so it is of the form $4k + 3$

M1 A1

Not a sum of two squares by (a)

E1

$2029 = 45^2 + 2^2$ ($2025 + 4$)

B1

Answer: $2023 = 4 \times 505 + 3$; $a = 45$, $b = 2$

4 marks

Euclidean Algorithm

1 (3 marks)

$$252 = 2 \times 105 + 42$$

M1

$$105 = 2 \times 42 + 21$$

A1

$$42 = 2 \times 21 + 0, \text{ so the HCF is } 21$$

A1

Answer: 21

3 marks

2 (3 marks)

$$221 = 1 \times 119 + 102$$

M1

$$119 = 1 \times 102 + 17$$

A1

$$102 = 6 \times 17 + 0, \text{ so the HCF is } 17$$

A1

Answer: 17

3 marks

3 (2 marks)

$$37 \times 27 = 999$$

M1

$$1000 = 37 \times 27 + 1: \text{ quotient } 27, \text{ remainder } 1$$

A1

Answer: Quotient 27, remainder 1

2 marks

4 (3 marks)

$$144 = 1 \times 91 + 53, 91 = 1 \times 53 + 38$$

M1

$$53 = 1 \times 38 + 15, 38 = 2 \times 15 + 8, 15 = 1 \times 8 + 7, 8 = 1 \times 7 + 1$$

A1

$$\text{HCF} = 1, \text{ so they are coprime}$$

A1

Answer: Coprime

3 marks

5 (2 marks)

$$\text{HCF} \times \text{LCM} = 18 \times 24 = 432$$

M1

$$\text{LCM} = 432 \div 6 = 72$$

A1

Answer: 72

2 marks

6 (2 marks)

$$n \text{ is a multiple of } 12 \text{ in the range: } 60$$

M1

$$\text{gcd}(48, 60) = 12, \text{ so } n = 60$$

A1

Answer: 60

2 marks

7 (3 marks)

$$2415 = 1 \times 1449 + 966$$

M1

$$1449 = 1 \times 966 + 483; 966 = 2 \times 483 + 0$$

A1

$$\text{The last non-zero remainder is } 483, \text{ so the HCF is } 483$$

A1

Answer: 483

3 marks

8 (4 marks)

$$5593 = 2 \times 2431 + 731; 2431 = 3 \times 731 + 238$$

M1 A1

$$731 = 3 \times 238 + 17; 238 = 14 \times 17 + 0$$

M1

$$\text{The last non-zero remainder is } 17, \text{ so the HCF is } 17$$

A1

Answer: 17

4 marks

9 (4 marks)

$$35 = 2 \times 12 + 11, 12 = 1 \times 11 + 1, \text{ so HCF} = 1$$

M1 A1

$$1 = 12 - 11 = 12 - (35 - 2 \times 12)$$

M1

$$1 = 3 \times 12 - 35, \text{ so } x = -1, y = 3$$

A1

Answer: $x = -1, y = 3$

4 marks

10 (4 marks)

$$91 = 2 \times 35 + 21, 35 = 1 \times 21 + 14, 21 = 1 \times 14 + 7$$

M1 A1

$$7 = 21 - 14 = 21 - (35 - 21) = 2 \times 21 - 35$$

M1

$$= 2(91 - 2 \times 35) - 35 = 2 \times 91 - 5 \times 35, \text{ so } x = 2, y = -5$$

A1

Answer: $x = 2, y = -5$

4 marks

11 (4 marks)

$$1989 = 1 \times 1547 + 442; 1547 = 3 \times 442 + 221; 442 = 2 \times 221 + 0$$

M1 A1

$$\text{HCF} = 221$$

A1

$$\text{LCM} = \frac{1989 \times 1547}{221} = 9 \times 1547 = 13923$$

A1

Answer: HCF 221, LCM 13923

4 marks

12 (3 marks)Let the integers be n and $n + 1$: $n + 1 = 1 \times n + 1$

M1

The remainder is 1, so Euclid's algorithm gives $\text{hcf}(n + 1, n) = \text{hcf}(n, 1) = 1$

M1 A1

Answer: hcf = 1

3 marks

13 (3 marks)Remainder r ($r < 13$), quotient $2r$: $N = 13(2r) + r = 27r$

M1

$$40 < 27r < 60 \text{ gives } r = 2$$

M1

$$N = 54 \text{ (check: } 54 = 13 \times 4 + 2 \text{)}$$

A1

Answer: 54

3 marks

14 (5 marks)

$$341 = 2 \times 154 + 33; 154 = 4 \times 33 + 22$$

M1 A1

$$33 = 1 \times 22 + 11 \text{ and } 22 = 2 \times 11 + 0, \text{ so } h = 11$$

A1

$$11 = 33 - 22 = 33 - (154 - 4 \times 33) = 5 \times 33 - 154$$

M1

$$= 5(341 - 2 \times 154) - 154 = 5 \times 341 - 11 \times 154, \text{ so } x = 5, y = -11$$

A1

Answer: $h = 11, x = 5, y = -11$

5 marks

15 (5 marks)

$$(a) 233 = 1 \times 144 + 89, 144 = 1 \times 89 + 55, 89 = 1 \times 55 + 34$$

M1 A1

$$55 = 1 \times 34 + 21, 34 = 1 \times 21 + 13, \dots, 3 = 1 \times 2 + 1, \text{ so } \text{HCF} = 1$$

A1

Answer: 1

3 marks

$$(b) \text{hcf}(F_{n+1}, F_n) = \text{hcf}(F_n, F_{n+1} - F_n) = \text{hcf}(F_n, F_{n-1})$$

M1

$$\text{Repeating gives } \text{hcf}(F_2, F_1) = \text{hcf}(1, 1) = 1$$

A1

Answer: hcf = 1

2 marks

16 (4 marks)Let $d = \text{hcf}(a, b)$: d divides a and b , so d divides $r = a - bq$

M1 A1

So d is a common divisor of b and r , hence $d \leq \text{hcf}(b, r)$

M1

A common divisor of b and r divides $a = bq + r$, so $\text{hcf}(b, r) \leq \text{hcf}(a, b)$; they are equal

A1

Answer: Proved

4 marks

17 (5 marks)

$$12 \text{ divides } x: x = 12k, k = 1, \dots, 8$$

M1 A1

$$84 = 12 \times 7, \text{ so } \text{hcf}(12k, 84) = 12 \times \text{hcf}(k, 7)$$

M1

Need $\text{hcf}(k, 7) = 1$, i.e. k is not a multiple of 7, so $k \neq 7$

A1

$$x = 12, 24, 36, 48, 60, 72, 96$$

A1

Answer: 12, 24, 36, 48, 60, 72, 96

5 marks

18 (5 marks)

$$43 = 2 \times 17 + 9; 17 = 1 \times 9 + 8; 9 = 1 \times 8 + 1$$

M1 A1

$$1 = 9 - 8 = 9 - (17 - 9) = 2 \times 9 - 17$$

M1

$$= 2(43 - 2 \times 17) - 17 = 2 \times 43 - 5 \times 17$$

A1

$$-5 \times 17 \equiv 1, \text{ so } x = 43 - 5 = 38 \text{ (check: } 17 \times 38 = 646 = 15 \times 43 + 1 \text{)}$$

A1

Answer: $x = 38$

5 marks

19 (4 marks)

$$\text{hcf}(504, 360): 504 = 1 \times 360 + 144; 360 = 2 \times 144 + 72; 144 = 2 \times 72$$

M1 A1

$$\text{hcf} = 72$$

A1

$$\text{hcf}(1260, 72): 1260 = 17 \times 72 + 36; 72 = 2 \times 36, \text{ so overall HCF} = 36$$

A1

Answer: 36

4 marks

20 (4 marks)

Let $h = \text{hcf}(15n + 4, 10n + 3)$: h divides $(15n + 4) - (10n + 3) = 5n + 1$

M1 A1

h divides $(10n + 3) - 2(5n + 1) = 1$

M1

So $h = 1$: coprime

A1

Answer: $\text{hcf} = 1$

4 marks

21 (6 marks)

Let $h = \text{hcf}(a + b, a - b)$

B1

h divides the sum $2a$ and the difference $2b$

M1 A1

So h divides $\text{hcf}(2a, 2b) = 2 \text{hcf}(a, b)$

M1

$= 2$ since $\text{hcf}(a, b) = 1$

A1

h divides 2, so $h = 1$ or 2

A1

Answer: 1 or 2

6 marks

22 (6 marks)

$\text{hcf}(a, b) = 1$, so there are integers x, y with $ax + by = 1$ (Euclid's algorithm in reverse)

M1 A1

Multiply by c : $acx + bcy = c$

M1

a divides acx , and a divides bc so a divides bcy

M1 A1

Hence a divides the sum c

A1

Answer: a divides c

6 marks

23 (7 marks)

(a) $221 = 1 \times 143 + 78$; $143 = 1 \times 78 + 65$; $78 = 1 \times 65 + 13$; $65 = 5 \times 13$

M1

$h = 13$

A1

Answer: 13

2 marks

(b) $13 = 78 - 65 = 78 - (143 - 78) = 2 \times 78 - 143$

M1

$= 2(221 - 143) - 143 = 2 \times 221 - 3 \times 143$

M1

$x = -3, y = 2$

A1

Answer: $x = -3, y = 2$

3 marks

(c) Multiply (b) by 3: $143 \times (-9) + 221 \times 6 = 39$

M1

$p = -9, q = 6$

A1

Answer: $p = -9, q = 6$

2 marks

24 (6 marks)

$2^{12} - 1 = 4095$ and $2^{18} - 1 = 262143$

B1

$262143 = 64 \times 4095 + 63$

M1 A1

$4095 = 65 \times 63 + 0$

M1

HCF = 63

A1

$\text{hcf}(12, 18) = 6$ and $2^6 - 1 = 63$

B1

Answer: $63 = 2^6 - 1$

6 marks

25 (6 marks)

$n^2 + 1 = (n + 1)(n - 1) + 2$

M1 A1

$\text{hcf}(n^2 + 1, n + 1) = \text{hcf}(n + 1, 2)$

M1 A1

If n is odd, $n + 1$ is even so the hcf is 2

A1

If n is even, $n + 1$ is odd so the hcf is 1

A1

Answer: 2 if n odd; 1 if n even

6 marks

26 (6 marks)

(a) The HCF is the last non-zero remainder (1), not the divisor 7 in the step before it

E1

Answer: Last non-zero remainder is 1

1 mark

(b) HCF = 1

B1

Answer: 1

1 mark

(c) $1 = 8 - 7 = 8 - (175 - 21 \times 8) = 22 \times 8 - 175$

M1

$= 22(533 - 3 \times 175) - 175 = 22 \times 533 - 67 \times 175$

M1

$= 22 \times 533 - 67(1241 - 2 \times 533) = 156 \times 533 - 67 \times 1241$

M1

$$x = -67, y = 156$$

Answer: $x = -67, y = 156$

A1

4 marks

27 (8 marks)

Let $d = \text{hcf}(a, b)$, $a = dm$, $b = dn$, with $\text{hcf}(m, n) = 1$

M1 A1

Let $L = dmn$. Then $L = a n = b m$ is a common multiple of a and b

M1 A1

Let C be any common multiple: $C = ax = dm x$ and $C = by = dn y$

M1

$mx = ny$, and m, n coprime so n divides x (previous result)

M1

$x = nk$: $C = dm nk = kL$, so L divides every common multiple, hence $L = \text{lcm}$

A1

$\text{hcf} \times \text{lcm} = d \times dm n = (dm)(dn) = ab$

A1

Answer: Proved

8 marks

28 (9 marks)

$$2^a - 1 = 2^b(2^{a-b} - 1) + (2^b - 1)$$

M1 A1

So $\text{hcf}(2^a - 1, 2^b - 1) = \text{hcf}(2^b(2^{a-b} - 1), 2^b - 1)$ (subtracting a multiple)

M1

2^b and $2^b - 1$ are coprime (consecutive integers), so the factor 2^b can be dropped

M1 A1

hence $= \text{hcf}(2^{a-b} - 1, 2^b - 1)$

A1

The exponents (a, b) change to $(a - b, b)$: the same subtraction steps as Euclid's algorithm on a and b

M1 A1

The process ends with exponents (h, h) where $h = \text{hcf}(a, b)$, giving $2^h - 1$

A1

Answer: $2^{\text{hcf}(a, b)} - 1$

9 marks

29 (8 marks)

$a = 6m$, $b = 6n$ with $\text{hcf}(m, n) = 1$ and $m < n$

M1 A1

$$\text{lcm} = 6mn = 180$$

M1

$$mn = 30$$

A1

Factor pairs of 30: $(1, 30), (2, 15), (3, 10), (5, 6)$

M1 A1

All four pairs are coprime

B1

$(a, b) = (6, 180), (12, 90), (18, 60), (30, 36)$

A1

Answer: $(6, 180), (12, 90), (18, 60), (30, 36)$

8 marks

30 (8 marks)

Let $h = \text{hcf}(n! + 1, (n + 1)! + 1)$

B1

$$(n + 1)! + 1 = (n + 1)n! + 1 = (n + 1)(n! + 1) - n$$

M1 A1

h divides $(n + 1)(n! + 1)$, so h divides n

M1 A1

n divides $n!$, so h divides $n!$

M1

h divides $n! + 1$ and $n!$, so h divides 1

A1

$$h = 1$$

A1

Answer: $\text{hcf} = 1$

8 marks

Modular Arithmetic

1 (2 marks)

$$7 \times 17 = 119$$

M1

$$123 - 119 = 4, \text{ so } x = 4$$

A1

Answer: 4

2 marks

2 (3 marks)

$$47 \equiv 2 \text{ and } 58 \equiv 4 \pmod{9}$$

M1 A1

$$47 \times 58 \equiv 2 \times 4 = 8 \pmod{9}, \text{ so the remainder is } 8$$

A1

Answer: 8

3 marks

3 (2 marks)

$$x = 5k + 3 \text{ for integer } k$$

M1

$$13, 18, 23, 28$$

A1

Answer: 13, 18, 23, 28

2 marks

4 (2 marks)

$$2^5 = 32 \equiv -1 \pmod{11} \quad (32 = 33 - 1)$$

M1

$$2^{10} = (2^5)^2 \equiv (-1)^2 = 1 \pmod{11}$$

A1

$$\text{Answer: } 2^{10} = 1024 = 93 \times 11 + 1$$

2 marks

5 (2 marks)

$$8 + 9 = 17 \equiv 6$$

B1

$$8 \times 9 = 72 = 66 + 6 \equiv 6$$

B1

Answer: Both are 6

2 marks

6 (2 marks)

$$x \equiv 3 - 7 = -4$$

M1

$$x \equiv 7 \pmod{11}$$

A1

Answer: $x = 7$

2 marks

7 (3 marks)

$$5 \times 5 = 25 \equiv 1 \pmod{8}, \text{ so } 5 \text{ is its own inverse}$$

M1

$$x \equiv 5 \times 3 = 15 \equiv 7 \pmod{8}$$

A1

$$\text{Check: } 5 \times 7 = 35 = 32 + 3$$

B1

Answer: $x \equiv 7 \pmod{8}$

3 marks

8 (3 marks)

$$3^6 = 729 \equiv 1 \pmod{7}$$

M1

$$3^{100} = (3^6)^{16} \times 3^4 \equiv 3^4 = 81$$

M1

$$81 = 77 + 4, \text{ so the remainder is } 4$$

A1

Answer: 4

3 marks

9 (3 marks)

