

Topic 16 · Sheet A: Worked answers and mark scheme

Group actions, orbits, fields and linear congruences

Suggested time

About 75 minutes

Total marks

76

Questions

12

Builds on

Topics 1 to 15

How marks are awarded. Each mark has a code, as on most UK exam papers.

B A mark for a correct statement or value on its own. It does not depend on any other mark.

M A method mark, for a correct approach, even if the final answer is wrong.

A An accuracy mark, for the correct answer *after* a correct method. It cannot be awarded without the M mark before it.

E An explanation mark, for a clear reason in words. A correct reason that is worded differently scores in full.

For true or false questions, the mark is for the correct decision; where a reason is asked for, it must be the right reason.

1 Action or not?

4 marks

(a) **Yes:** $0 \cdot x = x$ and $m \cdot (n \cdot x) = x + n + m = (m + n) \cdot x$.

(b) **Yes:** $(-1)^k$ depends only on $[k]_2$, $(-1)^0 x = x$, and $(-1)^j (-1)^k x = (-1)^{j+k} x$.

(c) **No:** the identity 0 gives $0 \cdot x = 0 \neq x$ when $x \neq 0$. (d) **Yes:** this is the trivial action.

B1 each part, naming the failing property in (c)

4

Common mistake In (b) and (c) the group is additive, so the second rule reads $g \cdot (h \cdot x) = (g + h) \cdot x$, not $(gh) \cdot x$.

2 Days of the week

4 marks

(a) **Mon.** (b) $10 = 7 + 3$, so **Thu.** (c) **Sun.** (d) Every day is reached from Wed, so the orbit is **all of X** , and there is **one orbit**.

B1 each part correct

4

Why this question The days of the week are a classic first example. The action only depends on n modulo 7, which links it to $\mathbb{Z}/7\mathbb{Z}$ from Topic 8.

3 The permutation action

6 marks

- (a) $\sigma(0) = 1, \sigma(1) = 3, \sigma(3) = 0, \sigma(2) = 4, \sigma(4) = 2$. So $y_1 = a, y_3 = b, y_0 = d, y_4 = c, y_2 = e$:
 $\sigma \cdot x = (d, a, e, b, c)$.
- (b) $\sigma^{-1} = (0\ 3\ 1)(2\ 4)$, one-line $[3\ 0\ 4\ 1\ 2]$. Then $y_0 = x_3 = d, y_1 = x_0 = a, y_2 = x_4 = e$,
 $y_3 = x_1 = b, y_4 = x_2 = c$. **It agrees.**
- (c) $(0\ 1) \cdot (x, y, z) = (y, x, z)$ and $(0\ 2\ 1) \cdot (x, y, z) = (y, z, x)$.
- (d) Left: $(1\ 2) \cdot (x, y, z) = (x, z, y)$, then $(0\ 1) \cdot (x, z, y) = (z, x, y)$. Right: $(0\ 1)(1\ 2) = (0\ 1\ 2)$,
and $(0\ 1\ 2) \cdot (x, y, z) = (z, x, y)$. **They agree.**

M1	(a) placing x_i in position $\sigma(i)$	1
A1	(a)	1
B1	(b)	1
B1	(c) $(0\ 1)$	1
B1	(c) $(0\ 2\ 1)$	1
B1	(d)	1

Common mistake Using $y_i = x_{\sigma(i)}$ instead. That rule is not an action at all. In (c) it would swap the answers for the two 3-cycles.

4 Orbits in the plane

6 marks

- (a) $\{(0,0)\}$: the origin is a fixed point.
- (b) $\{(1,0), (0,1), (-1,0), (0,-1)\}$.
- (c) $\{(1,1), (-1,1), (-1,-1), (1,-1)\}$.
- (d) $\{(\pm 2, \pm 1), (\pm 1, \pm 2)\}$, all eight sign choices: 8 points.
- (e) The orbits are $\{x, -x\}$, and the only fixed point is 0.

B1	(a)	1
B1	(b)	1
B1	(c)	1
M1	(d) applying rotations and reflections	1
A1	(d) all eight points	1
B1	(e)	1

Why this question Orbit sizes here are 1, 4, 4 and 8. Points on a mirror line, like $(1,0)$ and $(1,1)$, are fixed by a reflection, so their orbits are smaller than $|D_8|$.

