Review exercise 1

1 We wish to prove that for any natural number we have

$3|(n^3+2n)$

We proceed by induction and the division algorithm.

For the base case $n=1$ we have $n^3+2n=3$ so the claim is true.

Now suppose the claim is true for $n-1$.

Then by the division algorithm we have $(n-1)^3+2(n-1)=3q$ for some natural number q

Now we can write

$$n^3+2n=(n-1+1)^3+2(n-1+1)$$
$$=(n-1)^3+3(n-1)^2+3(n-1)+1+2(n-1)+2$$
$$=(n-1)^3+2(n-1)+3((n-1)^2+(n-1)+1)$$
$$=3q+3((n-1)^2+(n-1)+1)$$
$$=3q'$$

for some natural number q'.

Hence the induction is complete and the claim is true.

2 **a** Paul is incorrect. Suppose he was correct, then we could write $1096=43q+17$ for a natural number q, in particular we have

$$q=\frac{1096-17}{43}$$

and this is not a natural number

b Applying the division algorithm gives

$514098=178\times2873+2704$

Carrying out the Euclidean algorithm gives

$2873=2704+169$

This is a non-zero remainder so we need to do another step:

$2704=16\times169$

Hence $\gcd(2873,514098)=169$

So the fraction can be simplified further

3 We wish to compute $\gcd(808,2256)$ using the Euclidean Algorithm.

The first step is to write:

$2256=2\times808+640$

Then:

$808=640+168$

$640=3\times168+136$

$168=136+32$

$136=4\times32+8$

Finally we have

$32=4\times8$

Hence $\gcd(808,2256)=8$

4 **a** We will use the Euclidean algorithm to compute $\gcd(201, 5365)$

We have

$5365 = 26\times 201+139$

$201 = 139+62$

$139 = 2\times 62+15$

$62 = 4\times 15+2$

$15 = 7\times 2+1$

$2 = 2\times 1$

Hence $\gcd(201, 5365) = 1$

b Working backwards through the Euclidean algorithm:

$$\begin{aligned}1 &= 15-7\times 2\\ &= 15-7\times(62-4\times 15) = 29\times 15-7\times 62\\ &= 29\times(139-2\times 62)-7\times 62 = 29\times 139-65\times 62\\ &= 29\times 139-65\times(201-139) = 94\times 139-65\times 201\\ &= 94\times(5365-26\times 201)-65\times 201\\ &= 94\times 5365-2509\times 201\end{aligned}$$

5 We wish to find integers x and y such that

$142x+1023y = 1$

We apply the Euclidean algorithm then work backwards:

$1023 = 7\times 142+29$

$142 = 4\times 29+26$

$29 = 26+3$

$26 = 8\times 3+2$

$3 = 2+1$

$2 = 2\times 1$

Now working backwards:

$$\begin{aligned}1 &= 3-2\\ &= 3-(26-8\times 3) = 9\times 3-26\\ &= 9\times(29-26)-26 = 9\times 29-10\times 26\\ &= 9\times 29-10\times(142-4\times 29) = 49\times 29-10\times 142\\ &= 49\times(1023-7\times 42)-10\times 142\\ &= 49\times 1023-353\times 142\end{aligned}$$

6 **a** Any weight that can be measured using this method is of the form $75x+270y$, where x and y are integers but have opposite sign. The smallest weight that can be measured is the smallest positive linear combination of this form, which is $\gcd(75, 270) = 15$.

6 **b** Applying the Euclidean algorithm:

$$270 = 3\times 75 + 45$$
$$75 = 45 + 30$$
$$45 = 30 + 15$$
$$30 = 2\times 15$$

Working backwards:

$$15 = 45 - 1\times 30$$
$$15 = 45 - (75 - 1\times 45)$$
$$15 = 2\times 45 - 75$$
$$15 = 2\times(270 - 3\times 75) - 75$$
$$15 = 2\times 270 - 7\times 75$$

Now multiplying through by 27:

$$405 = 270\times 54 + 75\times(-189)$$
$$405 = 270\times(5 + 10\times 4) + 75\times(-10\times 18 - 9)$$
$$405 = (270\times 4) + (1350\times 10) + (1350\times -10) + 75\times(-9)$$
$$405 = (270\times 4) + 75\times(-9)$$

Therefore you should place the fish and $9\times 75\text{g}$ weights together and $4\times 270\text{g}$ weights on the other side.

7 **a** We have $a \equiv b \pmod n$ hence there is an integer q such that $a = qn + b$ so $a + c = qn + b + c$ hence $a + c \equiv b + c \pmod n$

b We have $a \equiv b \pmod n$ and $c \equiv d \pmod n$ so there are integers p and q such that $a = qn + b$ and $c = pn + d$ so

$$ac = (qn + b)(pn + d)$$
$$= qpn^2 + qnd + bpn + bd$$
$$= n(qpn + qd + bp) + bd$$

Hence $ac \equiv bd \pmod n$ as required

c We have $a \equiv b \pmod n$ and we wish to prove that $a^2 + ac = b^2 + bc \pmod n$.

By part **a** we know $a + c \equiv b + c \pmod n$.

Applying part b then gives

$$a(a + c) \equiv b(b + c) \pmod n$$
$$a^2 + ac = b^2 + bc \pmod n$$

8 We have $N = 25^{400} + 11^{200}$ and wish to compute $N(\text{mod}\,3)$.

We consider each term in the sum separately.

First note that $25(\text{mod}\,3) = 1,$ hence $25^{400}(\text{mod}\,3) = 1^{400} = 1$

Also $11(\text{mod}\,3) = 2,$ so $11^2(\text{mod}\,3) = 4(\text{mod}\,3) = 1.$

Therefore we have $11^{200}(\text{mod}\,3) = 1^{200} = 1.$

Hence $N = 2(\text{mod}\,3)$

9 We wish to prove that $2^{5n+1} + 5^{n+2}(\text{mod}\,27) = 0$

We proceed by induction.

In the $n = 0$ case one has $2 + 5^2 = 27 = 0(\text{mod}\,27)$ so the base case is true.