Powers of 7 end in 7, 9, 3, 1 and then repeat with period 4

M1

$$2023 = 4 \times 505 + 3$$

M1

The last digit is the third in the cycle: 3

A1

Answer: 3

3 marks

10 (3 marks)

Every integer is 0, 1 or 2 modulo 3

B1

$$\text{Squares: } 0^2 = 0, 1^2 = 1, 2^2 = 4 \equiv 1 \pmod{3}$$

M1

A square is 0 or 1 modulo 3, never 2

A1

Answer: Squares are 0 or 1 (mod 3)

3 marks

11 (4 marks)

$$26 = 3 \times 7 + 5, 7 = 1 \times 5 + 2, 5 = 2 \times 2 + 1; 1 = 5 - 2 \times 2 = 3 \times 5 - 2 \times 7 = 3 \times 26 - 11 \times 7$$

M1 A1

$$\text{Inverse of } 7 \text{ is } -11 \equiv 15 \text{ (check } 7 \times 15 = 105 = 4 \times 26 + 1)$$

A1

$$x \equiv 15 \times 5 = 75 \equiv 23 \pmod{26}$$

A1

Answer: inverse 15; $x \equiv 23 \pmod{26}$

4 marks

12 (4 marks)

$$10 \equiv 1 \pmod{9}, \text{ so } 10^n \equiv 1^n = 1$$

M1 A1

$$N = a_k 10^k + \dots + a_1 10 + a_0 \equiv a_k + \dots + a_1 + a_0 \pmod{9}$$

M1

So $N \equiv \text{digit sum} \pmod{9}$; $N \equiv 0$ exactly when the digit sum $\equiv 0$

A1

Answer: $N \equiv \text{digit sum} \pmod{9}$

4 marks

13 (3 marks)

Squares modulo 7 for $x = 0, 1, \dots, 6$ are 0, 1, 4, 2, 2, 4, 1

M1 A1

$$x = 3 \text{ and } x = 4$$

A1

Answer: $x = 3, 4$

3 marks

14 (5 marks)

$\text{hcf}(14, 35) = 7$ and 7 divides 21, so there are solutions

M1 A1

Divide through by 7, including the modulus: $2x \equiv 3 \pmod{5}$

M1

$$2 \times 3 = 6 \equiv 1, \text{ so } x \equiv 3 \times 3 = 9 \equiv 4 \pmod{5}$$

A1

$$x = 4, 9, 14, 19, 24, 29, 34$$

A1

Answer: $x = 4, 9, 14, 19, 24, 29, 34$

5 marks

15 (4 marks)

If p is prime and p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$

B1

$$2^{12} \equiv 1 \pmod{13}$$

M1

$$2^{100} = (2^{12})^8 \times 2^4 \equiv 16$$

M1

$$16 \equiv 3, \text{ so the remainder is } 3$$

A1

Answer: 3

4 marks

16 (5 marks)

$N \equiv 2 \pmod{3}$ and $N \equiv 2 \pmod{7}$ gives $N \equiv 2 \pmod{21}$: $N = 21k + 2$

M1 A1

$21k + 2 \equiv 3 \pmod{5}$, so $k + 2 \equiv 3$, $k \equiv 1 \pmod{5}$

M1 A1

$N = 21 + 2 = 23$ (check: $23 = 7 \times 3 + 2$, $23 = 4 \times 5 + 3$, $23 = 3 \times 7 + 2$)

A1

Answer: 23

5 marks

17 (4 marks)

The last two digits are the remainder modulo 100

B1

$$7^2 = 49, 7^4 = 2401 \equiv 1 \pmod{100}$$

M1 A1

$$7^{2024} = (7^4)^{506} \equiv 1, \text{ so the last two digits are } 01$$

A1

Answer: 01

4 marks

18 (5 marks)

$$2^{12} \equiv 1 \pmod{13} \text{ by Fermat, so } 2^{50} = (2^{12})^4 \times 2^2 \equiv 4$$

M1 A1

$$3^3 = 27 \equiv 1 \pmod{13}$$

M1

$$3^{50} = (3^3)^{16} \times 3^2 \equiv 9$$

A1

$$2^{50} + 3^{50} \equiv 4 + 9 = 13 \equiv 0 \pmod{13}$$

A1

Answer: Remainder 0

5 marks

19 (5 marks)

From the second: $x \equiv 3 - 4y \pmod{7}$

M1

Substitute: $3(3 - 4y) + 2y = 9 - 10y \equiv 1$, so $-10y \equiv -8$, i.e. $10y \equiv 8$, i.e. $3y \equiv 1 \pmod{7}$

M1 A1

$$3 \times 5 = 15 \equiv 1, \text{ so } y \equiv 5 \pmod{7}$$

A1

$$x \equiv 3 - 20 = -17 \equiv 4 \pmod{7}. \text{ So } x = 4, y = 5$$

A1

Answer: $x = 4, y = 5$

5 marks

20 (5 marks)

Squares modulo 3 are 0 (for multiples of 3) and 1 (otherwise)

M1 A1

Possible values of $x^2 + y^2$ modulo 3: $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, $1 + 1 = 2$

M1 A1

Only $0 + 0$ gives 0, so x and y are both multiples of 3

E1

Answer: Proved

5 marks

21 (6 marks)

(a) $6! = 720$

M1

$$720 = 7 \times 103 - 1 \equiv -1 \pmod{7}$$

A1

Answer: $6! = 720 \equiv -1$

2 marks

(b) $22! = 22 \times 21 \times 20! \equiv -1 \pmod{23}$

M1

$$22 \equiv -1 \text{ and } 21 \equiv -2, \text{ so } 22 \times 21 \equiv 2$$

M1

$$2 \times 20! \equiv -1 \equiv 22, \text{ so } 20! \equiv 11 \pmod{23} \text{ (dividing by 2 is valid since 2 is invertible)}$$

M1 A1

Answer: 11

4 marks

22 (6 marks)**(a)** $3^1, 3^2, \dots, 3^6 \equiv 3, 2, 6, 4, 5, 1 \pmod{7}$

M1

First 1 at $k = 6$, so the order is 6

A1

Answer: 6

2 marks

(b) $2^1, 2^2, 2^3 \equiv 2, 4, 1 \pmod{7}$

M1

The order is 3

A1

Answer: 3

2 marks

(c) Powers of 3 give 3, 2, 6, 4, 5, 1: all six non-zero residues

B1

Powers of 2 give only 2, 4, 1; 3 is never obtained

B1

Answer: Powers of 3 give all; powers of 2 give 1, 2, 4 only

2 marks

23 (6 marks)Squares modulo 8: $0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2 \equiv 0, 1, 4, 1, 0, 1, 4, 1$

M1 A1

So every square is 0, 1 or 4 (mod 8)

A1

Sums of three values from $\{0, 1, 4\}$ give 0, 1, 2, 3, 4, 5, 6 (mod 8), for example $4 + 1 + 1 = 6$ and $4 + 4 + 0 = 0$

M1 A1

7 is never obtained, so $8k + 7$ is not a sum of three squares

E1

Answer: Squares are 0, 1, 4 (mod 8)

6 marks

24 (6 marks)Test $x = 0, \dots, 12$: values of $x^2 + x + 1$ are 1, 3, 7, 13, 21, 31, 43, 57, 73, 91, 111, 133, 157

M1 A1

13 and 91 = 7×13 are multiples of 13: $x = 3$ and $x = 9$

A1

Modulo 11 the values for $x = 0, \dots, 10$ are 1, 3, 7, 2, 10, 9, 10, 2, 7, 3, 1 (using $x^2 + x + 1 \pmod{11}$)

M1 A1

None is 0, so there are no solutions

A1

Answer: $x = 3$ and $x = 9$; none mod 11

6 marks

25 (6 marks)**(a)** Dividing a congruence by 3 requires the modulus to be divided by $\text{hcf}(3, 15) = 3$ as well

E1

Dividing without changing the modulus loses solutions: the congruence has 3 solutions, not 1

E1

Answer: The modulus must also be divided by 3

2 marks

(b) $\text{hcf}(6, 15) = 3$ divides 9, so there are 3 solutions modulo 15

M1 A1

Dividing by 3: $2x \equiv 3 \pmod{5}$, so $x \equiv 3 \times 3 = 9 \equiv 4 \pmod{5}$

M1

 $x = 4, 9, 14$

A1

Answer: $x = 4, 9, 14$

4 marks

26 (6 marks)**(a)** Work modulo 7: $3^6 \equiv 1$ ($3^6 = 729 = 104 \times 7 + 1$)

M1

 $3^{50} = (3^6)^8 \times 3^2 \equiv 9 \equiv 2 \pmod{7}$

M1

Thursday + 2 days is Saturday

A1

Answer: Saturday

3 marks

(b) Need $3^n \equiv 0 \pmod{7}$, but 3^n is never a multiple of 7 (7 is prime and does not divide 3)

M1 A1

So there is no such n

A1

Answer: No such n

3 marks

27 (8 marks)Consider the $p - 1$ numbers $a, 2a, 3a, \dots, (p - 1)a$

B1

None is divisible by p , as p divides neither a nor any of $1, \dots, p - 1$ (p is prime)

M1 A1

If $ia \equiv ja \pmod{p}$ with $1 \leq i < j \leq p - 1$ then p divides $(j - i)a$; impossible as p divides neither factor, so the residues are distinct

M1 A1

So they are a rearrangement of $1, 2, \dots, p - 1$ modulo p

A1

Multiply: $a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}$

M1

 $(p - 1)!$ is coprime to p , so cancel: $a^{p-1} \equiv 1$

A1

Answer: Proved

8 marks

28 (8 marks)

$N = 5a + 2$ and $N \equiv 3 \pmod{7}$: $5a + 2 \equiv 3$, so $5a \equiv 1 \pmod{7}$ M1 A1
 $5 \times 3 = 15 \equiv 1$, so $a \equiv 3 \pmod{7}$: $N \equiv 17 \pmod{35}$ M1 A1
 $N = 17 + 35m$: $17 + 35m \equiv 4 \pmod{9}$, i.e. $8 + 8m \equiv 4$ M1
 $8m \equiv -4 \equiv 5 \pmod{9}$; $8 \times 8 = 64 \equiv 1$, so $m \equiv 40 \equiv 4 \pmod{9}$ M1 A1
 $N \equiv 17 + 140 = 157 \pmod{315}$; 5, 7, 9 are pairwise coprime so solutions repeat every 315, and 157 is the smallest positive one A1
Answer: 157 8 marks

29 (8 marks)

2^n modulo 7 has period 3: 2, 4, 1, 2, 4, 1, ... M1 A1
 3^n modulo 7 has period 6: 3, 2, 6, 4, 5, 1, ... M1 A1
Both repeat every 6, so consider $n = 1, \dots, 6$: sums 5, 6, 0, 6, 9 $\equiv 2, 2$ M1 A1
Only $n = 3$ gives 0 A1
So 7 divides $2^n + 3^n$ exactly when $n \equiv 3 \pmod{6}$, i.e. $n = 6k + 3$ A1
Answer: $n \equiv 3 \pmod{6}$ 8 marks

30 (9 marks)

Suppose p does not divide b . Then b has an inverse c modulo p M1
 $a^2 + b^2 \equiv 0$, so $(ac)^2 \equiv -(bc)^2 \equiv -1 \pmod{p}$. Let $t = ac$ M1 A1
Then $t^2 \equiv -1$, so $t^{4k+2} = (t^2)^{2k+1} \equiv (-1)^{2k+1} = -1$ M1 A1
 p does not divide t (else $t^2 \equiv 0$), so Fermat gives $t^{p-1} = t^{4k+2} \equiv 1$ M1 A1
Hence $1 \equiv -1 \pmod{p}$, so p divides 2, impossible as $p \geq 3$ A1
So p divides b ; then p divides a^2 , so p divides a A1
Answer: Proved 9 marks

Diophantine Equations

1 (2 marks)

Try $x = 2$: $6 + 5y = 1$ gives $y = -1$ M1
 $x = 2, y = -1$ ($6 - 5 = 1$) A1
Answer: $x = 2, y = -1$ 2 marks

2 (2 marks)

$6x + 9y = 3(2x + 3y)$ is a multiple of 3 M1
20 is not a multiple of 3, so there are no integer solutions E1
Answer: $\text{hcf}(6, 9) = 3$ does not divide 20 2 marks

3 (2 marks)

$\text{hcf}(4, 6) = 2$ divides 10, so integer solutions exist M1
 $x = 1, y = 1$ ($4 + 6 = 10$) A1
Answer: $x = 1, y = 1$ 2 marks

4 (2 marks)

$x = 10 - 3y$ requires $y = 1, 2, 3$ for $x > 0$ M1
 $(x, y) = (7, 1), (4, 2), (1, 3)$ A1
Answer: (7,1), (4,2), (1,3) 2 marks

5 (2 marks)

Adjust by multiples of (7, -5) M1
 $x = 3 + 7t, y = -2 - 5t$, t an integer A1
Answer: $x = 3 + 7t, y = -2 - 5t$ 2 marks

6 (2 marks)

$2x + 4y = 2(x + 2y)$ is even for integers x and y

M1

7 is odd, so there are no solutions

E1

Answer: LHS even, RHS odd

2 marks

7 (3 marks)