5 Triples summing to 3

6 marks

- (a) $(0, 0, 3), (0, 1, 2), (0, 2, 1), (0, 3, 0), (1, 0, 2), (1, 1, 1), (1, 2, 0), (2, 0, 1), (2, 1, 0), (3, 0, 0)$.
- (b) $(0\ 1\ 2) \cdot (x, y, z) = (z, x, y)$, so we get $(0, 2, 1)$, and $0 + 2 + 1 = 3$. **Yes.**
- (c) $\{(3, 0, 0), (0, 3, 0), (0, 0, 3)\}$, **the six permutations of $(2, 1, 0)$, and $\{(1, 1, 1)\}$.**
- (d) **Only $(1, 1, 1)$.**

B2	(a) all ten. <i>B1 for eight or nine</i>	2
B1	(b)	1
B2	(c) all three orbits. <i>B1 for two</i>	2
B1	(d)	1

Why this question The permutation action only reorders the entries, so the orbit of a triple is all its rearrangements. This warms up for question 11.

6 More orbits

6 marks

- (a) **No:** $g + h = h$ forces $g = 0$, so the orbit of h is all of C_4 .
- (b) The orbits are the cosets of H : $\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6, 10\}, \{3, 7, 11\}$.
- (c) **All of $\mathbb{Z}_4$.**
- (d) $\{0, 1\}$ **and** $\{2, 3\}$.
- (e) Orbits $\{0, 1, 2\}$ **and** $\{3\}$; the fixed point is 3.

B1	(a)	1
B2	(b) all four. <i>B1 for two or three</i>	2
B1	(c)	1
B1	(d)	1
B1	(e)	1

Why this question Part (b) shows cosets from Topic 15 as orbits of an action. Parts (d) and (e) show the orbits of a single permutation are exactly its cycles from Topic 14. Orbits of any action always form a partition, which is the common pattern here.

7 Field or not?

6 marks

- (a) **No:** no additive inverses, e.g. for 1. (b) **No:** 2 has no multiplicative inverse. (c) **Yes.**
- (d) **No:** $[2]_6 \times [3]_6 = [0]_6$, so the non-zero classes are not closed under $\times$. (e) **Yes:** 7 is prime.
- (f) **Yes:** 2 is prime.

B1	each part, with a reason for each “no”	6
-----------	--	---

Why this question One theorem settles (d), (e) and (f) at once: $\mathbb{Z}/n\mathbb{Z}$ is a field exactly when n is prime.

8 Inverses in finite fields

6 marks

- (a) $2 \cdot 6 = 12$, $3 \cdot 4 = 12$, $7 \cdot 8 = 56 = 55 + 1$. So $[6]_{11}$, $[4]_{11}$, $[8]_{11}$.
- (b) $19 = 2 \cdot 7 + 5$, $7 = 1 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0$, so $N = 4$. Backwards from $(C_4, D_4) = (0, 1)$: $(1, 0)$, $(2, 1)$, $(3, 2)$, $(C_0, D_0) = (8, 3)$. So $19 \cdot 3 - 7 \cdot 8 = 1$, and $7 \cdot (-8) \equiv 1$: $[11]_{19}$. Check: $77 = 4 \cdot 19 + 1$.
- (c) $-1 = [6]_7$, and $6 \cdot 6 = 36 = 35 + 1$, so $[6]_7 \times [6]_7 = [1]_7$.

B1	(a) each inverse	3
M1	(b) both algorithms	1
A1	(b)	1
B1	(c)	1

Why this question Trial and error needs up to n multiplications. The algorithm in (b) needs only a few steps, which matters for large n .

9 Linear congruences

7 marks

- (a) $[4]_7^{-1} = [2]_7$, so $x \equiv 2$: $[2]_7$.
- (b) $[3]_7^{-1} = [5]_7$, so $x \equiv 25 \equiv 4$: $[4]_7$.
- (c) $[5]_{11}^{-1} = [9]_{11}$, as $45 = 44 + 1$. So $x \equiv 27 \equiv 5$: $[5]_{11}$.
- (d) $[7]_{13}^{-1} = [2]_{13}$, as $14 = 13 + 1$. So $x \equiv 8$: $[8]_{13}$. Check: $7 \cdot 8 = 56 = 4 \cdot 13 + 4$.