For the induction step assume the claim is true for n

For $n+1$ one has

$2^{5(n+1)+1} + 5^{n+3}(\text{mod}\,27)$

$= 2^{5n+6} + 5^{n+3}(\text{mod}\,27)$

$= 2^5 \times 2^{5n+1} + 5 \times 5^{n+2}$

$= 32 \times 2^{5n+1} - 5 \times 2^{5n+1}(\text{mod}\,27)$

$= 27(\text{mod}\,27) = 0(\text{mod}\,27)$

10 We wish to compute $3^{999}(\text{mod}\,7)$.

We start by computing some small powers:

$3^1 = 3(\text{mod}\,7)$

$3^2 = 2(\text{mod}\,7)$

$3^3 = 6(\text{mod}\,7)$

$3^4 = 4(\text{mod}\,7)$

$3^5 = 5(\text{mod}\,7)$

$3^6 = 1(\text{mod}\,7)$

After this the pattern repeats itself.

So $3^{999} = 3^{166\times 6+3} = 6(\text{mod}\ 7)$

Therefore the remainder is 6

11 We write $N = pqrs$ where the digits satisfy $-p+q-r+s = 0(\text{mod}\,11)$.

So $N(\text{mod}\,11) = 10^3 p + 10^2 q + 10r + s(\text{mod}\,11)$

Now using properties of modular arithmetic we have

$10r = -r(\text{mod}\,11)$

$100q = (9\times 11+1)q(\text{mod}\,11)$

$1000p = (91\times 11-1)p = -p(\text{mod}\,11)$

Hence $N(\text{mod}\,11) = -p+q-r+s(\text{mod}\,11) = 0(\text{mod}\,11)$

12 The sum of the digits of 3 848 517 is 36 which is clearly divisible by 9, hence by the test 3 848 517 is also divisible by 9.

13 A number has digits $6a193b8$. Since we are told the number is divisible by 11, we have that $6-a+1-9+3-b+8=0(\text{mod } 11)$.

Which simplifies to

$9-a-b=0(\text{mod } 11)$

Since it is divisible by 4, we have that the number with digits $b8$ is divisible by 4.
This limits the choice of possible b to just 0, 2, 4, 6, 8.
Now using the relation $a+b=9(\text{mod } 11)$, the following pairs of (a,b) are possible:

$(a,b)=(9,0)$

$(a,b)=(7,2)$

$(a,b)=(5,4)$

$(a,b)=(3,6)$

$(a,b)=(1,8)$

14 We wish to solve $75x\equiv 2(\text{mod}\,8)$.

Firstly, $(9\times 8+3)x\equiv 2(\text{mod}\,8)$.

So the equation reduces to $3x\equiv 2(\text{mod}\,8)$.

Now since $\gcd(3,8)=1$, 3 has a multiplicative inverse modulo 8, which is 3.

Multiplying through by 3 gives

$9x\equiv 6(\text{mod}\,8)\Rightarrow x\equiv 6(\text{mod}\,8)$

Hence the solution is given by $x\equiv 6\,\text{mod}(8)$.

15 a Suppose there was a solution to $40x\equiv 1(\text{mod}\,12)$.

Then there would exist a q such that $40x=12q+1$.
However, the left-hand side of the above equation is even, whereas the right hand side is odd.
This is a contradiction, therefore there are no solutions.

b We wish to solve $40x\equiv 1(\text{mod } 11)$.

Since $\gcd(4,11)=1$, 4 has a multiplicative inverse mod 11 which is 3.
Multiplying through by 3 gives

$120x\equiv 3(\text{mod } 11)\Rightarrow 10x\equiv 3(\text{mod } 11)$

Hence the equation reduces to $10x\equiv 3(\text{mod } 11)$.

Similarly, since $\gcd(10,11)=1$, 10 has a multiplicative inverse mod 11 which is 10.

$100x\equiv 30(\text{mod } 11)\Rightarrow x\equiv 30(\text{mod } 11)$

Hence the equation reduces to

$x\equiv 30(\text{mod } 11)=8(\text{mod } 11)$

16 a By inspection, the congruence equations are

$n=0(\text{mod}\,18)$

$n=2(\text{mod}\,14)$

16 b We wish to solve these for n.

$n = 0(\text{mod}\,18)$ gives the possible values.

$18, 36, 54, 72, 90, 108, 126, 144, 162, 180, 198$

The condition $n = 2(\text{mod}\,14)$ gives the possible values.

$2, 16, 30, 44, 58, 72, 86, 100, 114, 128, 142, 156, 170, 184, 198$

Hence the two solutions are 72 and 198.

17 a Fermat's Little Theorem states that p is a prime number and a is any integer, then $a^p \equiv a(\text{mod}\,p)$ or $a^{p-1} \equiv 1(\text{mod}\,p)$

b We wish to compute $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}(\text{mod}\,7)$

We have by Fermat:

$2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1(\text{mod}\ 7)$

Therefore $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$

$\equiv 2^2 + 3^0 + 4^4 + 5^2 + 6^0$

$\equiv 4 + 1 + 2^8 + 25 + 1$

$\equiv 14 \equiv 0(\text{mod}\ 7)$

as required

18 We wish to solve $x^{86} \equiv 4(\text{mod}\,7)$.

By Fermat's Little Theorem, $x^6 \equiv 1(\text{mod}\,7)$.

Therefore, $x^{86} \equiv x^{80}(\text{mod}\,7) \equiv \ldots \equiv x^2(\text{mod}\,7)$.

Hence we need to solve $x^2 \equiv 4(\text{mod}\,7)$, hence $x \equiv 2(\text{mod}\,7)$ or $x \equiv 5(\text{mod}\,7)$.

19 a The residue representing the encoding of A is given by $7(\text{mod}\,26)$, hence A gets encoded to G.

The residue representing the encoding of B is given by $14(\text{mod}\,26)$, hence B gets encoded to N. Hence ABBA gets encoded to GNNG.

b We wish to use Bezout's identity to find a multiplicative inverse of 7 mod 26.
Applying the Euclidean algorithm:

$26 = 3 \times 7 + 5$

$7 = 5 + 2$

$5 = 2 \times 2 + 1$

$2 = 2 \times 1$

Working backwards gives

$1 = 5 - 2 \times 2$

$= 5 - 2 \times (7 - 5) = 3 \times 5 - 2 \times 7$

$= 3 \times (26 - 3 \times 7) - 2 \times 7 = 3 \times 26 - 11 \times 7$

Hence the multiplicative inverse of 7 is $-11 \equiv 15(\text{mod}\,26)$.

19 c We wish to decode HIT.
The residue representing the decoding of H is equal to $15\times 8(\text{mod }26)=16.$ Hence H is decoded to P.

The residue representing the decoding of I is equal to $15\times 9(\text{mod }26)=5.$ Hence I is decoded to E.

The residue representing the decoding of T is equal to $15\times 20(\text{mod }26)=14.$ Hence T is decoded to N.