By inspection $x = -1$, $y = 2$ works ($-3 + 8 = 5$)

M1

Other solutions differ by multiples of $(4, -3)$

M1

$x = -1 + 4t$, $y = 2 - 3t$

A1

Answer: $x = -1 + 4t$, $y = 2 - 3t$

3 marks

8 (4 marks)

$17 = 1 \times 13 + 4$, $13 = 3 \times 4 + 1$

M1 A1

$1 = 13 - 3 \times 4 = 13 - 3(17 - 13) = 4 \times 13 - 3 \times 17$

M1

$x = -3 + 13t$, $y = 4 - 17t$

A1

Answer: $x = -3 + 13t$, $y = 4 - 17t$

4 marks

9 (4 marks)

$5x + 8y = 53$, so $8y \leq 53$ and $y \leq 6$

M1

$53 - 8y$ must be a multiple of 5: $y = 1$ gives 45, $y = 6$ gives 5 ($y = 2, 3, 4, 5$ give 37, 29, 21, 13;

M1 A1

$y = 0$ gives 53)

9 five-pence and 1 eight-pence stamp, or 1 five-pence and 6 eight-pence stamps

A1

Answer: (9, 1) or (1, 6)

4 marks

10 (3 marks)

Divide by 6: $2x + 3y = 5$

M1

$x, y \geq 1$ means $2x + 3y \geq 5$, with equality only when $x = y = 1$

M1

The only solution is $x = 1$, $y = 1$

A1

Answer: $x = 1$, $y = 1$

3 marks

11 (4 marks)

$\text{hcf}(14, 21) = 7$; 7 does not divide 100, so (i) has no solutions

M1 A1

7 divides 105, so (ii) has solutions; divide by 7: $2x + 3y = 15$

M1

$x = 0$, $y = 5$ works, so $x = 3t$, $y = 5 - 2t$

A1

Answer: (i) none; (ii) $x = 3t$, $y = 5 - 2t$

4 marks

12 (4 marks)

$20x + 50y = 230$, so $2x + 5y = 23$

M1

y must be odd ($23 - 5y$ even) with $5y \leq 23$: $y = 1, 3$

M1 A1

$y = 1$, $x = 9$; $y = 3$, $x = 4$. Two ways

A1

Answer: 2 ways: (9, 1) and (4, 3)

4 marks

13 (3 marks)

$(x - y)(x + y) = 21 = 1 \times 21 = 3 \times 7$

M1

$x - y = 1$, $x + y = 21$: $x = 11$, $y = 10$; $x - y = 3$, $x + y = 7$: $x = 5$, $y = 2$

M1 A1

Answer: (11, 10), (5, 2)

3 marks

14 (5 marks)

$37 = 1 \times 23 + 14$, $23 = 1 \times 14 + 9$, $14 = 1 \times 9 + 5$, $9 = 1 \times 5 + 4$, $5 = 1 \times 4 + 1$

M1 A1

Back-substitute: $1 = 5 - 4 = 2 \times 5 - 9 = 2 \times 14 - 3 \times 9 = 5 \times 14 - 3 \times 23 = 5 \times 37 - 8 \times 23$

M1

$x = -8 + 37t$, $y = 5 - 23t$

A1

$t = 1$: $x = 29$, $y = -18$ (check $667 - 666 = 1$)

A1

Answer: $x = -8 + 37t$, $y = 5 - 23t$; (29, -18)

5 marks

15 (5 marks)Divide by 3: $5x + 7y = 3$

M1

 $x = 2, y = -1$ is a solution ($10 - 7 = 3$)

M1 A1

General solution: $x = 2 + 7t, y = -1 - 5t$

A1

 $t = -1: x = -5, y = 4$

A1

Answer: $x = 2 + 7t, y = -1 - 5t; (-5, 4)$

5 marks

16 (5 marks) $7 = 3a + 5b: b = 0$ gives $7/3, b = 1$ gives $2/3$; neither is a non-negative integer, so $7p$ is impossible

M1 A1

 $8 = 3 + 5, 9 = 3 \times 3, 10 = 5 \times 2$

B1

Any $n \geq 8$ is one of these plus a multiple of 3: $n = (8, 9 \text{ or } 10) + 3k$

M1

Adding $3p$ coins keeps the payment exact, so all $n \geq 8$ can be paid

A1

Answer: 7 impossible; all $n \geq 8$ possible

5 marks

17 (4 marks) $x^2 \leq 124$ so $x \leq 11$. Test $x = 1, \dots, 11: 125 - x^2 = 124, 121, 116, 109, 100, 89, 76, 61, 44, 25, 4$

M1 A1

Perfect squares: $x = 2$ (121), $x = 5$ (100), $x = 10$ (25), $x = 11$ (4)

M1

(2, 11), (5, 10), (10, 5), (11, 2)

A1

Answer: (2,11), (5,10), (10,5), (11,2)

4 marks

18 (4 marks)Work modulo 5: $x^2 - 5y^2 \equiv x^2$

M1

So $x^2 \equiv 3 \pmod{5}$

A1

Squares modulo 5 are 0, 1, 4, 4, 1 (for $x = 0, \dots, 4$), never 3

M1

Hence no integer solutions

A1

Answer: Squares mod 5 are 0, 1, 4

4 marks

19 (5 marks)Subtract $2 \times$ (first) from the second: $y + 3z = 8$

M1 A1

 $z = 1: y = 5; z = 2: y = 2; z \geq 3$ gives $y \leq -1$ (not positive)

M1 A1

 $x = 10 - y - z: (x, y, z) = (4, 5, 1)$ and $(6, 2, 2)$

A1

Answer: (4, 5, 1), (6, 2, 2)

5 marks

20 (5 marks) $13x \equiv 300 \pmod{8}: 5x \equiv 4 \pmod{8}$

M1 A1

 $5 \times 5 = 25 \equiv 1$, so $x \equiv 20 \equiv 4 \pmod{8}$

M1

 $x = 4, 12, 20$ ($13x \leq 300$ gives $x \leq 23$)

A1

 $y = 31, 18, 5: (4, 31), (12, 18), (20, 5)$

A1

Answer: (4, 31), (12, 18), (20, 5)

5 marks

21 (6 marks) $m^2 + n^2 = 65$ with $m > n$

M1

Test $n = 1, \dots, 5: 65 - n^2 = 64, 61, 56, 49, 40$, so m^2 perfect square for $n = 1$ ($m = 8$) and $n = 4$ ($m = 7$)

M1 A1

(8, 1): coprime, opposite parity; (7, 4): coprime, opposite parity

M1

(8, 1): $a = 63, b = 16$

A1

(7, 4): $a = 33, b = 56$

A1

Answer: (63, 16, 65) and (33, 56, 65)

6 marks

22 (6 marks)(a) $y = 1: x^2 = 3$ no; $y = 2: x^2 = 9, x = 3$. Solution (3, 2)

B1

Answer: (3, 2)

1 mark

(b) $(3 + 2\sqrt{2})^2 = 9 + 12\sqrt{2} + 8 = 17 + 12\sqrt{2}$

M1 A1

(17, 12): $289 - 288 = 1$

A1

Answer: (17, 12)

3 marks

(c) $(3 + 2\sqrt{2})(17 + 12\sqrt{2}) = 51 + 36\sqrt{2} + 34\sqrt{2} + 48 = 99 + 70\sqrt{2}$

M1

(99, 70): $9801 - 9800 = 1$

A1

Answer: (99, 70)**2 marks****23 (6 marks)**

Squares are 0 or 1 modulo 4

M1 A1 $x^2 - y^2 \equiv 0 - 0, 0 - 1, 1 - 0$ or $1 - 1$, i.e. 0, 3, 1 or 0 (mod 4); never 2**M1 A1** $2018 = 4 \times 504 + 2$ **M1**

So 2018 cannot be a difference of two squares

A1**Answer: Differences of squares are never 2 (mod 4)****6 marks****24 (7 marks)**Let c, s, h be the numbers: $c + s + h = 100$ and $10c + 3s + \frac{h}{2} = 100$ **B1**Eliminate h : $h = 100 - c - s$ **M1** $10c + 3s + 50 - \frac{(c + s)}{2} = 100$, so $20c + 6s - c - s = 100$ **M1 A1** $19c + 5s = 100$ **A1** $19c \equiv 100 \pmod{5}$: $4c \equiv 0$, so c is a multiple of 5; $c = 5$ gives $s = 1$ ($c = 10$ gives $s < 0$)**M1** $c = 5, s = 1, h = 94$ (check $50 + 3 + 47 = 100$)**A1****Answer: 5 cows, 1 sheep, 94 hens****7 marks****25 (6 marks)****(a)** Solutions exist only if $\text{hcf}(12, 18) = 6$ divides c **E1**6 does not divide 15, so there are none; being smaller than c is irrelevant**E1****Answer: 6 must divide c****2 marks****(b)** c must be a multiple of 6: 6, 12, 18, 24, 30**M1 A1** $c = 30$: $2x + 3y = 5$ **M1** $x = 1, y = 1$ ($12 + 18 = 30$)**A1****Answer: 6, 12, 18, 24, 30; (1, 1)****4 marks****26 (6 marks)** $7x \equiv 1000 \pmod{11}$: $1000 = 90 \times 11 + 10$, so $7x \equiv 10$ **M1** $7 \times 8 = 56 \equiv 1 \pmod{11}$, so $x \equiv 80 \equiv 3 \pmod{11}$ **M1 A1** $x = 3 + 11t, y = 89 - 7t$ **A1** $y > 0$ gives $t \leq 12$, and $x > 0$ gives $t \geq 0$: 13 solutions**M1**Smallest x : (3, 89); largest x : (135, 5)**A1****Answer: 13 solutions; (3, 89) and (135, 5)****6 marks****27 (8 marks)****(a)** $23 - 7b$ for $b = 0, 1, 2, 3$ is 23, 16, 9, 2 ($b \leq 3$)**M1 A1**

None is a multiple of 5, so 23 is impossible

A1**Answer: Impossible****3 marks****(b)** Residues of $7b$ modulo 5 for $b = 0, 1, 2, 3, 4$ are 0, 2, 4, 1, 3 (all residues)**M1 A1**So for any n there is b in $\{0, 1, 2, 3, 4\}$ with $n - 7b \equiv 0 \pmod{5}$ **M1** $n \geq 24$ gives $n - 7b \geq 24 - 28 = -4$; since it is a multiple of 5 it is ≥ 0 (a multiple of 5 greater than -5)**M1 A1****Answer: Proved****5 marks****28 (10 marks)****(a)** Squares are 0 or 1 modulo 3**B1**If neither a nor b were a multiple of 3 then $a^2 + b^2 \equiv 1 + 1 = 2 \pmod{3}$ **M1 A1**But $c^2 \equiv 0$ or 1, never 2: contradiction, so 3 divides a or b **E1****Answer: Proved****4 marks****(b)** Divide by $\text{hcf}(a, b)$ to get a primitive triple; if one of its legs is divisible by 4 so is the matching leg of (a, b) . So assume a, b have no common factor**M1**Both odd: $a^2 + b^2 \equiv 2 \pmod{4}$, not a square; both even is excluded, so exactly one is even, say b , and a, c are odd**M1 A1**Odd squares are 1 (mod 8) (since $(2m + 1)^2 = 4m(m + 1) + 1$)**M1**

$$b^2 = c^2 - a^2 \equiv 0 \pmod{8}$$

A1

b^2 is a multiple of 8, hence of 16 (a square with factor 2 has an even power of 2 ≥ 4), so 4 divides b

A1

Answer: Proved

6 marks

29 (8 marks)

$$(x - y)(x + y) = 2024 = 2^3 \times 11 \times 23$$

M1 A1

$x - y$ and $x + y$ have the same parity (their sum is $2x$); the product is even so both are even

M1 A1

Write $x - y = 2d$, $x + y = 2e$ with $de = 506 = 2 \times 11 \times 23$ and $d < e$

M1

Factor pairs: (1, 506), (2, 253), (11, 46), (22, 23)

A1

$$x = d + e, y = e - d$$

M1

$$(x, y) = (507, 505), (255, 251), (57, 35), (45, 1)$$

A1

Answer: (507,505), (255,251), (57,35), (45,1)

8 marks

30 (9 marks)

Suppose there is a non-zero solution; take one with $|z|$ smallest (positive)

B1

Modulo 3: $x^2 + y^2 \equiv 0$, and squares are 0 or 1

M1

Only $0 + 0$ gives 0, so $x \equiv y \equiv 0 \pmod{3}$

A1

Write $x = 3a$, $y = 3b$: $9a^2 + 9b^2 = 3z^2$, so $z^2 = 3(a^2 + b^2)$

M1 A1

3 divides z^2 , so 3 divides z (prime): $z = 3c$

M1

$$9c^2 = 3(a^2 + b^2), \text{ so } a^2 + b^2 = 3c^2$$

A1

(a, b, c) is a solution with $|c| < |z|$, contradicting minimality (infinite descent)

M1

Hence the only solution is $(0, 0, 0)$

A1

Answer: Only (0, 0, 0)

9 marks

Binary Operations

1 (3 marks)

$$3 * 4 = 3 + 8 = 11$$

B1

$$4 * 3 = 4 + 6 = 10$$

B1

$3 * 4 \neq 4 * 3$, so $*$ is not commutative

B1

Answer: 11, 10; not commutative

3 marks

2 (2 marks)

(a) Not closed: $2 - 5 = -3$ is not a positive integer

B1

(b) Closed: the difference of two integers is an integer

B1

Answer: (a) not closed; (b) closed

2 marks

3 (2 marks)

The entry for $3 \circ 3$ is 4, which is not in $\{1, 2, 3\}$

M1

So the set is not closed under $\circ$

E1

Answer: $3 \circ 3 = 4$ is not in the set

2 marks

4 (3 marks)

$$2 * 3 = 7, \text{ so } (2 * 3) * 4 = 7 * 4 = 29$$

B1

$$3 * 4 = 13, \text{ so } 2 * (3 * 4) = 2 * 13 = 27$$

B1

The results differ, so $*$ is not associative

B1

Answer: 29, 27; not associative

3 marks

5 (2 marks)

$$a * e = a \text{ gives } a + e - 3 = a$$

M1

$$e = 3 \text{ (also } 3 * a = a)$$

A1

Answer: $e = 3$

2 marks

6 (2 marks)

