

Topic 8 · Sheet A: Worked answers and mark scheme

Modular arithmetic and linear congruences

Suggested time

About 75 minutes

Total marks

75

Questions

12

Builds on

Topics 1 to 7

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 Divisors

4 marks

(a) **Yes:** $91 = 13 \times 7$. (b) **No:** $26/(-4) = -6.5$ is not an integer. (c) **1, 2, 3, 4, 6, 9, 12, 18, 36.** (d) **No:** $k \times 0 = 0 \neq 5$ for every k .

B1 each part correct

4

Why this question Part (d) shows that zero divides only itself.

2 Checking congruences

4 marks

(a) **Yes:** $17 - 2 = 15 = 3 \times 5$. (b) **No:** $-3 - 11 = -14$ is not a multiple of 6. (c) **Yes:** $99 = 11 \times 9$. (d) **No:** 21 is not a multiple of 6.

B1 each part, with the difference checked

4

Why this question Always test a congruence by its definition: subtract, then check for a multiple of the modulus.

3 Least residues

5 marks

(a) $47 = 7 \times 6 + 5$: 5. (b) $-13 = -3 \times 5 + 2$: 2. (c) $1000 = 142 \times 7 + 6$: 6. (d) $2^5 = 32 \equiv -1$, so $2^{10} \equiv 1$: 1. (e) $3 \equiv -1 \pmod{4}$, so $3^{100} \equiv (-1)^{100} = 1$: 1.

B1 each part correct

5

Common mistake In (b), giving -3 or 3 . The answer must lie in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, and $-13 + 15 = 2$.

4 Congruence classes

6 marks

- (a) For example $-11, -4, 3, 10, 17$.
(b) **Yes**: $17 - (-8) = 25$.
(c) **No**: $17 - (-7) = 24$.
(d) $[0]_4, [1]_4, [2]_4, [3]_4$.
(e) **12**.
(f) **One class**, $[0]_1 = \mathbb{Z}$: every integer is a multiple of 1.

B1 each part correct

6

Why this question $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$ is a whole infinite set. Two classes are equal exactly when their representatives are congruent, which is why $[17]_5$ and $[-8]_5$ are the same set.

5 Arithmetic in $\mathbb{Z}/n\mathbb{Z}$

6 marks

(a) $[9]_6 = [3]_6$. (b) $[20]_6 = [2]_6$. (c) $[-2]_6 = [4]_6$.

(d) Writing r for $[r]_4$:

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

B1 (a)

1

B1 (b)

1

B1 (c)

1

B3 (d) all 16 entries. B2 for 14 or 15; B1 for 12 or 13

3

Why this question The table shows that $[2]_4 \times [2]_4 = [0]_4$: in $\mathbb{Z}/4\mathbb{Z}$ two non-zero classes can multiply to zero, which never happens in $\mathbb{Z}$.

6 Multiplying to one, and to zero

6 marks

- (a) Check $a = 0, \dots, 6$: $3 \times 5 = 15 \equiv 1$. $[a]_7 = [5]_7$.
- (b) $2a$ is always even, so $2a \equiv 0, 2, 4, 6 \pmod{8}$ and never 1. Checking all eight $a \in \mathbb{[8]}$ confirms it. **No solution.**
- (c) For example $[2]_6 \times [3]_6 = [6]_6 = [0]_6$ (also $[3]_6 \times [4]_6$).

M1	(a) systematic checking	1
A1	(a) $[5]_7$	1
M1	(b) $2a$ is even, or all eight cases	1
A1	(b) conclusion	1
B2	(c) a correct pair	2

Why this question Parts (a) and (b) preview Topic 16: dividing by $[3]_7$ works, dividing by $[2]_8$ does not. The difference is that 3 and 7 share no factor, while 2 and 8 do.

7 Solving linear congruences

6 marks

- (a) Check $x \in \mathbb{[5]}$: only $3 \times 3 = 9 \equiv 4$. Solutions $[3]_5$.
- (b) Check $x \in \mathbb{[6]}$: $4 \times 2 = 8 \equiv 2$ and $4 \times 5 = 20 \equiv 2$. Solutions $[2]_6 \cup [5]_6$, which is $[2]_3$.
- (c) Check $x \in \mathbb{[9]}$: $x = 2, 5, 8$ give 12, 30, 48, all $\equiv 3$. Solutions $[2]_9 \cup [5]_9 \cup [8]_9$, which is $[2]_3$.

M1	(a) checking all of $\mathbb{[5]}$	1
A1	(a)	1
M1	(b) checking all of $\mathbb{[6]}$	1
A1	(b) both classes	1
M1	(c) checking all of $\mathbb{[9]}$	1
A1	(c) all three classes	1

Common mistake Stopping at the first solution. A linear congruence can have several solutions in $\mathbb{[n]}$, so check every case.