Hence HIT is decoded to PEN.

d Since 6 and 26 are not coprime, 6 does not have a multiplicative inverse mod 26.
Therefore the encoding is not reversible, as multiple letters may be encoded to the same letter.

20 Given that there are 7 people who must sit downstairs and 6 people who must sit upstairs, the problem reduces to finding the number of ways to distribute the remaining 20 people among the remaining 11 free downstairs slots and 9 free upstairs slots.
Once we have determined how many are sitting upstairs, this determines who is seated downstairs.

Therefore the number of combinations is $\begin{pmatrix}20\\9\end{pmatrix}=167960.$

21 For n to be divisible by 9, the digits must add up to a multiple of 9.
The digits 0 through 9 add up to a multiple of 9, so if you omit two of them, those two must also add up to 9. So if you omit 0, then you must also omit 9 etc.
This means that there are only five possible pairs of numbers that you can omit.

If you omit 0 and 9, then the remaining 8 digits can be arranged in any order, giving 8! possibilities.
In each of the other cases, you cannot place 0 in the first position, thus giving 7(7!) possible ways of ordering the numbers.
So, of the five pairs of possible omissions, you have one choice that leads to 8! numbers, and four choices that each lead to 7(7!) numbers.

Summing these gives $8!+(4\times 7)7!=8(7!)+28(7!)=36(7!).$

Therefore $a = 36$.

22 a We can view each subset of $S=\{1,2,3,4,5,6,7\}$ as a way of assigning to each element a 1 or 0 depending on whether the element is in the subset or not respectively.
Since we have 2 choices for each element, the number of assignments and hence subsets is $2^7=128.$

b We are choosing 4 elements from 7 to be in the subset.

Therefore, the number of ways we can do this is $\begin{pmatrix}7\\4\end{pmatrix}=35.$

Therefore there are 35 subsets.

c i If we can repeat digits, then there are 7 choices for each digit hence $7^4=2401$ possible numbers.

ii If we cannot repeat digits, then there are $7\times 6\times 5\times 4=840$ choices.

23 a **i** Closure is satisfied since all entries in the Cayley table are members of *S*.
ii By inspecting the row/column associated to *s*, we can see that *s* acts as the identity.

b The flaw in the argument is that for an element *y* to be the inverse of the element *x*, not only do we require that $x * y = e$, but we also require $y * x = e$. By inspecting the table, one can see this is not the case for all elements; for example, $p * t = s$ but $t * p = r$.

c The axiom for associativity is not satisfied. For example:
$p * (p * t) = p * s = p$
$(p * p) * t = q * t = r$

24 a We show that *M* forms a group.
We are allowed to assume associativity, so we just need to prove closure, identity and inverse.

Closure follows from properties of modular arithmetic.
In particular for $x, y \in M$ $x * y$ is the residue when $x + y$ is divided by 6.
By the division algorithm, this is always an integer in *M*.

Identity exists since $x + 0 \equiv x (\text{mod}\, 6)$. Hence 0 is the identity element.
Inverse follows since $x + (6 - x) \equiv 0 (\text{mod}\, 6)$ for any *x*, hence $6 - x$ is the inverse of *x*.

b 1 has order 6, 2 has order 3, 3 has order 2, 4 has order 3 and 5 has order 6

c The order of any subgroup must divide the order of the group. Hence *M* cannot have a subgroup of order 4, as 4 does not divide 6.

25 Suppose G is a group and $a, b, c \in G$ with $a * c = b * c$. We will show that $a = b$.
Since G is a group, we may multiply on the right by c^{-1}.
This gives $(a * c) * c^{-1} = (b * c) * c^{-1}$.
Then by associativity:
$a * (c * c^{-1}) = b * (c * c^{-1})$
By the definition of inverse:
$a * e = b * e$
Therefore $a = b$.

26 Firstly, note that the order of the group is 3. Let the element corresponding to a rotation by 120° be *x*.
Then x^2 is a rotation by 240° and x^3 is a rotation by 360° which is the identity, hence x has order 3.
Hence the group is cyclic, generated by *x*.

27 a Let G be the set of integers that are less than 8 and relatively prime to 8, i.e. $\{1,3,5,7\}$.
We claim these form a group under multiplication modulo 8.
One can compute a Cayley table giving

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Closure: All elements in the table are members of G.
Identity: The row and column corresponding to 1 are the same as the column and row headings, so 1 is the identity.
Associativity: $(a\times_8 b)\times_8 c \equiv a\times_8 b\times_8 c \equiv a\times_8 (b\times_8 c)$
Therefore $(G,\times_8)$ is a group.

b If the group were cyclic there would be an element of order 4.
However, inspecting the table above, we can see that every element has order 2.
Hence the group cannot be cyclic.

28 By the division theorem, $k = mq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leqslant r < m$.

So $b = a^k = a^{mq+r} = (a^m)^q a^r$

So $a^r = (a^m)^{-q} a^k$

Now $a^m, a^k \in H$, so $a^r \in H$

Since a^m is the smallest power of a in H, and $r < m$, we have that $r = 0$.

Therefore $k = mq$ and every element of H is of the form $(a^m)^q$.

Therefore H has generating element a^m, so is cyclic.

29 a There are 4 elements in the group, so the order is 4.

b $H = \{e, a\}$ cannot be a subgroup since $a^2 = b \notin H$, similarly $H = \{e, c\}$ cannot be a subgroup since $c^2 = b \notin H$.

c Let $S = \{e, b\}$. We claim that this is a subgroup.
Associativity follows from the associativity of the group operation on G.
From considering the Cayley table, every element is in S, so S is closed.

	e	b
e	e	b
b	b	e

From the table we also see that the identity is in S.
Also, every element has an inverse since $e^{-1} = e$ and $b^{-1} = b$.

30 a The order of any element must be 1 or p.
So any element $a \neq e$ has order p and is a generator for C.
Therefore C is cyclic.

30 b By Lagrange's theorem, the order of any subgroup of C has to divide p.
Therefore, the order of any subgroup is either 1 or p, so the only subgroups of C are itself and $\{e\}$.
Therefore C has no non-trivial proper subgroups.

31 Let H be the subgroup generated by a, then the order of H is the smallest positive k such that $a^k = e$, on the other hand By Lagrange's theorem k must divide n so there is an integer q such that $n = qk$ and then we have $a^n = a^{qk} = \left(a^k\right)^q = e^q = e$ as required.