$r \circ q = q \circ r$ by commutativity = p

B1

$r \circ p = p \circ r = r$

B1

Answer: $r \circ q = p, r \circ p = r$

2 marks

7 (4 marks)

$a * b = a + b + ab = b + a + ba = b * a$, so commutative

B1

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

M1

$= a + b + c + ab + ac + bc + abc$

A1

This is symmetric in a, b, c, so equals $a * (b * c)$. Hence associative

A1

Answer: Commutative and associative

4 marks

8 (4 marks)

$a * e = a: a + e + 2 = a$, so $e = -2$

M1 A1

$a * a' = -2: a + a' + 2 = -2$

M1

$a' = -4 - a$

A1

Answer: $e = -2$; inverse $-4 - a$

4 marks

9 (4 marks)

$|a - b| = |b - a|$, so commutative

M1 A1

$(1 * 2) * 3 = 1 * 3 = 2$

M1

$1 * (2 * 3) = 1 * 1 = 0$, so not associative

A1

Answer: (i) yes (ii) no

4 marks

10 (4 marks)

Identity: 1

B1

$1 \times 1 = 1$ and $5 \times 5 = 25 \equiv 1$, so 1 and 5 are self-inverse

M1 A1

2, 3, 4 have none: $2 \times k, 3 \times k, 4 \times k$ are always even or multiples of 3, never 1 (mod 6); 0 has none

A1

Answer: Identity 1; inverses exist for 1 and 5 only

4 marks

11 (4 marks)

$\max(a, b)$ is one of a, b so is an integer: closed. $\max(a, b) = \max(b, a)$: commutative

B1

$\max(\max(a, b), c) = \max(a, b, c) = \max(a, \max(b, c))$: associative

M1

An identity e would need $\max(a, e) = a$ for all a, so $e \leq a$ for every integer a

M1

No integer is less than or equal to all integers, so no identity

A1

Answer: No identity

4 marks

12 (3 marks)

Choose $a = 1, b = 2, c = 3$

M1

$a + (b \times c) = 1 + 6 = 7$

A1

$(a + b) \times (a + c) = 3 \times 4 = 12 \neq 7$

A1

Answer: $7 \neq 12$

3 marks

13 (4 marks)

The row and column of 1 repeat the headings, so the identity is 1

B1

1 appears in row 1 col 1, row 2 col 3, row 3 col 2, row 4 col 4

M1

$1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$

A1 A1

Answer: Identity 1; inverses 1, 3, 2, 4

4 marks

14 (5 marks)

(a) $a * b = 1 - (1 - a)(1 - b)$

M1

$a, b \neq 1$ gives $(1 - a)(1 - b) \neq 0$, so $a * b \neq 1$

A1

Answer: Closed

2 marks

(b) $a * e = a: e - ae = 0, e(1 - a) = 0$, so $e = 0$

B1

Answer: $e = 0$

1 mark

(c) $a + a' - aa' = 0$, so $a'(1 - a) = -a$

M1

$$a' = \frac{a}{(a-1)}$$

A1

Answer: $\frac{a}{(a-1)}$

2 marks

15 (6 marks)

(a) $((a, b) * (c, d)) * (e, f) = (ac, ad + b) * (e, f) = (ace, acf + ad + b)$

M1 A1

$(a, b) * ((c, d) * (e, f)) = (a, b) * (ce, cf + d) = (ace, acf + ad + b)$. Equal

A1

Answer: Associative

3 marks

(b) $(a, b) * (1, 0) = (a, b)$ and $(1, 0) * (a, b) = (a, b)$: identity $(1, 0)$

B1

$(a, b) * (x, y) = (ax, ay + b) = (1, 0)$: $x = \frac{1}{a}$, $y = -\frac{b}{a}$

M1

Inverse $(\frac{1}{a}, -\frac{b}{a})$; $a \neq 0$ so it is in G

A1

Answer: Identity $(1, 0)$; inverse $(\frac{1}{a}, -\frac{b}{a})$

3 marks

16 (5 marks)

Row a, column b: entries $a + 2b \pmod{4}$

M1

Rows: 0 2 0 2 / 1 3 1 3 / 2 0 2 0 / 3 1 3 1

A1

$1 \circ 0 = 1$ but $0 \circ 1 = 2$, so not commutative

M1 A1

$a \circ 0 = a$ for all a (0 is a right identity), but $0 \circ b = 2b \pmod{4} \neq b$ for $b = 1$; no two-sided identity

A1

Answer: Not commutative; no identity

5 marks

$\circ$	0	1	2	3
0	0	2	0	2
1	1	3	1	3
2	2	0	2	0
3	3	1	3	1

17 (5 marks)

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, which is in H: closed

M1 A1

$x + y = y + x$, so commutative

B1

$x = 0$ gives the identity matrix

B1

The inverse of the matrix with x is the matrix with $-x$ since $x + (-x) = 0$

B1

Answer: Closed, commutative, identity I, inverse $x \rightarrow -x$

5 marks

18 (5 marks)

$a^2 + b^2 = b^2 + a^2$: commutative

B1

$(1 * 2) * 3 = 5 * 3 = 34$

M1

$1 * (2 * 3) = 1 * 13 = 170$, so not associative

A1

An identity e needs $a^2 + e^2 = a$ for all a; at $a = 0$ this forces $e = 0$, but then $a^2 = a$ fails for $a = 2$

M1 A1

Answer: Commutative, not associative, no identity

5 marks

19 (5 marks)

$2 * 3 = 8$ but $3 * 2 = 9$: not commutative

M1 A1

$(2 * 2) * 3 = 4^3 = 64$, $2 * (2 * 3) = 2^8 = 256$: not associative

M1 A1

$a * 1 = a$ for all a (1 is a right identity), but $1 * b = 1 \neq b$ for $b = 2$, so there is no identity

A1

Answer: None of these properties

5 marks

20 (5 marks)

$\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$, $\{1, 2\} \cap \{2, 3\} = \{2\}$, so the result is $\{1, 3\}$

M1 A1

$A * \emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A$, and similarly $\emptyset * A = A$: identity $\emptyset$

M1 A1

$A * A = A - A = \emptyset$, the identity, so each A is self-inverse

A1

Answer: $\{1, 3\}$; identity $\emptyset$; self-inverse

5 marks

21 (7 marks)

(a) $(a * b) * c = a + b + kab + c + k(a + b + kab)c$ M1

$= a + b + c + k(ab + ac + bc) + k^2abc$, symmetric in a, b, c A1

$a * (b * c)$ gives the same expression, so associative A1

Answer: Associative 3 marks

(b) $a * e = a$ gives $e(1 + ka) = 0$ for all a , so $e = 0$ B1

Answer: $e = 0$ 1 mark

(c) $a + x + kax = 0$, so $x(1 + ka) = -a$ M1

$$x = -\frac{a}{(1 + ka)}$$
A1

No inverse when $1 + ka = 0$, i.e. $a = -\frac{1}{k}$ A1

Answer: $-\frac{a}{(1 + ka)}$; none for $a = -\frac{1}{k}$ 3 marks

22 (6 marks)

(a) Suppose e and f are both identities. Then $e * f = f$ (as e is an identity) M1

and $e * f = e$ (as f is an identity), so $e = f$ A1

Answer: $e = f$ 2 marks

(b) Let b and c both be inverses of a : $a * b = b * a = e = a * c = c * a$ B1

$b = b * e = b * (a * c)$ M1

$= (b * a) * c$ by associativity M1

$= e * c = c$ A1

Answer: $b = c$ 4 marks

23 (6 marks)

(a) The table has $2 \times 2 = 4$ entries M1

Each entry is 0 or 1 independently: $2^4 = 16$ operations A1

Answer: 16 2 marks

(b) Commutative: the entries $0 \circ 1$ and $1 \circ 0$ are equal; 3 independent entries M1

$2^3 = 8$ A1

Answer: 8 2 marks

(c) Identity 0: the entries $0 \circ 0 = 0$, $0 \circ 1 = 1$, $1 \circ 0 = 1$ are fixed, $1 \circ 1$ free: 2 operations. Identity 1: similarly 2 M1

No operation has both 0 and 1 as identity (would give $0 = 0 \circ 1 = 1$), so $2 + 2 = 4$ A1

Answer: 4 2 marks

24 (6 marks)

(a) Commutativity says nothing about how three elements regroup; the two properties are independent E1

Answer: Commutativity does not imply associativity 1 mark

(b) $(1 * 2) * 3 = 1.5 * 3 = 2.25$ M1

$1 * (2 * 3) = 1 * 2.5 = 1.75 \neq 2.25$ A1

Answer: 2.25 and 1.75 2 marks

(c) $(a * b) * c = \frac{(a + b)}{4} + \frac{c}{2}$ M1

$a * (b * c) = \frac{a}{2} + \frac{(b + c)}{4}$ M1

Equating and simplifying: $\frac{c}{4} = \frac{a}{4}$, so $a = c$ A1

Answer: $a = c$ 3 marks

25 (6 marks)

(a) The row and column of e repeat the headings: identity e B1

$e \circ e = e$, $a \circ a = e$, $b \circ c = c \circ b = e$ M1

Inverses: $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$ A1

Answer: Identity e ; inverses e, a, c, b 3 marks

(b) $a \circ b = b$, so $(a \circ b) \circ c = b \circ c = e$ M1 A1

$b \circ c = e$, so $a \circ (b \circ c) = a \circ e = a \neq e$, hence not associative

Answer: $e \neq a$

A1

3 marks

26 (6 marks)

$$(a * b) * c = \frac{\frac{ab}{(a+b)} \times c}{\frac{ab}{(a+b)} + c}$$

B1

Multiply numerator and denominator by $(a + b)$: $\frac{abc}{(ab + c(a + b))} = \frac{abc}{(ab + bc + ca)}$

M1 A1

By symmetry $a * (b * c) = \frac{abc}{(bc + a(b + c))} = \frac{abc}{(ab + bc + ca)}$: associative

A1

Identity e : $\frac{ae}{(a + e)} = a$ gives $e = a + e$, so $a = 0$

M1

$a > 0$, so this is impossible: no identity

A1

Answer: Associative; no identity

6 marks

27 (8 marks)

Let $a, b \in S$. Then $(a * b) * (a * b) = e$

B1

Consider $(a * b) * (b * a) = a * (b * b) * a$ (associativity)

M1 A1

$= a * e * a = a * a = e$

M1 A1

So $b * a$ is an inverse of $a * b$

A1

$a * b$ is also an inverse of itself, and inverses are unique (if $x * y = y * x = e$ and $x * z = z * x = e$

M1

then $y = y * (x * z) = (y * x) * z = z$)

Hence $a * b = b * a$

A1

Answer: Commutative

8 marks

28 (9 marks)

$(a * b) * c = p(pa + qb + r) + qc + r = p^2a + pqb + qc + pr + r$

M1 A1

$a * (b * c) = pa + q(pb + qc + r) + r = pa + pqb + q^2c + qr + r$

M1 A1

Equal for all a, b, c : compare coefficients: $p^2 = p$, $q = q^2$, $pr = qr$

M1 A1

So $p, q \in \{0, 1\}$

A1

$(p, q) = (0, 0)$ or $(1, 1)$: $pr = qr$ holds for every r

M1

$(1, 0)$: $r = 0$; $(0, 1)$: $r = 0$. Triples: $(0, 0, r)$, $(1, 1, r)$, $(1, 0, 0)$, $(0, 1, 0)$

A1

Answer: $(0,0,r)$, $(1,1,r)$, $(1,0,0)$, $(0,1,0)$

9 marks

29 (9 marks)

(a) $1 + ab > 0$ since $|ab| < 1$

B1

$(1 + ab)^2 - (a + b)^2 = (1 - a^2)(1 - b^2) > 0$

M1 A1

Answer: Closed

3 marks

$$(b) (a * b) * c = \frac{\left(\frac{(a+b)}{(1+ab)} + c\right)}{\left(1 + \frac{(a+b)c}{(1+ab)}\right)}$$

M1

Multiply through by $(1 + ab)$: $\frac{(a + b + c + abc)}{(1 + ab + ac + bc)}$

M1 A1

This is symmetric in a, b, c , and $a * (b * c)$ gives the same, so associative

A1

Answer: Associative

4 marks

(c) $a * e = a$: $\frac{(a + e)}{(1 + ae)} = a$ gives $e = 0$ (using $e(1 - a^2) = 0$)

M1

$a * a' = 0$ gives $a' = -a$

A1

Answer: $e = 0$; inverse $-a$

2 marks

30 (8 marks)

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

M1 A1

$a * (b * c) = a * (b|c|) = a|b|c| = a|b||c|$. Equal

A1

Answer: Associative

3 marks

(b) $1 * (-1) = 1 \times |-1| = 1$

M1

$(-1) * 1 = -1 \times 1 = -1 \neq 1$

A1

Answer: Not commutative**2 marks****(c)** $a|e| = a$ for all a requires $|e| = 1$: $e = 1$ or $e = -1$ **M1 A1**Left identity f : $f|a| = a$ for all a ; $a = 1$ gives $f = 1$ but $a = -1$ gives $f = -1$, a contradiction**A1****Answer: Right identities 1 and -1; no left identity****3 marks**

Groups

1 (3 marks)

Identity: $a + 0 = 0 + a = a$, so 0 is the identity**B1**Inverse of a is $-a$ since $a + (-a) = 0$ **M1** $-a$ is an integer, so inverses lie in $\mathbb{Z}$ **A1****Answer: Identity 0, inverse $-a$** **3 marks**

2 (2 marks)

Identity 0 is present, but a positive integer a needs inverse $-a$ **M1** $-a$ is not a non-negative integer, so inverses fail**E1****Answer: No inverses****2 marks**

3 (2 marks)

The order is the number of elements: 4

B1 $i \times (-i) = -i^2 = 1$, so the inverse of i is $-i$ **B1****Answer: Order 4; inverse $-i$** **2 marks**

4 (2 marks)

 $0 \times x = 0 \neq 1$ for every x , so 0 has no inverse**M1**

The inverse axiom fails

E1**Answer: 0 has no inverse****2 marks**

5 (3 marks)

Identity 0

B1 $4 + 2 = 6 \equiv 0$, so the inverse of 4 is 2**B1**

Order 6

B1**Answer: 0; 2; 6****3 marks**

6 (2 marks)