8 When there are no solutions, or many

6 marks

- (a) $2x$ is even, and $5 + 8k$ is odd for every k , so they are never equal. **No solutions.**
- (b) $5x$ is a multiple of 10 exactly when x is even: $[0]_2$.
- (c) **4**: $x = 2, 5, 8, 11$.

M1	(a) parity argument	1
A1	(a) conclusion	1
M1	(b)	1
A1	(b) the even integers	1
M1	(c) checking $\llbracket 12 \rrbracket$	1
A1	(c) 4	1

Why this question A linear congruence can have no solutions, exactly one class, or several. Which happens depends on what a and n have in common, which is made precise in Topic 16.

9 Powers and digits

7 marks

- (a) $7^2 = 49 \equiv 9 \equiv -1$, so $7^4 \equiv 1$ and $7^{20} = (7^4)^5 \equiv 1$. The last digit is **1**.
- (b) $5 \equiv -1 \pmod{3}$, so $5^{100} \equiv (-1)^{100} = 1$.
- (c) Each power of 10 is $\equiv 1$, so a number is congruent to its digit sum: $1 + 2 + 3 + 4 + 5 + 6 = 21 \equiv 3$.

M1	(a) $7^2 \equiv -1$, or another small power $\equiv \pm 1$	1
M1	(a) $7^4 \equiv 1$ and $20 = 4 \times 5$	1
A1	(a) 1	1
M1	(b) $5 \equiv -1$	1
A1	(b) 1	1
M1	(c) digit sum	1
A1	(c) 3	1

Why this question Because congruence respects multiplication, you can reduce first and multiply after. Finding a power that is congruent to 1 or -1 turns a huge exponent into a tiny one.

10 Squares and cubes modulo n

7 marks

- (a) Squares of $0, \dots, 6$ modulo 7 are $0, 1, 4, 2, 2, 4, 1$. So $x = 3$ **and** $x = 4$.
- (b) From the same list, 3 is never a square: **no** x .
- (c) Cubes of $0, \dots, 5$ are $0, 1, 8, 27, 64, 125$, which modulo 6 are $0, 1, 2, 3, 4, 5$. **Yes, for every x .**

M1	(a) list of squares	1
A1	(a) 3 and 4	1
B2	(b) none, from the list	2
M1	(c) computing cubes	1
A1	(c) all six reduced correctly	1
A1	(c) yes	1

Why this question Notice the squares in (a) come in pairs, x and $7 - x$, since $(-x)^2 = x^2$. Checking every case in $\llbracket n \rrbracket$ settles any question like this for good.

11 Exam style: multiplication modulo 12

9 marks

- (a) $0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7$, for $x = 0, \dots, 11$.
 (b) 7 appears at $x = 11$ only, so $x \in [11]_{12}$.
 (c) $0, 4, 8, 0, 4, 8, 0, 4, 8, 0, 4, 8$. The value 6 never appears, so **no solution**.
 (d) 8 appears at $x = 2, 5, 8, 11$, so $x \in [2]_{12} \cup [5]_{12} \cup [8]_{12} \cup [11]_{12} = [2]_3$.

B2	(a) all twelve. <i>B1 for ten or eleven</i>	2
B1	(b) $x = 11$	1
B1	(b) as a class	1
B1	(c) list	1
B1	(c) no solution	1
M1	(d) reading the four values from the list	1
A1	(d) union of four classes	1
A1	(d) $[2]_3$	1

Why this question Multiplying by 5 shuffles $\llbracket 12 \rrbracket$ (every value appears once), so every congruence $5x \equiv b$ has exactly one solution class. Multiplying by 4 only hits three values, so most congruences $4x \equiv b$ have no solution.

12 Exam style: powers, calendars and two congruences

9 marks

- (a) The powers are $3, 2, 6, 4, 5, 1$, so $3^6 \equiv 1$. Since $40 = 6 \times 6 + 4$, $3^{40} \equiv 3^4 = 81 \equiv 4$.
 (b) $100 = 14 \times 7 + 2$, so two days after Sunday: **Tuesday**.
 (c) Numbers $\equiv 3 \pmod{5}$ are $3, 8, 13, \dots$; the first that is $\equiv 2 \pmod{3}$ is 8.
 (d) $23 = 8 + 15$: $23 = 7 \times 3 + 2$ and $23 = 4 \times 5 + 3$. **Both hold**.

B1	(a) the six powers	1
M1	(a) using $3^6 \equiv 1$	1
M1	(a) $40 = 6 \times 6 + 4$	1
A1	(a) 4	1
M1	(b) $100 \equiv 2 \pmod{7}$	1
A1	(b) Tuesday	1
M1	(c) listing one condition and testing the other	1
A1	(c) 8	1
B1	(d)	1

Why this question Part (b) is modular arithmetic in everyday life: days of the week are $\mathbb{Z}/7\mathbb{Z}$. Part (d) hints at why every solution of (c) is 8 plus a multiple of 15, an idea made precise later in the module.

Total: 75 marks. Spotted a mistake? Report it at unimixedtutor.com and we will fix it.