32 By Bezout's identity we can find integers x, y such that $mx + ny = 1$.

So $a = a^{mx+ny} = \left(a^x\right)^m \left(a^n\right)^y = \left(a^x\right)^m$ since $a^n = e.$

So there exists $b = a^x$ such that $b^m = a.$

To prove uniqueness, assume there is another element $c \in G$ such that $c^m = a.$

Then $b^m = c^m \Rightarrow b^{mx} = c^{mx} \Rightarrow b^{1-my} = c^{1-my} \Rightarrow b\left(b^n\right)^{-y} = c\left(c^n\right)^{-y}$

But $b^n = c^n = e,$ so $b = c.$

33 a S_4 has order $4! = 4\times3\times2\times1 = 24,$ since for any permutation there are 4 choices on where to send 1, 3 choices on where to send 2, 2 choices on where to send 3 and then just 1 choice on where to send 4.

33 b We compute the Cayley table of V_4 :

Clearly v_1 is the identity, so the products we need to compute are:

$$v_2 \circ v_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = v_4$$

$$v_3 \circ v_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = v_4$$

$$v_2 \circ v_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = v_3$$

$$v_4 \circ v_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = v_3$$

$$v_3 \circ v_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = v_2$$

$$v_4 \circ v_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = v_2$$

$$v_2 \circ v_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = v_1$$

$$v_3 \circ v_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = v_1$$

$$v_4 \circ v_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = v_1$$

So the Cayley table is

	v_1	v_2	v_3	v_4
v_1	v_1	v_2	v_3	v_4
v_2	v_2	v_1	v_4	v_3
v_3	v_3	v_4	v_1	v_2
v_4	v_4	v_3	v_2	v_1

The table clearly shows the subgroup is closed, has an identity and every element has an inverse. Hence it is a subgroup.

c V_4 is isomorphic to the Klein 4-group K_4.

34 a We compute the orders of the various elements.
Since the order of the group is 8, the possible orders are 1,2,4,8 and 1 has order 1.

Now $7^2 \equiv 19(\bmod 30)$ so $7^3 \equiv 7\times 19(\bmod 30) \equiv 13(\bmod 30)$ so $7^4 \equiv 7\times 13(\bmod 30) \equiv 1(\bmod 30)$ so 7 has order 4.

Now $11^2 \equiv 121(\bmod 30) \equiv 1(\bmod 30)$ so 11 has order 2.

Now $13^2 \equiv 169(\bmod 30) \equiv 19(\bmod 30)$ so $13^3 \equiv 13\times 19(\bmod 30) \equiv 7(\bmod 30)$
so $13^4 \equiv 13\times 7(\bmod 30) \equiv 1(\bmod 30)$ so 13 has order 4

Now $17^2 \equiv 19(\bmod 30)$ so $17^3 \equiv 17\times 19(\bmod 30) \equiv 23(\bmod 30)$ so
$17^4 \equiv 17\times 23(\bmod 30) \equiv 1(\bmod 30)$ so 17 has order 4

Now $19^2 \equiv 361(\bmod 30) \equiv 1(\bmod 30)$ so 19 has order 2

Now $23^2 \equiv 529(\bmod 30) \equiv 19(\bmod 30)$ so $23^4 \equiv 19^2(\bmod 30) \equiv 1(\bmod 30)$ so 23 has order 4

Finally $29^2 \equiv 841(\bmod 30) \equiv 1(\bmod 30)$ so 29 has order 2

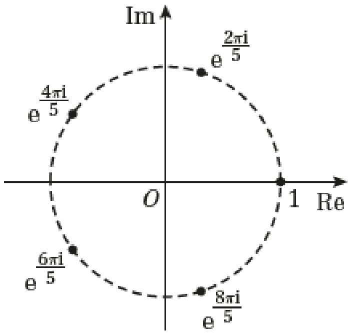
b To find a cyclic subgroup of order 4, we can simply take the cyclic subgroup generated by an element of order 4. For example, taking 7 as the generator gives $H = \{1,7,13,19\}$.

c One may verify by computing the products that $H = \{1,19,29,11\}$ is a subgroup, and since it contains no elements of order 4, it must be isomorphic to the Klein 4-group.

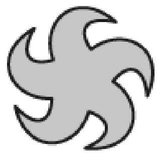
d *H* has element 1 with order 8, whereas *G* contains no elements of order 8.
Therefore *G* is not isomorphic to *H*.

35 a The elements of *G* are $G = \left\{1, e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\right\}$ and hence *G* has order 5.

b



c



36 a Firstly, we find matrices for the rotations by multiples of 90°.
Since these are all generated by a single rotation by 90°, it suffices to find the matrix for this.
The other matrices are then just powers of this matrix.

A clockwise rotation by 90° is represented by the matrix $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

So the other rotations are:

$$a^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$a^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

The identity symmetry has matrix $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

The other four symmetries come from reflections in the horizontal/vertical and two diagonal axes.

A reflection in the x-axis is represented by the matrix $r_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

A reflection in the y-axis is represented by the matrix $r_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

A reflection in the 'North-East' diagonal axis is represented by the matrix $r_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

A reflection in the 'South-East' diagonal axis is represented by the matrix $r_4 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$

b We compute the Cayley table:

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_2	g_2	g_3	g_4	g_1	g_6	g_7	g_8	g_5
g_3	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_4	g_4	g_3	g_1	g_2	g_8	g_5	g_6	g_7
g_5	g_5	g_8	g_7	g_6	g_1	g_4	g_3	g_2
g_6	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_7	g_7	g_6	g_5	g_8	g_3	g_2	g_1	g_4
g_8	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

Closure: All entries in the Cayley table are in H.
Identity: The row and column corresponding to g_1 are the same as the row and column headings, so g_1 is the identity.
Inverse: $g_2^{-1} = g_4$; all other elements are self-inverse.
Associativity assumed
Therefore H forms a group under $\circ$.

36 c The groups are isomorphic, since by viewing the square from part **a** as living in the complex plane we may identify clockwise rotation by 90° with multiplication by $-i$.

This identifies all the rotation matrices with g_2, g_3, g_4, so it remains to identify the reflections.

Reflection in the x-axis can be represented by the function $g_5(z) = z^*$

Reflection in the y-axis can be represented by the function $g_7(z) = -z^*$

Reflection in the 'North East' diagonal axis can be represented by the function $g_6(z) = iz^*$

Reflection in the 'South-East' diagonal axis can be represented by the function $g_8(z) = -iz^*$

Hence this map between the two groups is an isomorphism.