Multiply on the left by a^{-1} : $a^{-1} * (a * b) = a^{-1} * (a * c)$ **M1** $(a^{-1} * a) * b = (a^{-1} * a) * c$, so $e * b = e * c$, giving $b = c$ **A1****Answer: $b = c$** **2 marks**

7 (4 marks)

Closure: $a * b \in G$ for all $a, b \in G$ **B1**Associativity: $(a * b) * c = a * (b * c)$ **B1**Identity: there is $e \in G$ with $e * a = a * e = a$ for all a **B1**Inverses: for each a there is $a^{-1} \in G$ with $a * a^{-1} = a^{-1} * a = e$ **B1****Answer: Closure, associativity, identity, inverses****4 marks**

8 (4 marks)

Closure: every entry in the table is 1, 2 or 4

B1

Associativity is inherited from multiplication of integers (mod 7)

B1

Identity: 1

B1Inverses: $1^{-1} = 1$, $2^{-1} = 4$, $4^{-1} = 2$ (1 appears in every row and column)**B1****Answer: A group****4 marks**

9 (3 marks)

Identity is 1

B1

0 has no inverse since $0 \times x \equiv 0 \pmod{6}$

M1

(also $2 \times x \equiv 1 \pmod{6}$ has no solution), so the inverse axiom fails

A1

Answer: 0 (and 2, 3, 4) have no inverse

3 marks

10 (4 marks)Products: $\omega \times \omega = \omega^2$, $\omega \times \omega^2 = \omega^3 = 1$, $\omega^2 \times \omega^2 = \omega^4 = \omega$; all in the set: closed

M1 A1

Associativity is inherited from multiplication of complex numbers; identity 1

B1

Inverses: $1^{-1} = 1$, $\omega^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$

A1

Answer: A group

4 marks

11 (3 marks) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

M1

 $= a e a^{-1} = aa^{-1} = e$

A1

Similarly $(b^{-1}a^{-1})(ab) = e$, so $b^{-1}a^{-1}$ is the inverse of ab

A1

Answer: Proved

3 marks

12 (4 marks)Order of a is the smallest $k > 0$ with $ka \equiv 0 \pmod{8}$

M1

1, 3, 5, 7: order 8 (e.g. 3, 6, 1, 4, 7, 2, 5, 0)

A1

2, 6: order 4 (2, 4, 6, 0)

A1

4: order 2

A1

Answer: 1, 3, 5, 7: 8; 2, 6: 4; 4: 2

4 marks

13 (4 marks)(a) $7 \times 8 = 56 = 55 + 1 \equiv 1$

M1

The inverse of 7 is 8

A1

Answer: 8

2 marks

(b) $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 5$, $3^4 \equiv 15 \equiv 4$

M1

 $3^5 \equiv 12 \equiv 1$, so the order is 5

A1

Answer: 5

2 marks

14 (5 marks)Table: $3 \times 3 = 9 \equiv 1$, $3 \times 5 = 15 \equiv 7$, $3 \times 7 = 21 \equiv 5$, $5 \times 5 = 25 \equiv 1$, $5 \times 7 = 35 \equiv 3$, $7 \times 7 = 49 \equiv 1$

M1 A1

All entries lie in the set: closed; associativity inherited

B1

Identity 1

B1

Each element squares to 1, so every element is its own inverse

A1

Answer: A group; yes, $a^2 = 1$ for all

5 marks

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

15 (5 marks)(a) $pq: 1 \rightarrow 2 \rightarrow 3$, $2 \rightarrow 1 \rightarrow 2$, $3 \rightarrow 3 \rightarrow 1$, so $pq = (1\ 3)$

M1 A1

 $qp: 1 \rightarrow 2 \rightarrow 1$, $2 \rightarrow 3 \rightarrow 3$, $3 \rightarrow 1 \rightarrow 2$, so $qp = (2\ 3) \neq pq$: not abelian

A1

Answer: $pq = (1\ 3)$, $qp = (2\ 3)$; not abelian

3 marks

(b) $p^{-1} = (1\ 3\ 2)$, $p^2 = (1\ 3\ 2) \neq e$, $p^3 = e$

M1

Order 3

A1

Answer: $p^{-1} = (1\ 3\ 2)$; order 3

2 marks

16 (5 marks)

1 has order 1

B1

2: 2, 4, 1 so order 3; 4: 4, 2, 1 so order 3

M1 A1

 $6 \equiv -1$: order 2

B1

3: 3, 2, 6, 4, 5, 1 so order 6; 5: 5, 4, 6, 2, 3, 1 so order 6

A1

Answer: 1:1, 2:3, 3:6, 4:3, 5:6, 6:2

5 marks

17 (6 marks)

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}$$

M1 A1

Upper triangular, and $aa' \times dd' \neq 0$, so closed

A1

Matrix multiplication is associative; identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ($a = d = 1, b = 0$)

B1

Inverse: $\begin{pmatrix} \frac{1}{a} & -\frac{b}{(ad)} \\ 0 & \frac{1}{d} \end{pmatrix}$ (check the product gives I)

M1

This is upper triangular with non-zero diagonal, so it lies in the set

A1

Answer: A group

6 marks

18 (4 marks) $abab = aabb$

M1

Multiply on the left by a^{-1} : $bab = abb$

M1

Multiply on the right by b^{-1} : $ba = ab$

A1

This holds for all a, b , so G is abelian

A1

Answer: $ab = ba$

4 marks

19 (5 marks)

$$f_2(f_3(x)) = \frac{1}{(-x)} = -\frac{1}{x} = f_4(x); f_3(f_2(x)) = -\frac{1}{x} = f_4(x)$$

M1 A1

Similarly $f_2 \circ f_4 = f_3, f_3 \circ f_4 = f_2$, and $f_i \circ f_i = f_1$ for each i : the table is closed

M1

Composition of functions is associative; identity f_1

B1

Each f_i is its own inverse ($f_i \circ f_i = f_1$)

A1

Answer: A group

5 marks

$\circ$	f₁	f₂	f₃	f₄
f₁	f_1	f_2	f_3	f_4
f₂	f_2	f_1	f_4	f_3
f₃	f_3	f_4	f_1	f_2
f₄	f_4	f_3	f_2	f_1

20 (5 marks)

$$|z_1 z_2| = |z_1| |z_2| = 1, \text{ so closed}$$

M1 A1

Multiplication of complex numbers is associative

B1

Identity 1, and $|1| = 1$

B1

$$\text{Inverse of } z \text{ is } \frac{1}{z} = \bar{z} \text{ since } z\bar{z} = |z|^2 = 1, \text{ and } \left|\frac{1}{z}\right| = 1$$

A1

Answer: A group

5 marks

21 (6 marks)

Let ab have order m , so $(ab)^m = e$

B1

$$(ba)^{m+1} = b(ab)^m a$$

M1 A1

$$(ba)^{m+1} = bea = ba, \text{ so } (ba)^m = e$$

M1

So the order of ba divides... is at most m (finite, order $\leq m$)

A1

By symmetry (swap a and b) the order of ab is at most that of ba , so the orders are equal

A1

Answer: Equal orders

6 marks

22 (7 marks)

$$(a) f_2(f_3(x)) = 1 - \frac{1}{x} = \frac{(x-1)}{x} = f_5(x)$$

M1 A1

$$f_3(f_2(x)) = \frac{1}{(1-x)} = f_4(x) \neq f_5(x); \text{ not abelian}$$

A1

Answer: f_5, f_4 ; not abelian

3 marks

$$(b) f_4(f_5(x)) = \frac{1}{(1 - \frac{(x-1)}{x})}$$

M1

$$= \frac{1}{(\frac{1}{x})} = x = f_1(x)$$

A1

$$\text{So } f_4^{-1} = f_5$$

A1

Answer: f_1 ; inverse f_5

3 marks

$$(c) f_4 \circ f_4 = f_5 \text{ (hence } f_4^3 = f_4 f_5 = f_1), \text{ so order 3}$$

B1

Answer: 3

1 mark

23 (6 marks)

(a) Powers of 2: 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1

M1 A1

The first power equal to 1 is 2^{12} , so the order is 12

A1

Answer: 12

3 marks

$$(b) 5 \equiv 2^9; 4 = 2^2$$

M1

$$\text{Order of } 2^k \text{ is } \frac{12}{\text{hcf}(12, k)}: 5 \text{ has order } \frac{12}{3} = 4, \text{ and } 4 \text{ has order } \frac{12}{2} = 6$$

M1 A1

Answer: 5: 4; 4: 6

3 marks

24 (6 marks)

(a) Closure fails: $1 + 3 = 4$ is even

B1

Identity fails: the identity is 0, which is not odd

B1

The inverse step used by the student is correct but irrelevant without closure and identity

E1

Answer: Closure and identity

3 marks

(b) Sum of two even integers is even: closed

B1

Associative; identity 0 is even

B1

Inverse of $2k$ is $-2k$, which is even

B1

Answer: A group

3 marks

25 (6 marks)

$ab = a$ would give $b = e$, and $ab = b$ would give $a = e$; both are false. With $ab \neq e$ (given) the only possibility is $ab = c$

M1 A1

A1

$ba = e$ would give $a = b^{-1} = b$, false; $ba = a$ or $ba = b$ gives $b = e$ or $a = e$, false; so $ba = c = ab$

M1

$ac = a(ab) = a^2b = b$ and $ca = (ba)a = b$, so $ac = ca$; $bc = b(ba) = b^2a = a$ and $cb = (ab)b = a$, so $bc = cb$

M1

Every pair commutes, so G is abelian. Table: $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$

A1

Answer: $ab = ba = c$; Klein four-group

6 marks

26 (6 marks)

$ab = a$ gives $b = e$ (cancellation); $ab = b$ gives $a = e$; both false, so $ab = e$

M1 A1

$ba = e$ too since $b = a^{-1}$

B1

$a^2 = e$ would give $a^2 = ab$, so $a = b$: false; $a^2 = a$ gives $a = e$: false. So $a^2 = b$

M1 A1

$b^2 = a$ similarly ($b^2 = e$ gives $b^2 = ba$, $b = a$; $b^2 = b$ gives $b = e$)

A1

Answer: $ab = ba = e$; $a^2 = b$; $b^2 = a$

6 marks

27 (9 marks)

Fix $a \in S$. The map $x \rightarrow ax$ is injective (left cancellation) on a finite set, so it is surjective

M1 A1

Hence there is $e \in S$ with $ae = a$

B1

For any b : $a(eb) = (ae)b = ab$, so $eb = b$: e is a left identity

M1 A1

$(be)b = b(eb) = bb$, so by right cancellation $be = b$: e is an identity

M1 A1

For each b , $x \rightarrow bx$ is surjective, so there is c with $bc = e$

M1

$b(cb) = (bc)b = eb = b = be$, so $cb = e$ (left cancellation). So c is the inverse of b

A1

Answer: S is a group

9 marks

28 (9 marks)

Since $ab = ba$, $(ab)^k = a^k b^k$ for every integer k

B1

$(ab)^{mn} = (a^m)^n (b^n)^m = e$, so the order of ab divides mn

M1 A1

Suppose $(ab)^k = e$. Then $a^k b^k = e$, so $x = a^k = b^{-k}$

M1 A1

$x^m = (a^m)^k = e$ and $x^n = (b^n)^{-k} = e$

M1

As $\text{hcf}(m, n) = 1$, there are integers u, v with $um + vn = 1$, so $x = x^{um + vn} = e$

M1 A1

Hence $a^k = e$, so m divides k ; similarly n divides k . As m, n are coprime, mn divides k , so the order is mn

A1

Answer: Order mn

9 marks

29 (8 marks)

Pair each element x with its inverse x^{-1}

M1

If $x \neq x^{-1}$ the elements x and x^{-1} form a pair of distinct elements: such elements come in pairs, so there is an even number of them

M1 A1

Let T be the set of x with $x = x^{-1}$, i.e. $x^2 = e$. $|G| = |T| + (\text{even number})$

M1

$|G|$ is even, so $|T|$ is even

A1

T contains e , whose order is 1, so T has $|T| - 1$ elements of order 2

M1 A1

$|T| - 1$ is odd

A1

Answer: An odd number

8 marks

30 (8 marks)

(a) Determinant $ad - bc$ is odd exactly when $ad + bc$ is odd, i.e. exactly one of ad, bc is 1

M1

$ad = 1$ ($a = d = 1$) with $bc = 0$: three choices of $(b, c) = (0, 0), (0, 1), (1, 0)$; $bc = 1$ with $ad = 0$:

M1

three choices of (a, d)

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$: 6 elements

A1

Answer: 6 elements

3 marks

(b) Row by column products, modulo 2: $AB = \begin{pmatrix} 1 \times 0 + 1 \times 1 & 1 \times 1 + 1 \times 0 \\ 0 \times 0 + 1 \times 1 & 0 \times 1 + 1 \times 0 \end{pmatrix}$

M1

$AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

A1

$BA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \neq AB$, so G is not abelian

A1

Answer: $AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, BA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

3 marks

(c) $(AB)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, (AB)^3 = I$, so AB has order 3

M1

Checking the orders of the six elements $(1, 2, 2, 2, 3, 3)$, none is 6 so G is not cyclic

A1

Answer: Order 3; no element of order 6**2 marks**

Subgroups

1 (2 marks)

Closure: $2 + 2 = 4$, $2 + 4 = 0$, $4 + 4 = 2$ (and 0 added to anything), all in the set; identity 0 is present

M1

Inverses: $2 + 4 \equiv 0$ so 2 and 4 are inverses; 0 is self-inverse

A1**Answer: Subgroup****2 marks**

2 (2 marks)

$2 + 2 = 4$

M1

4 is not in $\{0, 1, 2\}$, so the set is not closed

E1**Answer: Not closed****2 marks**

3 (2 marks)

The order of a subgroup of a finite group divides the order of the group

B1

5 does not divide 12

E1**Answer: 5 does not divide 12****2 marks**

4 (2 marks)

By Lagrange, the order must divide 15

M1

1, 3, 5, 15

A1**Answer: 1, 3, 5, 15****2 marks**

5 (2 marks)

Multiples of 3 modulo 12: $3, 6, 9, 12 \equiv 0$

M1

$\{0, 3, 6, 9\}$

A1**Answer: $\{0, 3, 6, 9\}$** **2 marks**

6 (2 marks)