B1	(a)	1
B1	(b)	1
M1	(c) inverse of 5	1
A1	(c)	1
M1	(d) inverse of 7	1
A1	(d)	1
B1	(d) check	1

Common mistake Dividing by a as if working in $\mathbb{R}$. In $\mathbb{Z}/n\mathbb{Z}$ you multiply by the inverse of a ; check your answer by substituting it back in.

10 When the gcd is not 1

7 marks

- (a) $4x \bmod 6$ for $x = 0, \dots, 5$: 0, 4, 2, 0, 4, 2. So $x \in \{2, 5\}$: $[2]_6 \cup [5]_6$, which is $[2]_3$.
- (b) From the list in (a), $4x \bmod 6$ is always 0, 2 or 4, never 3. **No solutions.**
- (c) $9x \bmod 15$ equals 6 for $x = 4, 9, 14$: the solutions are $[4]_{15} \cup [9]_{15} \cup [14]_{15} = [4]_5$.

M1	(a) checking every x	1
A1	(a)	1
E2	(b) a complete reason. <i>E1 for an incomplete one</i>	2
M1	(c) checking every x	1
A1	(c) $x = 4, 9, 14$	1
A1	(c) $[4]_5$	1

Why this question This goes beyond the case $\gcd(a, n) = 1$. Notice that solutions exist exactly when $\gcd(a, n)$ divides b : $\gcd(4, 6) = 2$ divides 2 but not 3.

11 Exam style: orbits in $\Delta(6)$

9 marks

- (a) For $a = 0, \dots, 6$ there are $7 - a$ choices of b , then c is fixed: $7 + 6 + 5 + 4 + 3 + 2 + 1 = 28$.
- (b) $(6, 0, 0)$: 3; $(5, 1, 0)$: 6; $(4, 2, 0)$: 6; $(4, 1, 1)$: 3; $(3, 3, 0)$: 3; $(3, 2, 1)$: 6; $(2, 2, 2)$: 1. That is 7 orbits.
- (c) $3 + 6 + 6 + 3 + 3 + 6 + 1 = 28$. **They agree**, because the orbits form a partition of $\Delta(6)$.
- (d) **Only** $(2, 2, 2)$.

M1	(a) a systematic count	1
A1	(a)	1
B4	(b) all seven orbits with sizes. <i>B3 for six; B2 for four or five; B1 for two or three</i>	4
B1	(c) sum	1
E1	(c) partition	1
B1	(d)	1

Why this question Orbit sizes 1, 3 and 6 all divide $|\text{Sym}(3)| = 6$. Orbits correspond to ways of writing 6 as a sum of three natural numbers, ignoring order.

12 Exam style: a larger congruence

9 marks

- (a) **43 is prime**, so $\mathbb{Z}/43\mathbb{Z}$ is a field and $[17]_{43}$ has an inverse. Multiplying by it gives exactly one class.
- (b) $43 = 2 \cdot 17 + 9$, $17 = 1 \cdot 9 + 8$, $9 = 1 \cdot 8 + 1$, $8 = 8 \cdot 1 + 0$. So $q = (2, 1, 1, 8)$, $N = 4$, $\gcd = 1$.

- (c) From $(C_4, D_4) = (0, 1)$: $(C_3, D_3) = (1, 0)$, $(C_2, D_2) = (1, 1)$, $(C_1, D_1) = (2, 1)$, $(C_0, D_0) = (5, 2)$. So $c = 5$, $d = 2$: $86 - 85 = 1$.
- (d) $17 \cdot (-5) \equiv 1$, so $[17]_{43}^{-1} = [38]_{43}$.
- (e) $x \equiv 38 \cdot 5 = 190 = 4 \cdot 43 + 18$: $x \in [18]_{43}$. Check: $17 \cdot 18 = 306 = 7 \cdot 43 + 5$.

B1	(a)	1
M1	(b) divisions	1
A1	(b)	1
M1	(c) backwards run with $D_4 = 1$	1
A1	(c) the table	1
A1	(c) $c = 5$, $d = 2$	1
B1	(d)	1
A1	(e) solution	1
B1	(e) check	1

Why this question This brings together Topic 8 (congruences), Topic 12 (the euclidean algorithm) and the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field. It is a fitting last question for the module.

Total: 76 marks. Spotted a mistake? Report it at unimixedtutor.com and we will fix it.