37 a The locus forms a major arc since $\theta = \frac{\pi}{4} < \frac{\pi}{2}$

b Let $z = x + \mathrm{i}y$

Then $\frac{z+\mathrm{i}}{z-\mathrm{i}} = \frac{x+\mathrm{i}(y+1)}{x+\mathrm{i}(y-1)} = \frac{(x+\mathrm{i}(y+1))(x-\mathrm{i}(y-1))}{x^2+(y-1)^2} = \frac{x^2+y^2-1+2\mathrm{i}x}{x^2+(y-1)^2}$

$$= \frac{x^2+y^2-1}{x^2+(y-1)^2} + \mathrm{i}\left(\frac{2x}{x^2+(y-1)^2}\right)$$

Now $\arg\left(\frac{z+\mathrm{i}}{z-\mathrm{i}}\right) = \frac{\pi}{4}$, so $\tan\left(\arg\left(\frac{z+\mathrm{i}}{z-\mathrm{i}}\right)\right) = \tan\frac{\pi}{4} = 1$

Therefore $\dfrac{\frac{2x}{x^2+(y-1)^2}}{\frac{x^2+y^2-1}{x^2+(y-1)^2}} = 1$

$$\frac{2x}{x^2+(y-1)^2} = \frac{x^2+y^2-1}{x^2+(y-1)^2}$$

$$x^2+y^2-1 = 2x$$

$$x^2-2x+y^2-1 = 0$$

$$(x-1)^2-1+y^2-1 = 0$$

$$(x-1)^2+y^2 = 2$$

Hence the centre is at $(1,0)$

38 a A is represented by the complex number $-1+3\mathrm{i}$.

38 b The radius of the circle is given by $\left|\overrightarrow{XA}\right| = \left|-1-2\text{i}-(-1+3\text{i})\right| = |-5\text{i}| = 5$

So the area of the sector is $\frac{1}{2}r^2\theta = \frac{25\pi}{12}$

Substituting $r = 5$ gives $\frac{25\theta}{2} = \frac{25\pi}{12}$

Therefore $\theta = \frac{\pi}{6}$

Now $\overrightarrow{XB} = -5\sin\frac{\pi}{6} + 5\cos\frac{\pi}{6}\text{i} = -\frac{5}{2} + \frac{5\sqrt{3}}{2}\text{i}$

Therefore $b = \overrightarrow{OB} = -1 - 2\text{i} - \frac{5}{2} + \frac{5\sqrt{3}}{2}\text{i}$

$= -\frac{7}{2} + \frac{5\sqrt{3}-4}{2}\text{i}$

39 Let $z = x + \text{i}y$

$|z-1| = \sqrt{2}|z-\text{i}|$

$|(x-1)+\text{i}y| = \sqrt{2}|x+(y-1)\text{i}|$

Squaring the modulus gives

$|x-1+\text{i}y|^2 = 2|x+(y-1)\text{i}|^2$

$(x-1)^2 + y^2 = 2\left(x^2 + (y-1)^2\right)$

$x^2 - 2x + 1 + y^2 = 2x^2 + 2y^2 - 4y + 2$

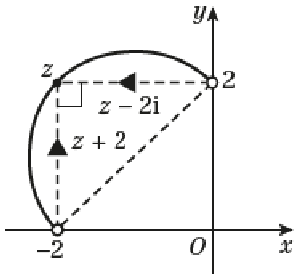
$x^2 + 2x + y^2 - 4y + 1 = 0$

$(x+1)^2 - 1 + (y-2)^2 - 4 + 1 = 0$

$(x+1)^2 + (y-2)^2 = 4$

Hence the circle has radius 2 and centre $(-1, 2)$

40 a

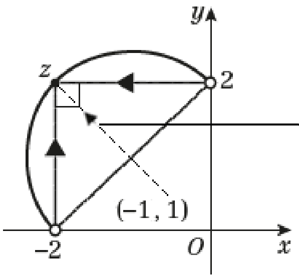


$\arg\left(\frac{z-2\text{i}}{z+2}\right) = \arg(z-2\text{i}) - \arg(z+2) = \frac{\pi}{2}.$

The angles which the vectors make with the positive x-axis differ by a right angle. As drawn here, the difference is $\pi - \frac{\pi}{2} = \frac{\pi}{2}$. The locus of the points, where the difference is a right angle, is a semi-circle, with the line joining –2 on the real axis to 2 on the imaginary axis as diameter.

It is a common error to complete the circle. The lower right hand completion of the circle has equation $\arg\left(\frac{z-2\text{i}}{z+2}\right) = -\frac{\pi}{2}$.

40 b



The dotted line represents the complex number $z+1-\mathrm{i}=z-(-1+\mathrm{i})$. The length of this vector is the radius of the circle.

The diameter of the circle is given by $d^2=2^2+2^2=8$, so $d=2\sqrt{2}$

Therefore $|z+1-\mathrm{i}|=\dfrac{2\sqrt{2}}{2}=\sqrt{2}$

41 a Both loci L and M are circles, hence they are similar

41 b Computing the scale factor of enlargement amounts to computing the radii of both circles.

For L we have:

$$
\begin{aligned}
&|z-4|=\sqrt{5}|z+2\mathrm{i}| \\
&|(x-4)+\mathrm{i}y|=\sqrt{5}|x+(y+2)\mathrm{i}| \\
&|(x-4)+\mathrm{i}y|^2=5|x+(y+2)\mathrm{i}|^2 \\
&(x-4)^2+y^2=5\left(x^2+(y+2)^2\right) \\
&x^2-8x+16+y^2=5x^2+5y^2+20y+20 \\
&4x^2+8x+4y^2+20y+4=0 \\
&x^2+2x+y^2+5y+1=0 \\
&(x+1)^2-1+\left(y+\frac{5}{2}\right)^2-\frac{25}{4}+1=0
\end{aligned}
$$

Which simplifies to

$$(x+1)^2+\left(y+\frac{5}{2}\right)^2=\frac{25}{4}$$

Hence the radius of L is $\frac{5}{2}$

For M we have:

$$
\begin{aligned}
&|z-6|=\sqrt{7}|z+6\mathrm{i}| \\
&|(x-6)+\mathrm{i}y|=\sqrt{7}|x+\mathrm{i}(y+6)| \\
&|(x-6)+\mathrm{i}y|^2=7|x+(y+6)\mathrm{i}|^2 \\
&(x-6)^2+y^2=7x^2+7(y+6)^2 \\
&x^2-12x+36+y^2=7x^2+7y^2+84y+252 \\
&6x^2+12x+6y^2+84y+216=0 \\
&x^2+2x+y^2+14y+36=0 \\
&(x+1)^2-1+(y+7)^2-49+36=0 \\
&(x+1)^2+(y+7)^2=14
\end{aligned}
$$