The trivial subgroup $\{e\}$, containing just the identity

B1

G itself

B1**Answer: $\{e\}$ and G****2 marks**

7 (3 marks)

Closure: $1 \times 1 = 1$, $1 \times (-1) = -1$, $(-1) \times (-1) = 1$

M1

Identity 1 is in the set

B1

Inverses: $1^{-1} = 1$ and $(-1)^{-1} = -1$

A1**Answer: Subgroup****3 marks**

8 (4 marks)

By Lagrange, orders can only be 1, 2, 3, 6

M1

Order 1: $\{0\}$; order 6: $\mathbb{Z}_6$

A1

Order 2: $\{0, 3\}$ ($3 + 3 = 0$)

A1

Order 3: $\{0, 2, 4\}$

A1**Answer: $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, $\mathbb{Z}_6$** **4 marks**

9 (3 marks)

Powers of 2: $2, 4, 8 \equiv 1$, so $\langle 2 \rangle = \{1, 2, 4\}$

M1 A1

Powers of 3: $3, 2, 6, 4, 5, 1$, so $\langle 3 \rangle$ is the whole group

A1**Answer: $\langle 2 \rangle = \{1, 2, 4\}$; $\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$** **3 marks**

10 (3 marks)

Cosets are $a + H$: $0 + H = \{0, 4, 8\}$

M1

$1 + H = \{1, 5, 9\}$, $2 + H = \{2, 6, 10\}$, $3 + H = \{3, 7, 11\}$

A1

Further cosets repeat these ($4 + H = H$ etc.): four distinct cosets

A1

Answer: $\{0,4,8\}$, $\{1,5,9\}$, $\{2,6,10\}$, $\{3,7,11\}$

3 marks

11 (3 marks)

Let f be the identity of H : $ff = f$

B1

In G , multiply by f^{-1} : $f = e$ ($f^{-1}ff = f^{-1}f$)

M1

So $f = e$

A1

Answer: $f = e$

3 marks

12 (3 marks)

$(1\ 2\ 3)^2 = (1\ 3\ 2)$, $(1\ 2\ 3)^3 = e$: subgroup $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$

M1 A1

$(1\ 2)^2 = e$: subgroup $\{e, (1\ 2)\}$

A1

Answer: $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$; $\{e, (1\ 2)\}$

3 marks

13 (3 marks)

Subgroup orders divide 7, so are 1 or 7

M1

A non-identity element a generates a subgroup of order greater than 1, so of order 7

M1

So a has order 7

A1

Answer: Orders 1 or 7 only

3 marks

14 (4 marks)

Non-empty: $1 = 2^0 \in H$

B1

Take $x = 2^m$ and $y = 2^n$ in H

M1

$xy^{-1} = 2^m \times 2^{-n} = 2^{m-n}$

M1

$m - n$ is an integer, so $xy^{-1} \in H$: H is a subgroup

A1

Answer: Subgroup

4 marks

15 (5 marks)

$0 \in 3\mathbb{Z}$; $3a - 3b = 3(a - b) \in 3\mathbb{Z}$, so a subgroup

M1 A1

$x \in 3\mathbb{Z} \cap 5\mathbb{Z}$ means 3 and 5 both divide x

M1

3 and 5 are coprime, so 15 divides x

A1

Conversely multiples of 15 are multiples of both: $3\mathbb{Z} \cap 5\mathbb{Z} = 15\mathbb{Z}$

A1

Answer: Proved

5 marks

16 (5 marks)

(a) $H \cap K = \{0\}$, the trivial subgroup

B1

It contains the identity and is closed: $0 + 0 = 0$

B1

Answer: $\{0\}$

2 marks

(b) $H \cup K = \{0, 2, 3, 4\}$

B1

$2 + 3 = 5$, which is not in $H \cup K$

M1

Not closed, so not a subgroup

A1

Answer: Not closed: $2 + 3 = 5$

3 marks

17 (4 marks)

(a) The order of an element divides $|G|$ (the order of $\langle a \rangle$ is a divisor)

M1

1, 2, 5, 10

A1

Answer: 1, 2, 5, 10

2 marks

(b) Orders other than 1 are 2, 5 or 10; 10 is excluded

M1

So each non-identity element has order 2 or 5

A1

Answer: 2 or 5

2 marks

18 (5 marks)

$e \in Z(G)$ since $ex = xe$, so non-empty

B1

Closure: if $y, z \in Z(G)$, $(yz)x = y(zx) = y(xz) = (yx)z = (xy)z = x(yz)$

M1 A1

Inverse: $zx = xz$ gives $x = z^{-1}xz$, so $xz^{-1} = z^{-1}x$

M1

So $z^{-1} \in Z(G)$: subgroup

A1

Answer: Subgroup

5 marks

19 (5 marks)

Left cosets are $pH = \{p, p(1\ 2)\}$; $eH = \{e, (1\ 2)\}$

M1

$(1\ 2\ 3)(1\ 2)$: $1 \rightarrow 2 \rightarrow 3$, $2 \rightarrow 1 \rightarrow 2$, $3 \rightarrow 3 \rightarrow 1$, so $= (1\ 3)$. $(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}$

M1 A1

$(1\ 3\ 2)(1\ 2)$: $1 \rightarrow 2 \rightarrow 1$, $2 \rightarrow 1 \rightarrow 3$, $3 \rightarrow 3 \rightarrow 2$, so $= (2\ 3)$. $(1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\}$

A1

The three cosets are disjoint and contain all six elements

A1

Answer: $\{e, (1\ 2)\}$, $\{(1\ 2\ 3), (1\ 3)\}$, $\{(1\ 3\ 2), (2\ 3)\}$

5 marks

20 (4 marks)

$e = a^0 \in \langle a \rangle$

B1

Closure: $a^m a^n = a^{m+n} \in \langle a \rangle$

M1

Inverse: $(a^n)^{-1} = a^{-n} \in \langle a \rangle$

M1

Associativity is inherited from G , so $\langle a \rangle$ is a subgroup

A1

Answer: Subgroup

4 marks

21 (6 marks)

By Lagrange the possible orders are 1, 2, 3, 4, 6, 12

M1

Order 1: $\{0\}$; order 12: the whole group

A1

Order 2: $\{0, 6\}$; order 3: $\{0, 4, 8\}$

A1

Order 4: $\{0, 3, 6, 9\}$; order 6: $\{0, 2, 4, 6, 8, 10\}$

A1

In a subgroup of order d every element x satisfies $dx \equiv 0 \pmod{12}$, so x is a multiple of $12/d$; there are exactly d such multiples, so the subgroup is $\langle 12/d \rangle$

M1

Hence exactly one subgroup for each order

A1

Answer: One subgroup of each order 1, 2, 3, 4, 6, 12

6 marks

22 (6 marks)

Orders divide 6, so are 1, 2, 3, 6

M1

Order 1: $\{e\}$; order 6: S_3

A1

Order 2: an element of order 2 generates $\{e, (1\ 2)\}$, $\{e, (1\ 3)\}$ or $\{e, (2\ 3)\}$

M1 A1

Order 3: an element of order 3 generates $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$, the only such subgroup

A1

Every subgroup of order 2 or 3 is generated by one of its non-identity elements (prime order), so these exhaust all possibilities: 6 subgroups

A1

Answer: 6 subgroups: $\{e\}$, three of order 2, one of order 3, S_3

6 marks

23 (6 marks)

$H \cap K$ is a subgroup of H , so $|H \cap K|$ divides $|H|$ (Lagrange)

M1 A1

$H \cap K$ is a subgroup of K , so $|H \cap K|$ divides $|K|$

M1

$|H|$ and $|K|$ coprime, so $|H \cap K|$ divides $\text{hcf}(|H|, |K|) = 1$

A1

$|H \cap K| = 1$, so $H \cap K = \{e\}$

A1

Orders 4 and 9 are coprime, so the intersection is $\{e\}$

A1

Answer: $H \cap K = \{e\}$

6 marks

24 (6 marks)

(a) Lagrange's theorem says subgroup orders divide $|G|$; it does not say every set whose size divides $|G|$ is a subgroup

E1

$3 + 3 = 6$ is not in the set

M1

Not closed, so not a subgroup

A1

Answer: Not closed: $3 + 3 = 6$

3 marks

(b) $\langle 2 \rangle = \{0, 2, 4, 6\}$

B1

A subgroup of order 4 has all its elements of order dividing 4; elements of order 1, 2 or 4 are 0, 4 and 2, 6

M1

So any such subgroup must be $\{0, 2, 4, 6\}$

Answer: $\{0, 2, 4, 6\}$

A1

3 marks

25 (6 marks)

(a) $8, 16, 24 \equiv 4, 12, 20 \equiv 0$

M1

$H = \{0, 4, 8, 12, 16\}$

A1

Answer: $\{0, 4, 8, 12, 16\}$

2 marks

(b) $|H| = 5$, so there are $20 \div 5 = 4$ cosets

M1

$H, 1 + H = \{1, 5, 9, 13, 17\}, 2 + H = \{2, 6, 10, 14, 18\}, 3 + H = \{3, 7, 11, 15, 19\}$

A1

Answer: 4 cosets

2 marks

(c) $7 + H = 19 + H$ if and only if $7 - 19 \in H$

M1

$-12 \equiv 8 \in H$, so yes (both are $3 + H$)

A1

Answer: Yes

2 marks

26 (6 marks)

$e^2 = e$, so $e \in H$

B1

If $g, h \in H$: $(gh)^2 = ghgh = g^2h^2$ (G abelian) $= ee = e$, so $gh \in H$

M1 A1

$g^2 = e$ means $g^{-1} = g \in H$, so inverses are in H

A1

In $(\mathbb{Z}_{12}, +)$: $g^2 = e$ means $2g \equiv 0 \pmod{12}$, so $g = 0$ or 6

M1

$H = \{0, 6\}$

A1

Answer: $H = \{0, 6\}$

6 marks

27 (9 marks)

Left cosets $aH = \{ah : h \in H\}$ for $a \in G$

B1

Every a lies in aH since $a = ae$

B1

Same size: the map $h \rightarrow ah$ from H to aH is a bijection (cancellation gives injectivity), so $|aH| = |H|$

M1 A1

Cosets are equal or disjoint: if $x \in aH \cap bH$ then $x = ah_1 = bh_2$, so $a = bh_2h_1^{-1} \in bH$

M1 A1

Then $aH \subseteq bH$, and symmetrically $bH \subseteq aH$, so $aH = bH$

M1

The distinct cosets partition G , each of size $|H|$, so $|G| = k|H|$

A1

Hence $|H|$ divides $|G|$

A1

Answer: $|G| = k|H|$

9 marks

28 (9 marks)

Take $a \neq e$. $\langle a \rangle$ is a subgroup other than $\{e\}$, so $\langle a \rangle = G$: G is cyclic

M1 A1

Suppose G is infinite. Then $\langle a^2 \rangle$ is a subgroup; it is not $\{e\}$ and does not contain a (else $a = a^{2k}$, $a^{2k-1} = e$, finite order)

M1 A1

This gives a proper non-trivial subgroup, a contradiction. So G is finite, of order n

A1

Suppose $n = rs$ with $1 < r, s < n$. Then a^r has order s (smallest positive multiple of r with $n \mid \cdot$)

M1

$\langle a^r \rangle$ has order s with $1 < s < n$: a proper non-trivial subgroup, a contradiction

A1

So n has no factorisation; n is prime ($n \geq 2$ as $G \neq \{e\}$)

A1

G is cyclic of prime order

A1

Answer: Cyclic of prime order

9 marks

29 (8 marks)

Consider the $|H||K|$ products hk ($h \in H, k \in K$)

B1

Suppose $hk = h'k'$. Then $h^{-1}h' = k'k^{-1}$

M1 A1

The left side lies in H and the right side in K , so $t = h^{-1}h' \in H \cap K$

M1

Then $h' = ht^{-1}$ and $k' = tk$ with $t \in H \cap K$

A1

Conversely every $t \in H \cap K$ gives a pair (ht^{-1}, tk) with the same product

M1

So each element of HK arises from exactly $|H \cap K|$ pairs

A1

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

A1

Answer: $\frac{|H||K|}{|H \cap K|}$

8 marks

30 (8 marks)**(a)** Coprime to 15 (not divisible by 3 or 5): 1, 2, 4, 7, 8, 11, 13, 14

M1

Order 8

A1

Answer: 8 elements

2 marks

(b) The order k of a is the order of the subgroup $\langle a \rangle$, so k divides 8

M1 A1

$$a^8 = (a^k)^{8/k} \equiv 1$$

A1

Answer: $a^8 \equiv 1$

3 marks

(c) $222 = 8 \times 27 + 6$

M1

$$7^{222} \equiv 7^6 \pmod{15}; 7^2 = 49 \equiv 4, 7^4 \equiv 16 \equiv 1$$

M1

$$7^6 \equiv 7^4 \times 7^2 \equiv 4; \text{ the remainder is } 4$$

A1

Answer: 4

3 marks

Cyclic Groups**1 (2 marks)**5 is prime, so for $a \neq 0$ the multiples $a, 2a, 3a, 4a, 5a \equiv 0$ are all different modulo 5

M1

So each non-zero element generates all of $\mathbb{Z}_5$; generators 1, 2, 3, 4

A1

Answer: 1, 2, 3, 4

2 marks

2 (2 marks)

Multiples of 3 modulo 7: 3, 6, 2, 5, 1, 4, 0

M1

All seven elements appear, so $\langle 3 \rangle = \mathbb{Z}_7$

A1

Answer: Cyclic, $\langle 3 \rangle = \mathbb{Z}_7$

2 marks

3 (3 marks)

$$G = \{e, a, a^2, a^3, a^4, a^5\}$$

B1

$$(a^2)^3 = a^6 = e, (a^2)^1, (a^2)^2 \neq e$$

M1

The order of a^2 is 3

A1

Answer: Order 3

3 marks

4 (2 marks)

$$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$$

M1

All elements are powers of i , so the group is cyclic with generator i

A1

Answer: Generator i

2 marks

5 (2 marks)

$$4, 8, 12 \equiv 2, 16 \equiv 6, 20 \equiv 0$$

M1

The order is 5

A1

Answer: 5

2 marks

6 (2 marks)

$$\text{Let } G = \langle a \rangle \text{ and } x = a^m, y = a^n$$

B1

$$xy = a^{m+n} = a^{n+m} = yx$$

B1

Answer: $xy = yx$

2 marks

7 (3 marks) k generates $\mathbb{Z}_{12}$ exactly when $\text{hcf}(k, 12) = 1$

M1

$$k = 1, 5, 7, 11$$

A1

(e.g. 5 has order 12, $6 \times 5 = 30 \neq 0$; $12/\text{hcf}(5, 12) = 12$)

B1

Answer: 1, 5, 7, 11

3 marks

8 (4 marks)

The order of a^k is $\frac{12}{\text{hcf}(12, k)}$

M1

$$a^2: \frac{12}{2} = 6; a^3: \frac{12}{3} = 4$$

A1

$$a^4: \frac{12}{4} = 3; a^5: \frac{12}{1} = 12$$

A1

$$a^6: \frac{12}{6} = 2$$

A1

Answer: 6, 4, 3, 12, 2

4 marks

9 (3 marks)

$$3^2 = 9 \equiv 1, 5^2 = 25 \equiv 1, 7^2 = 49 \equiv 1$$

M1 A1

Every element has order 1 or 2, none has order 4, so no element generates the group

A1

Answer: No element of order 4

3 marks

10 (3 marks)

Powers of 3: 3, 2, 6, 4, 5, 1

M1 A1

3 has order 6, so it generates the group of order 6

A1

Answer: Generated by 3

3 marks

11 (4 marks)

Multiples of (1, 1): (1, 1), (0, 2), (1, 0), (0, 1), (1, 2), (0, 0)

M1 A1

These are 6 different elements, which is the whole group of order 6

A1

So (1, 1) generates the group, which is cyclic

A1

Answer: Generator (1, 1)

4 marks

12 (4 marks)

$\omega^6 = e^{2\pi i} = 1$, and the roots are $e^{i\pi k/3}$, $k = 0, \dots, 5$

M1

Elements $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5$, all powers of ω

A1

$\omega^5 = \overline{\omega}$ has order 6 since $\text{hcf}(5, 6) = 1$

M1

So ω^5 is also a generator

A1

Answer: Generators ω and ω^5

4 marks

13 (3 marks)

Generators are k with $\text{hcf}(k, 20) = 1$

M1

1, 3, 7, 9, 11, 13, 17, 19

A1

There are 8 generators

A1

Answer: 1, 3, 7, 9, 11, 13, 17, 19; 8

3 marks

14 (5 marks)

Subgroup orders divide 18: 1, 2, 3, 6, 9, 18

M1 A1

The subgroup of order d is generated by $a^{18/d}$

M1

$\{e\}$; $\langle a^9 \rangle$ (order 2); $\langle a^6 \rangle$ (order 3); $\langle a^3 \rangle$ (order 6); $\langle a^2 \rangle$ (order 9); $\langle a \rangle$

A1

There is exactly one subgroup for each divisor

A1

Answer: One subgroup of each order 1, 2, 3, 6, 9, 18

5 marks

15 (5 marks)

$\mathbb{Z}_2 \times \mathbb{Z}_2$: each element satisfies $2(a, b) = (0, 0)$, so no element has order 4

M1 A1

$\mathbb{Z}_2 \times \mathbb{Z}_4$ has order 8; a generator would have order 8

M1

$2(a, b) = (2a, 2b) = (0, 2b)$, $4(a, b) = (0, 0)$: every element has order at most 4

A1

No element has order 8, so not cyclic

A1

Answer: Neither is cyclic

5 marks

16 (5 marks)

Let $d = \text{hcf}(n, k)$, $n = dn'$, $k = dk'$ with $\text{hcf}(n', k') = 1$

B1

$(a^k)^m = e$ if and only if n divides km

M1

dn' divides $dk'm$, so n' divides $k'm$

M1 A1

n' and k' coprime so n' divides m ; the least m is $n' = \frac{n}{d}$

A1

Answer: $\frac{n}{\text{hcf}(n, k)}$

5 marks

17 (5 marks)

Powers of 2: $2, 4, 8, 16 \equiv 1, 14 \equiv 5, 10 \equiv 1$

M1 A1

2 has order 6 = $|U|$, so $U = \langle 2 \rangle$ is cyclic

A1

Generators are 2^k with $\text{hcf}(k, 6) = 1$: $k = 1, 5$

M1

$2^1 = 2$ and $2^5 \equiv 5$, so the generators are 2 and 5

A1

Answer: Cyclic; generators 2 and 5

5 marks

18 (5 marks)

a^k has order $\frac{15}{\text{hcf}(15, k)}$

M1

Order 5 needs $\text{hcf}(15, k) = 3$: $k = 3, 6, 9, 12$

M1 A1

Order 3 needs $\text{hcf}(15, k) = 5$: $k = 5, 10$

M1

Order 5: a^3, a^6, a^9, a^{12} ; order 3: a^5, a^{10}

A1

Answer: Order 5: a^3, a^6, a^9, a^{12} ; order 3: a^5, a^{10}

5 marks

19 (5 marks)

$G = \langle a \rangle$, $x = a^k$, $x^2 = a^{2k} = e$ if and only if n divides $2k$

M1

(a) $n = 8$: 8 divides $2k$ when k is a multiple of 4: $k = 0, 4$. Two solutions (e and a^4)

M1 A1

(b) $n = 9$: 9 divides $2k$ only when 9 divides k (9 is odd): $k = 0$ only

M1

One solution ($x = e$)

A1

Answer: (a) 2 (b) 1

5 marks

20 (5 marks)

Fifth roots of unity are z^k , $k = 0, \dots, 4$, and $z^5 = 1$

B1

Powers of z^2 : $z^2, z^4, z^6 = z, z^8 = z^3, z^{10} = 1$

M1 A1

All five roots appear, so z^2 generates the group

A1

$z^3 = (z^2)^4$

A1

Answer: $z^3 = (z^2)^4$

5 marks

21 (6 marks)

If $H = \{0\}$ then $H = 0\mathbb{Z}$

B1

Otherwise H contains a positive integer (if $x \in H$ then $-x \in H$); let n be the smallest positive element

M1 A1

$n\mathbb{Z} \subseteq H$ since H is closed under addition and inverses

M1

For $x \in H$ write $x = nq + r$, $0 \leq r < n$; then $r = x - nq \in H$

M1

n is the smallest positive element, so $r = 0$ and $x \in n\mathbb{Z}$. Hence $H = n\mathbb{Z}$

A1

Answer: $H = n\mathbb{Z}$

6 marks

22 (6 marks)

Powers of 2 modulo 11: 2, 4, 8, 5, 10, 9, 7, 3, 6, 1

M1 A1

The first power equal to 1 is 2^{10} , so 2 has order 10 and is a primitive root

A1

Generators are 2^k with $\text{hcf}(k, 10) = 1$: $k = 1, 3, 7, 9$

M1

$2^3 = 8, 2^7 \equiv 7, 2^9 \equiv 6$

A1

Primitive roots: 2, 6, 7, 8

A1

Answer: 2, 6, 7, 8

6 marks

23 (6 marks)

(a) Element (a, b) has order $\text{lcm}(\text{ord } a, \text{ord } b)$, with $\text{ord } a \in \{1, 2, 4\}$ and $\text{ord } b \in \{1, 2, 3, 6\}$ **M1**

Largest possible value is $\text{lcm}(4, 6) = 12 < 24 = |\mathbb{Z}_4 \times \mathbb{Z}_6|$ **M1**

No element of order 24, so not cyclic **A1**

Answer: Not cyclic **3 marks**

(b) $(1, 1)$ has order $\text{lcm}(4, 9) = 36$ **M1 A1**

The group has order 36, so $(1, 1)$ generates it: cyclic **A1**

Answer: Generator $(1, 1)$ **3 marks**

24 (6 marks)

(a) $8, 16 \equiv 4, 24 \equiv 0$: order 3 ($= 12 \div \text{hcf}(8, 12)$) **M1**

Order 3 $\neq 12$, so 8 is not a generator **A1**

Answer: Order 3; not a generator **2 marks**

(b) 3 is odd but $\text{hcf}(3, 12) = 3$, so 3 has order 4 **M1**

3, 6, 9, 0: only 4 elements, so 3 is not a generator **A1**

Answer: 3 has order 4 **2 marks**

(c) k generates $(\mathbb{Z}_n, +)$ if and only if $\text{hcf}(k, n) = 1$ (k coprime to n) **B1**

e.g. for $n = 12$, the generators are 1, 5, 7, 11 **B1**

Answer: $\text{hcf}(k, n) = 1$ **2 marks**

25 (6 marks)

(a) Positions 6, 12, 3, 9, 0 **M1**

The dial returns to 0 after 5 turns (visiting 5 different positions in total) **A1**

Answer: 6, 12, 3, 9, 0; 5 turns **2 marks**

(b) Every position is visited exactly when k generates $(\mathbb{Z}_{15}, +)$ **M1**

This happens when $\text{hcf}(k, 15) = 1$ **M1**

$k = 1, 2, 4, 7, 8, 11, 13, 14$ **A1**

Answer: 1, 2, 4, 7, 8, 11, 13, 14 **3 marks**

(c) The turns needed is the order of k , which divides $|\mathbb{Z}_{15}| = 15$ (Lagrange) **E1**

Answer: Order divides 15 **1 mark**

26 (6 marks)

Existence: $a^{n/d}$ has order d , so $\langle a^{n/d} \rangle$ has order d **M1 A1**

Let H be a subgroup of order d . Every subgroup of a cyclic group is cyclic, $H = \langle a^m \rangle$ where m is the least positive power in H **M1**

Every element x of H satisfies $x^d = e$ (Lagrange); $x = a^j$ gives n divides jd , so j is a multiple of n/d **M1 A1**

So $H \subseteq \langle a^{n/d} \rangle$, and both have d elements, so $H = \langle a^{n/d} \rangle$: unique **A1**

Answer: Unique **6 marks**

27 (8 marks)

The order of any element divides n ; an element of order d generates a subgroup of order d **M1 A1**

That subgroup is the unique one of order d , namely $\langle a^{n/d} \rangle$, which is cyclic of order d **M1**

Its generators are the $\varphi(d)$ elements $a^{(n/d)j}$ with $\text{hcf}(j, d) = 1$; these are exactly the elements of order d **M1 A1**

Every element has exactly one order, so $n = \sum_{d|n} \varphi(d)$ **A1**

$n = 12$: divisors 1, 2, 3, 4, 6, 12 give $\varphi = 1, 1, 2, 2, 4$ **M1**

Sum = 12 **A1**

Answer: $\sum \varphi(d) = n$ **8 marks**

28 (8 marks)

Orders of elements divide 4: 1, 2 or 4

M1 A1

If some element has order 4 it generates the group, which is cyclic

A1

Otherwise every non-identity element x satisfies $x^2 = e$, so $x^{-1} = x$

M1

For any a, b : $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$

M1 A1

Hence the group is abelian

A1

(the elements are e, a, b, ab , the Klein four-group)

B1

Answer: Cyclic, or Klein four-group

8 marks

29 (8 marks)

g has order $p - 1$; g^k has order $\frac{(p-1)}{\text{hcf}(k, p-1)}$

M1 A1

This equals $p - 1$ exactly when $\text{hcf}(k, p - 1) = 1$

A1

For $p = 13$: $k \in \{1, 5, 7, 11\}$

M1

$2^1 = 2$

B1

$2^5 = 32 \equiv 6, 2^7 = 128 \equiv 11$

M1

$2^{11} = 2048 \equiv 7$ ($2048 = 13 \times 157 + 7$)

A1

Primitive roots: 2, 6, 7, 11

A1

Answer: 2, 6, 7, 11

8 marks

30 (9 marks)

(a) Let $G = \langle a \rangle$ have order n , $x = a^j$ with $0 \leq j < n$

B1

$x^2 = e$ if and only if n divides $2j$, i.e. j is a multiple of $n/\text{hcf}(n, 2)$

M1 A1

Between 0 and $n - 1$ there are exactly $\text{hcf}(n, 2) \leq 2$ such multiples

A1

Answer: At most 2

4 marks

(b) $(2^{k-1} \pm 1)^2 = 2^{2k-2} \pm 2^k + 1$

M1

$2^k - 2 \geq k$ when $k \geq 2$, so this is $\equiv 1 \pmod{2^k}$

A1

$(2^k - 1)^2 = 2^{2k} - 2^{k+1} + 1 \equiv 1$; also $1^2 = 1$

B1

The four residues are odd and distinct when $k \geq 3$ ($2^{k-1} - 1 > 1$ and $2^{k-1} + 1 < 2^k - 1$)

M1

Four elements with $x^2 = 1$ contradicts part (a), so U_{2^k} is not cyclic

A1

Answer: Four square roots of 1; not cyclic

5 marks

Group Isomorphisms**1 (2 marks)**

φ is a bijection (one-to-one and onto)

B1

$\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$

B1

Answer: Bijection with $\varphi(ab) = \varphi(a)\varphi(b)$

2 marks

2 (2 marks)

An isomorphism is a bijection, so the groups must have the same number of elements

M1

$6 \neq 8$, so they are not isomorphic

E1

Answer: Different orders

2 marks

3 (3 marks)

$\varphi(0) = 1, \varphi(1) = i, \varphi(2) = -1, \varphi(3) = -i$

B1 B1

$\varphi(1 + 3) = \varphi(0) = 1$ and $\varphi(1)\varphi(3) = i \times (-i) = 1$

B1

Answer: 1, i, -1, -i; both sides equal 1

3 marks

4 (2 marks)

If φ is an isomorphism and G is abelian, $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$, and every element of H is some $\varphi(a)$, so H is abelian

M1

So an abelian group is never isomorphic to a non-abelian one

E1

Answer: Commutativity is preserved

2 marks

5 (2 marks)

$$\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b)$$

M1

φ is a bijection (inverse $y \rightarrow \frac{y}{2}$)

A1

Answer: Isomorphism

2 marks

6 (2 marks)

$$f(0 + 0) = f(0) = 1$$

M1

$$f(0) + f(0) = 2 \neq 1, \text{ so } f(a + b) \neq f(a) + f(b) \text{ in general}$$