Hence this circle has radius $\sqrt{14}$

So the scale factor of enlargement is $\frac{\sqrt{14}}{\frac{5}{2}}=\frac{2\sqrt{14}}{5}$

42 The locus is given by

$$\arg\left(\frac{z+1}{z}\right)=\frac{\pi}{4}$$

Substituting $z=x+\mathrm{i}y$

$$\frac{z+1}{z}=\frac{x+1+\mathrm{i}y}{x+\mathrm{i}y}=\frac{(x+1+\mathrm{i}y)(x-\mathrm{i}y)}{(x+\mathrm{i}y)(x-\mathrm{i}y)}=\frac{x^2+x+\mathrm{i}xy-\mathrm{i}xy-\mathrm{i}y+y^2}{x^2+y^2}$$

$$=\frac{x^2+x+y^2-\mathrm{i}y}{x^2+y^2}=\frac{x^2+x+y^2}{x^2+y^2}+\frac{-y}{x^2+y^2}\mathrm{i}$$

Now $\arg\left(\frac{z+1}{z}\right)=\frac{\pi}{4}$, so $\tan\left(\arg\left(\frac{z+1}{z}\right)\right)=\tan\frac{\pi}{4}=1$

So $\dfrac{\frac{-y}{x^2+y^2}}{\frac{x^2+x+y^2}{x^2+y^2}}=1$

$$-y=x^2+x+y^2$$

$$x^2+x+y^2+y=0$$

$$\left(x+\frac{1}{2}\right)^2-\frac{1}{4}+\left(y+\frac{1}{2}\right)^2-\frac{1}{4}=0$$

$$\left(x+\frac{1}{2}\right)^2+\left(y+\frac{1}{2}\right)^2=\frac{1}{2}$$

So the centre of the circle is $\left(-\frac{1}{2},-\frac{1}{2}\right)$ and the radius is $\frac{1}{\sqrt{2}}$

Therefore, this is the major arc of a circle.

The length of the curve required is $r(2\pi-\theta)$, where θ is the angle between the lines connecting the endpoints of the arc to the centre of the circle.

Geometrically we can see that $\tan\frac{\theta}{2}=\frac{\frac{1}{2}}{\frac{1}{2}}=1$, so $\theta=\frac{\pi}{2}$

Therefore the length of the arc is $\frac{1}{\sqrt{2}}\left(2\pi-\frac{\pi}{2}\right)=\frac{1}{\sqrt{2}}\left(\frac{3\pi}{2}\right)=\frac{3\pi}{2\sqrt{2}}$

43 We consider the locus $|z-\mathrm{i}|=\sqrt{p}|z+1|$

Squaring gives $|z-\mathrm{i}|^2=p|z+1|^2$

Substituting $z=x+\mathrm{i}y$:

$$|x+(y-1)\mathrm{i}|^2=p|(x+1)+\mathrm{i}y|^2$$
$$x^2+(y-1)^2=p\left((x+1)^2+y^2\right)$$
$$x^2+y^2-2y+1=px^2+2px+p+py^2$$
$$(p-1)x^2+2px+2y+(p-1)y^2+p-1=0$$
$$x^2+\frac{2px}{p-1}+y^2+\frac{2y}{p-1}+1=0$$
$$\left(x+\frac{p}{p-1}\right)^2-\frac{p^2}{(p-1)^2}+\left(y+\frac{1}{p-1}\right)^2-\frac{1}{(p-1)^2}+1=0$$
$$\left(x+\frac{p}{p-1}\right)^2+\left(y+\frac{1}{p-1}\right)^2=\frac{p^2}{(p-1)^2}+\frac{1}{(p-1)^2}-1$$
$$\left(x+\frac{p}{p-1}\right)^2+\left(y+\frac{1}{p-1}\right)^2=\frac{p^2+1-(p-1)^2}{(p-1)^2}$$
$$\left(x+\frac{p}{p-1}\right)^2+\left(y+\frac{1}{p-1}\right)^2=\frac{2p}{(p-1)^2}$$

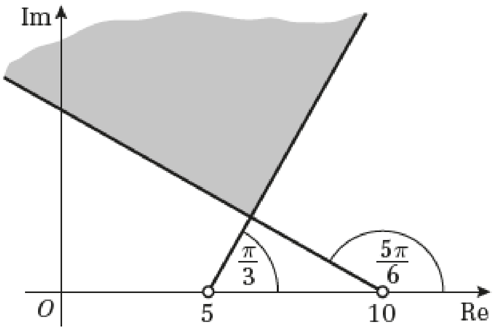
Hence the radius is $\dfrac{\sqrt{2p}}{p-1}$

For a circumference of 24π the radius is 12

Hence $\dfrac{\sqrt{2p}}{p-1}=12$

$$2p=(12p-12)^2$$

44



45 a The locus is given by the inequalities $|z-6\text{i}|\leqslant 2|z-3|$ and $\text{Re}(z)\leqslant k$

Taking the first inequality:

$|z-6\text{i}|^2\leqslant 4|z-3|^2$

$|x+(y-6)\text{i}|^2\leqslant 4|x-3+\text{i}y|^2$

$x^2+(y-6)^2\leqslant 4\left((x-3)^2+y^2\right)$

$x^2+y^2-12y+36\leqslant 4x^2-24x+36+4y^2$

$0\leqslant 3x^2-24x+3y^2+12y$

$0\leqslant x^2-8x+y^2+4y$

$x^2-8x+y^2+4y\geqslant 0$

$(x-4)^2-16+(y+2)^2-4\geqslant 0$

$(x-4)^2+(y+2)^2\geqslant 20$

Hence the circle has centre $(4,-2)$

Hence, for a semi-circle, we should take $k=4$

b The area of the semicircle is $\dfrac{\pi r^2}{2}=\dfrac{\pi\times 20}{2}=10\pi$

46 The line corresponding to $|z-p|=|z-q|$ is given by the perpendicular bisector of p and q, that is $x=\dfrac{p+q}{2}$

The area of the triangular region is therefore $\dfrac{1}{2}\times\left(\dfrac{q-p}{2}\right)^2=x$

So $(q-p)^2=8x$

$q-p=\sqrt{8x}$

So $q=p+\sqrt{8x}$, as required

47 a The transformation defined by $w=3z+4-2\text{i}$ represents a scaling by 3, followed by a translation by the complex number $4-2\text{i}$.