A1

Answer: $f(0) = 1 \neq 0$

2 marks

7 (4 marks)

$$\varphi(a + b) = e^{a+b} = e^a e^b = \varphi(a)\varphi(b)$$

M1 A1

Injective: $e^a = e^b$ implies $a = b$

B1

Surjective: for $y > 0$, $\varphi(\ln y) = y$

B1

Answer: Isomorphism

4 marks

8 (4 marks)Well defined since $i^4 = 1$: $i^{k+4} = i^k$

B1

$$\varphi(a + b) = i^{a+b} = i^a i^b = \varphi(a)\varphi(b)$$

M1 A1

 $\varphi(0), \varphi(1), \varphi(2), \varphi(3) = 1, i, -1, -i$ are distinct and cover the set: a bijection

A1

Answer: Isomorphism

4 marks

9 (3 marks) $(\mathbb{Z}_4, +)$ has an element of order 4: 1, 2, 3, 0

M1

In $\{1, 3, 5, 7\}$ every element squares to 1, so no element has order 4

M1

An isomorphism preserves orders of elements, so the groups are not isomorphic

E1

Answer: Orders of elements differ

3 marks

10 (3 marks) $(\mathbb{Z}_6, +)$ is abelian

B1

In S_3 : $(1\ 2)(1\ 3) = (1\ 3\ 2)$ but $(1\ 3)(1\ 2) = (1\ 2\ 3)$, so S_3 is not abelian

M1

An isomorphism preserves commutativity, so they are not isomorphic

E1

Answer: One is abelian, the other is not

3 marks

11 (4 marks)

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$$

M1

$$\text{Multiply by } \varphi(e_G)^{-1}: e_H = \varphi(e_G)$$

A1

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H$$

M1

So $\varphi(a^{-1})$ is the inverse of $\varphi(a)$

A1

Answer: Proved

4 marks

12 (4 marks) $\mathbb{Z}_8$: orders of 0, 1, ..., 7 are 1, 8, 4, 8, 2, 8, 4, 8

M1 A1

In $\mathbb{Z}_2 \times \mathbb{Z}_4$ every (a, b) satisfies $4(a, b) = (0, 0)$, so the maximum order is 4

M1

 $\mathbb{Z}_8$ has an element of order 8, so they are not isomorphic

A1

Answer: $\square_8$ has elements of order 8; the other does not

4 marks

13 (4 marks)Define $\varphi(e) = 0$, $\varphi(a) = 1$, $\varphi(b) = 2$

B1

Since $a \circ a = b$: $\varphi(a \circ a) = 2 = 1 + 1 = \varphi(a) + \varphi(a)$

M1

Since $a \circ b = e$ and $b \circ b = a$: $1 + 2 = 0 = \varphi(e)$, $2 + 2 = 1 = \varphi(a)$; the table of G matches the addition table of $\mathbb{Z}_3$ entry by entry

A1

 φ is a bijection preserving the operation, so G is isomorphic to $\mathbb{Z}_3$

A1

Answer: $\varphi(e) = 0$, $\varphi(a) = 1$, $\varphi(b) = 2$

4 marks

14 (5 marks)

$\varphi(k+4) = 2^{k+4} = 2^k \times 16 \equiv 2^k \pmod{5}$, so φ is well defined

M1 A1

$\varphi(a+b) = 2^{a+b} = 2^a 2^b = \varphi(a)\varphi(b)$

M1

$\varphi(0), \varphi(1), \varphi(2), \varphi(3) = 1, 2, 4, 3$: distinct, all four elements, so bijective

A1

Hence φ is an isomorphism

A1

Answer: Isomorphism

5 marks

15 (5 marks)

$\varphi(0), \dots, \varphi(5) = (0,0), (1,1), (0,2), (1,0), (0,1), (1,2)$

M1 A1

These six pairs are distinct, so φ is a bijection

A1

$(a+b) \bmod 2 = (a \bmod 2 + b \bmod 2) \bmod 2$, and likewise mod 3

M1

So $\varphi(a+b) = \varphi(a) + \varphi(b)$; isomorphism

A1

Answer: Isomorphism

5 marks

16 (5 marks)

Define $\varphi(1) = (0, 0)$, $\varphi(3) = (1, 0)$, $\varphi(5) = (0, 1)$, $\varphi(7) = (1, 1)$

B1

Bijection by construction

B1

$3 \times 5 = 15 \equiv 7$ and $(1, 0) + (0, 1) = (1, 1)$

M1

$3 \times 7 \equiv 5$ and $(1, 0) + (1, 1) = (0, 1)$; $5 \times 7 \equiv 3$ and $(0, 1) + (1, 1) = (1, 0)$

M1

All squares are 1 and $(a, b) + (a, b) = (0, 0)$; all products agree, so isomorphic

A1

Answer: Isomorphic

5 marks

17 (5 marks)

$\varphi(a)^n = \varphi(a^n) = \varphi(e_G) = e_H$, so the order of $\varphi(a)$ divides n

M1 A1

Suppose $\varphi(a)^m = e_H$. Then $\varphi(a^m) = e_H = \varphi(e_G)$

M1

φ is injective, so $a^m = e_G$, and n divides m

A1

So the order of $\varphi(a)$ is exactly n

A1

Answer: Order n

5 marks

18 (5 marks)

In the group of non-zero real numbers under multiplication the element -1 satisfies $(-1) \times (-1) = 1$, so it has order 2

M1 A1

In $(\mathbb{R}, +)$, $x + x = 0$ implies $x = 0$, so the only element with $2x = 0$ is the identity: no element of order 2

M1 A1

An isomorphism preserves orders of elements, so the groups are not isomorphic

E1

Answer: -1 has order 2; $(\mathbb{R}, +)$ has no element of order 2

5 marks

19 (4 marks)

Define $\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$

B1

$\varphi(x)\varphi(y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \varphi(x+y)$

M1 A1

φ is clearly a bijection from $\mathbb{R}$ to the set of matrices; hence an isomorphism

A1

Answer: Isomorphism

4 marks

20 (5 marks)

Define $\varphi(a^k) = b^k$

B1

Well defined: $a^j = a^k$ iff $n \mid (j - k)$ iff $b^j = b^k$

M1 A1

$\varphi(a^j a^k) = \varphi(a^{j+k}) = b^{j+k} = b^j b^k$

M1

Bijection: the n elements of G map to the n distinct elements of H

A1

Answer: $\varphi(a^k) = b^k$

5 marks

21 (6 marks)

Any group of order 4 is isomorphic to $(\mathbb{Z}_4, +)$ if it has an element of order 4, and to $\mathbb{Z}_2 \times \mathbb{Z}_2$ if all non-identity elements have order 2

M1 A1

A: i has order 4 ($i, -1, -i, 1$), so A is isomorphic to $\mathbb{Z}_4$

A1

C: 2, 4, 3, 1 so 2 has order 4, so C is isomorphic to $\mathbb{Z}_4$

A1

B: $3^2 = 5^2 = 7^2 \equiv 1 \pmod{8}$, so B is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$

A1

D: $5^2 = 25 \equiv 1, 7^2 = 49 \equiv 1, 11^2 = 121 \equiv 1 \pmod{12}$, so D is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$

A1

Answer: A and C are isomorphic to $\mathbb{Z}_4$; B and D are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$

6 marks

22 (6 marks)

(a) Since 4 divides 12, $(x + y) \pmod{12}$ and $x + y$ have the same remainder mod 4

M1

So $\varphi(x + y) = \varphi(x) + \varphi(y) \pmod{4}$

A1

Answer: Homomorphism

2 marks

(b) Kernel: $x \equiv 0 \pmod{4}$: $\{0, 4, 8\}$

B1

Image: $\varphi(0), \varphi(1), \varphi(2), \varphi(3) = 0, 1, 2, 3$, so all of $\mathbb{Z}_4$

B1

Answer: Kernel $\{0, 4, 8\}$; image $\mathbb{Z}_4$

2 marks

(c) $\varphi(4) = \varphi(0) = 0$, so φ is not injective

M1

($|\mathbb{Z}_{12}| = 12 \neq 4 = |\mathbb{Z}_4|$)

E1

Answer: Not injective

2 marks

23 (6 marks)

$\mathbb{Z}_8$: the order of k is $\frac{8}{\text{hcf}(8, k)}$: order 1: $\{0\}$; order 2: $\{4\}$; order 4: $\{2, 6\}$; order 8: $\{1, 3, 5, 7\}$

M1 A1

$\mathbb{Z}_2 \times \mathbb{Z}_4$: (a, b) has order $\text{lcm}(\text{ord } a, \text{ord } b)$, where $\text{ord } a \in \{1, 2\}$, $\text{ord } b \in \{1, 2, 4\}$

M1

Order 1: $(0, 0)$; order 2: $(1, 0), (0, 2), (1, 2)$; order 4: $(0, 1), (0, 3), (1, 1), (1, 3)$

A1

No element has order 8 in $\mathbb{Z}_2 \times \mathbb{Z}_4$

M1

An isomorphism preserves orders, so the groups are not isomorphic

A1

Answer: Orders differ: $\mathbb{Z}_8$ has 4 elements of order 8

6 marks

24 (6 marks)

(a) Having the same order and being abelian are necessary conditions for isomorphism, not sufficient ones

E1

Other structure, such as the orders of elements, must also match

E1

Answer: Necessary, not sufficient

2 marks

(b) 1 has order 4 in $(\mathbb{Z}_4, +)$

B1

Every element of $\{1, 3, 5, 7\}$ has order at most 2, but isomorphisms preserve order

E1

Answer: Orders differ

2 marks

(c) All non-identity elements have order 2

M1

The Klein four-group, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$

A1

Answer: $\mathbb{Z}_2 \times \mathbb{Z}_2$

2 marks

25 (6 marks)

$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1}$

M1 A1

$\varphi(x)\varphi(y) = x^{-1}y^{-1}$

B1

If G is abelian, $y^{-1}x^{-1} = x^{-1}y^{-1}$, so φ is a homomorphism

A1

Conversely, if φ is a homomorphism then $y^{-1}x^{-1} = x^{-1}y^{-1}$ for all x, y ; replacing x, y by their inverses $a = x^{-1}, b = y^{-1}$: $ba = ab$

M1

So G is abelian

A1

Answer: Homomorphism iff abelian

6 marks

26 (6 marks)

Name the values $P = 2, Q = -1, R = \frac{1}{2}$

B1

$f_2: 2 \rightarrow -1, -1 \rightarrow 2, \frac{1}{2} \rightarrow \frac{1}{2}$: (P Q); $f_3: P \leftrightarrow R$ and Q fixed: (P R); $f_6: Q \leftrightarrow R$: (Q R)

M1 A1

$f_4: 2 \rightarrow -1, -1 \rightarrow \frac{1}{2}, \frac{1}{2} \rightarrow 2$: (P Q R); $f_5: 2 \rightarrow \frac{1}{2}, -1 \rightarrow 2, \frac{1}{2} \rightarrow -1$: (P R Q); f_1 : identity

A1

The six functions give six different permutations: a bijection onto S_3

M1

Composition of functions corresponds to composition of the permutations they induce, so $\varphi(f \circ g) = \varphi(f)\varphi(g)$: isomorphism

A1

Answer: Isomorphic to S_3

6 marks

27 (8 marks)

Let $G = \langle a \rangle$. Define $\varphi(k) = a^k$

B1

$\varphi(j+k) = a^{j+k} = a^j a^k = \varphi(j)\varphi(k)$: a homomorphism from $(\mathbb{Z}, +)$

M1 A1

Infinite order: $a^j = a^k$ implies $a^{j-k} = e$, so $j = k$; φ is injective, and surjective since $G = \langle a \rangle$: φ is an isomorphism $\mathbb{Z} \rightarrow G$

M1 A1

Order n : define $\varphi(k \bmod n) = a^k$; well defined as $a^n = e$

M1

$a^j = a^k$ iff $n \mid (j - k)$, so injective on $\mathbb{Z}_n$; both groups have n elements so bijective

A1

Homomorphism as before: G is isomorphic to $(\mathbb{Z}_n, +)$

A1

Answer: G is isomorphic to $\square$ or $\square_n$

8 marks

28 (8 marks)

Define $\varphi(k) = (k \bmod m, k \bmod n)$

B1

Well defined: if $k \equiv k' \pmod{mn}$ then $k \equiv k' \pmod{m}$ and $\pmod{n}$

M1 A1

Homomorphism: remainders add componentwise

A1

Injective: $\varphi(j) = \varphi(k)$ means $m \mid (j - k)$ and $n \mid (j - k)$; m, n coprime so $mn \mid (j - k)$, so $j = k$ in $\mathbb{Z}_{mn}$

M1 A1

Both groups have mn elements, so φ is also surjective

M1

$m = 3, n = 5$ (coprime) gives that $\mathbb{Z}_{15}$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_5$

A1

Answer: Isomorphic

8 marks

29 (9 marks)

Let G be abelian of order 6; orders of elements divide 6: 1, 2, 3, 6

M1

If an element has order 6, G is cyclic

B1

G has even order, so some x has order 2

M1 A1

Suppose no element has order 3. Then (no element of order 6) every non-identity element has order 2

M1

Take distinct non-identity a, b : $\{e, a, b, ab\}$ is a subgroup of order 4 (G abelian, $a^2 = b^2 = e$)

A1

4 does not divide 6, contradicting Lagrange. So some y has order 3

M1 A1

$xy = yx$ has order $2 \times 3 = 6$, so G is cyclic and isomorphic to $(\mathbb{Z}_6, +)$

A1

Answer: Cyclic, isomorphic to $\square_6$

9 marks

30 (8 marks)

A homomorphism φ is determined by $k = \varphi(1)$: $\varphi(x) = \varphi(1 + 1 + \dots + 1) = kx$

M1 A1

Each such φ_k is a homomorphism: $\varphi_k(x + y) = kx + ky$

B1

φ_k is bijective iff its image is all of $\mathbb{Z}_n$, i.e. iff k generates $\mathbb{Z}_n$ (the image is $\langle k \rangle$)

M1 A1

k generates $\mathbb{Z}_n$ iff $\text{hcf}(k, n) = 1$

A1

$n = 12$: $k = 1, 5, 7, 11$

M1

$\varphi_1(x) = x, \varphi_5(x) = 5x, \varphi_7(x) = 7x, \varphi_{11}(x) = 11x \pmod{12}$

A1

Answer: k coprime to n ; for $n = 12, k = 1, 5, 7, 11$

8 marks