The translation leaves the area of the triangle invariant.

Therefore the new area is $3^2\times 8=72$.

b We consider what happens to the line $\text{Im}(z)=4$ under the transformation.

Consider a point $z=x+4\text{i}$ on the line.

This is mapped to $w=3(x+4\text{i})+4-2\text{i}=3x+4+10\text{i}$.

Hence the line is mapped to the line $\text{Im}(z)=10$.

48 $w = \dfrac{2z-1}{z-2} \Rightarrow wz - 2w = 2z - 1$

$$wz - 2z = 2w - 1 \Rightarrow z(w-2) = 2w - 1$$

$$z = \frac{2w-1}{w-2}$$

$$|z| = 1 \Rightarrow \left|\frac{2w+1}{w-2}\right| = 1$$

You know that $|z| = 1$ and you are trying to find out about w. So it is a good idea to change the subject of the formula to z. You can then put the modulus of the right hand side of the new formula, which contains w, equal to 1.

$$|2w-1| = |w-2|$$

It is not easy to interpret this locus geometrically and so it is sensible to transform the problem into algebra, using the rule that if $z = x + \mathrm{i}y$, then $|z|^2 = x^2 + y^2$.

Let $w = u + \mathrm{i}v$

$$|2(u+\mathrm{i}v) - 1| = |u + \mathrm{i}v - 2|$$

$$|(2u-1) + \mathrm{i}2v| = |(u-2) + \mathrm{i}v|$$

$$|(2u-1) + \mathrm{i}2v|^2 = |(u-2) + \mathrm{i}v|^2$$

$$(2u-1)^2 + 4v^2 = (u-2)^2 + v^2$$

$$4u^2 - 4u + 1 + 4v^2 = u^2 - 4u + 4 + v^2$$

$$3u^2 + 3v^2 = 3 \Rightarrow u^2 + v^2 = 1$$

This is a circle centre O, radius 1 and has the equation $|w| = 1$ in the Argand plane.

Hence, the circle $|z| = 1$ is mapped onto the circle $|w| = 1$, as required.

49 a $z = x + \frac{1}{2}\text{i}$

The real part of a complex number on Im $z = \frac{1}{2}$ can have any real value, which you can represent by the symbol x, but the imaginary part must be $\frac{1}{2}$.

$$w = \frac{z - \text{i}}{z}$$

$$zw = z - \text{i} \Rightarrow z - wz = \text{i}$$

$$z = \frac{\text{i}}{1 - w}$$

Let $w = u + \text{i}v$

$$x + \frac{1}{2}\text{i} = \frac{\text{i}}{1 - u - \text{i}v}$$

Multiplying the numerator and denominator by $1 - u + \text{i}v$

Multiply the numerator and the denominator of the right hand side by the conjugate complex of $1 - u - \text{i}v$ which is $1 - u + \text{i}v$.

$$x + \frac{1}{2}\text{i} = \frac{\text{i}(1 - u + \text{i}v)}{(1 - u)^2 + v^2},$$

$$= \frac{-v}{(1 - u)^2 + v^2} + \frac{1 - u}{(1 - u)^2 + v^2}\text{i}$$

Equating imaginary parts

$$\frac{1}{2} = \frac{1 - u}{u^2 - 2u + 1 + v^2}$$

You are aiming at $|w| = 1$. If $w = u + \text{i}v$, this is the equivalent to $u^2 + v^2 = 1$. So that is the expression you are looking for.

$$u^2 - 2u + 1 + v^2 = 2 - 2u$$

$$u^2 + v^2 = 1$$

$u^2 + v^2 = 1$ is a circle centre O, radius 1.

Hence the line, Im $z = \frac{1}{2}$ is mapped onto the circle with equation $|w| = 1$.

49 b The transformation $w' = \frac{z - \mathrm{i}}{z}$ maps the line $\operatorname{Im} z = \frac{1}{2}$ onto the circle with centre O and radius 1.

The first transformation is the transformation in part **a**.

The transformation $w'' = 2w'$ maps the circle with centre O and radius 1 onto the circle with centre O and radius 2.

The transformation $z \mapsto kz$ increases the radius of the circle by a factor of k. This transformation is an enlargement, factor k, centre of enlargement O.

The transformation $w = w'' + 3 - \mathrm{i}$ maps the circle with centre O and radius 2 onto the circle with centre $3 - \mathrm{i}$ and radius 2.

The transformation $z \mapsto z + a$ maps a circle centre O to a circle centre a. This transformation is a translation.

Combining the transformations

$$w = 2\left(\frac{z - \mathrm{i}}{z}\right) + 3 - \mathrm{i}$$

$$= \frac{2z - 2\mathrm{i} + 3z - \mathrm{i}z}{z}$$

$$= \frac{(5 - \mathrm{i})z - 2\mathrm{i}}{z}$$

50 a If $z = x + \mathrm{i}y$, then $\arg z = \frac{\pi}{4} \Rightarrow \frac{y}{x} = 1$

Let $x = y = \lambda$

$$w = \frac{\lambda + \lambda\mathrm{i} + 1}{\lambda + \lambda\mathrm{i} + \mathrm{i}} = \frac{(\lambda + 1) + \lambda\mathrm{i}}{\lambda + (\lambda + 1)\mathrm{i}}$$

$$|w| = \left|\frac{(\lambda + 1) + \lambda\mathrm{i}}{\lambda + (\lambda + 1)\mathrm{i}}\right| = \frac{|(\lambda + 1) + \lambda\mathrm{i}|}{|\lambda + (\lambda + 1)\mathrm{i}|}$$

$$= \frac{\left((\lambda + 1)^2 + \lambda^2\right)^{\frac{1}{2}}}{\left(\lambda^2 + (\lambda + 1)^2\right)^{\frac{1}{2}}} = 1$$

For all complex numbers a and b, $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$

Hence the points on $\arg z = \frac{\pi}{4}$ map, under T, onto points on the circle $|w| = 1$.

As $\lambda > 0$, the image would only be part of this circle but the wording of the question does not require you to be more specific. You are only required to show that the image points are points on the circle; not all of the points on the circle. (The image is, in fact, just the lower right quadrant of the circle.)

50 b $wz + w\mathrm{i} = z + 1$

$$wz - z = 1 - \mathrm{i}w$$

$$z = \frac{1 - \mathrm{i}w}{w - 1}$$

$$|z| = \frac{|1 - \mathrm{i}w|}{|w - 1|} = 1$$

Hence $|1 - \mathrm{i}w| = |w - 1|$

This is the image under T of $|z| = 1$ but it is difficult to interpret and part **c** would be difficult without some further working.

$$|1 - \mathrm{i}w| = |-\mathrm{i}(w + 1)| = |-\mathrm{i}||w + \mathrm{i}| = 1 \times |w + \mathrm{i}| = |w + \mathrm{i}|$$

The image of $|z| = 1$ in the z-plane is

$$|w + \mathrm{i}| = |w - 1|$$

in the w-plane.

This is the locus of points equidistant from the points in the Argand plane representing –i and one. That is the perpendicular bisector of $(0, -1)$ and $(1, 0)$.

Writing $w = u + \mathrm{i}v$:

$$|u + \mathrm{i}v + \mathrm{i}| = |u + \mathrm{i}v - 1|$$

$$|u + (v + 1)\mathrm{i}| = |(u - 1) + \mathrm{i}v|$$

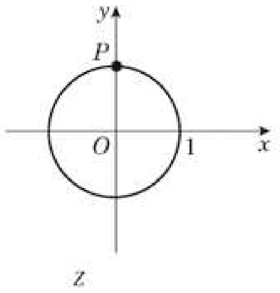
$$|u + (v + 1)\mathrm{i}|^2 = |(u - 1) + \mathrm{i}v|^2$$

$$u^2 + (v + 1)^2 = (u - 1)^2 + v^2$$

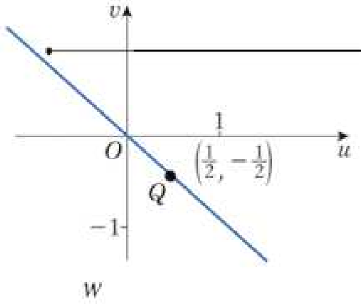
$$u^2 + v^2 + 2v + 1 = u^2 - 2u + 1 + v^2$$

So $v = -u$

c, d



$$z = \mathrm{i} \Rightarrow w = \frac{1 + \mathrm{i}}{2\mathrm{i}} = \frac{\mathrm{i} + 1}{2\mathrm{i}} = \frac{1}{2} - \frac{1}{2}\mathrm{i}$$



The perpendicular bisector of $(0, -1)$ and $(1, 0)$ is the line $v = -u$.

51 a $z = a^{-1}e^{i\theta}$

b Let $z = a^{-1}e^{i\theta}$ then we have $w = az + \frac{1}{z} = e^{i\theta} + ae^{-i\theta}$

$= \cos\theta + \mathrm{i}\sin\theta + a(\cos\theta - \mathrm{i}\sin\theta)$

$= (1+a)\cos\theta + (1-a)\mathrm{i}\sin\theta$

$= u + \mathrm{i}v$

Hence $u = (1+a)\cos\theta$ and $v = (1-a)\sin\theta$

$$\left(\frac{u}{1+a}\right)^2 + \left(\frac{v}{1-a}\right)^2 = 1$$

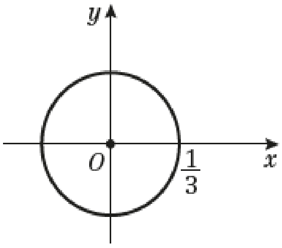
$$u^2(1-a)^2 + v^2(1+a)^2 = (1+a)^2(1-a)^2$$

$$u^2(1-a)^2 + v^2(1+a)^2 = \left[(1+a)(1-a)\right]^2$$

$$u^2(1-a)^2 + v^2(1+a)^2 = (1-a^2)^2$$

as required

c This ellipse corresponds to the case $a = 3$, hence the points on the z-plane that are transformed to the ellipse are those such that $|z| = \frac{1}{3}$



Challenge

1 We wish to find integers *a*, *b*, *c* such that $91a+65b+35c=1$.
Firstly note that no two pairs of these numbers are coprime, which will force *a*, *b*, *c* to all be non-zero.

Firstly, $\gcd(65,35)=5$, so we can find integers p and q such that $65p+35q=5$.
Since $\gcd(5,91)=1$, we can find integers *s*, *t* such that $5s+91t=1$.
Carrying out the first application of the Euclidean algorithm gives

$$65=35+30$$
$$35=30+5$$
$$30=6\times5$$

So working in reverse gives

$$5=35-30$$
$$5=35-(65-35)$$
$$5=2\times35-65$$

Now we carry out the Euclidean algorithm on 5 and 91 giving $1=91-18\times5$

Hence $1=91-18\times5=91-18\times(2\times35-65)=1\times91-36\times35+18\times65$

Therefore we can choose $a=1,\ b=18,\ c=-36.$

2 We wish to prove that there are infinitely many primes congruent to 3 mod 4.
Suppose this were not true.
Then there would only be finitely many prime numbers congruent to 3 mod 4.
Call these prime numbers $p_1, p_2, ..., p_n$.
Now consider the number $N=4p_1p_2...p_n-1$.
This is clearly congruent to 3 mod 4, and by construction is not divisible by any of the p_k.
Hence all the prime factors of *N* must be congruent to 1 mod 4 (since are not even) and *N* is a product of all its prime factors.
However, the product of a sequence of numbers congruent to 1 mod 4 is itself congruent to 1 mod 4.
Hence *N* must be congruent to *N* mod 4.
This is a contradiction, meaning that our initial assumption is false.
Therefore there must be infinitely many primes congruent to 3 modulo 4.

3 **a** Suppose every element of *G* has order 2 or less and let $a,b\in G$.
Then $e=(ab)^2=(ab)(ab)$
Therefore $ba=(ab)(ab)(ba)$
$=abab^2a$
$=aba^2$ since $b^2=e$
$=ab$ since $a^2=e$
Hence *G* is abelian.

Challenge

3 b We can simply compute the Cayley table giving:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Note that every element has order 2 so is self-inverse and the group operation is closed.
Hence it is a subgroup.

c Let G be a non-cyclic subgroup of order $2p$ with p an odd prime.
Suppose there is no element of order p.
The only factors of $2p$ are $1, 2, p$ and $2p$
Therefore every element has order 2.
Hence G is abelian and since $|G| \geqslant 2 \times 3 = 6,$ there must exist distinct elements $e, a, b \in G$.
By part b we have that $H = \{e, a, b, ab\}$ is a subgroup of G, but the order of H is 4 which does not divide $2p$, the order of G.
Hence by Lagrange, we have a contradiction.
Therefore G must contain an element of order p.