

Topic 8 · Sheet A: Questions

Modular arithmetic and linear congruences

Suggested time

About 75 minutes

Total marks

75

Questions

12

Builds on

Topics 1 to 7

How to use this sheet. Work on your own paper. The questions start gently and get harder; questions 11 and 12 are exam style. Marks are a guide to how much working is expected, roughly one minute per mark. You need multiples and divisors, congruence modulo n , the sets $\mathbb{Z}/n\mathbb{Z}$ and their arithmetic, and linear congruences, plus Topics 1 to 7. Solve linear congruences by checking each case in $\llbracket n \rrbracket$; the euclidean algorithm is not needed.

Notation. n divides m when $m = kn$ for some integer k . $a \equiv b \pmod{n}$ when $a - b$ is a multiple of n . $[a]_n$ is the congruence class of a , and $\mathbb{Z}/n\mathbb{Z} = \{[a]_n \mid a \in \mathbb{Z}\}$, with $[a]_n + [b]_n = [a + b]_n$, $[a]_n \times [b]_n = [ab]_n$ and $-[a]_n = [-a]_n$.

1

4 marks

- (a) Does 7 divide 91? [1]
- (b) Does -4 divide 26? [1]
- (c) List the positive divisors of 36. [1]
- (d) Does 0 divide 5? [1]

2

4 marks

Decide whether each congruence holds.

- (a) $17 \equiv 2 \pmod{5}$ [1]
- (b) $-3 \equiv 11 \pmod{6}$ [1]
- (c) $100 \equiv 1 \pmod{9}$ [1]
- (d) $25 \equiv 4 \pmod{6}$ [1]

3

5 marks

In each part, find the unique $r \in \llbracket n \rrbracket$ with $a \equiv r \pmod{n}$.

- (a) $a = 47, n = 6$ [1]
- (b) $a = -13, n = 5$ [1]
- (c) $a = 1000, n = 7$ [1]

- (d) $a = 2^{10}, n = 11$ [1]
 (e) $a = 3^{100}, n = 4$ [1]

4

6 marks

- (a) List five elements of $[3]_7$, including at least two negative ones. [1]
 (b) Is $[17]_5 = [-8]_5$? [1]
 (c) Is $[17]_5 = [-7]_5$? [1]
 (d) List the elements of $\mathbb{Z}/4\mathbb{Z}$, using representatives from $\llbracket 4 \rrbracket$. [1]
 (e) How many elements does $\mathbb{Z}/12\mathbb{Z}$ have? [1]
 (f) Describe $\mathbb{Z}/1\mathbb{Z}$. [1]

5

6 marks

Give each answer as $[r]_n$ with $r \in \llbracket n \rrbracket$.

- (a) In $\mathbb{Z}/6\mathbb{Z}$, find $[4]_6 + [5]_6$. [1]
 (b) In $\mathbb{Z}/6\mathbb{Z}$, find $[4]_6 \times [5]_6$. [1]
 (c) In $\mathbb{Z}/6\mathbb{Z}$, find $-[2]_6$. [1]
 (d) Write out the multiplication table of $\mathbb{Z}/4\mathbb{Z}$. [3]

6

6 marks

- (a) In $\mathbb{Z}/7\mathbb{Z}$, find $[a]_7$ with $[3]_7 \times [a]_7 = [1]_7$. [2]
 (b) In $\mathbb{Z}/8\mathbb{Z}$, show there is no $[a]_8$ with $[2]_8 \times [a]_8 = [1]_8$. [2]
 (c) In $\mathbb{Z}/6\mathbb{Z}$, find two classes, neither equal to $[0]_6$, whose product is $[0]_6$. [2]

7

6 marks

Find all integer solutions of each linear congruence, as a union of congruence classes.

- (a) $3x \equiv 4 \pmod{5}$ [2]
 (b) $4x \equiv 2 \pmod{6}$ [2]
 (c) $6x \equiv 3 \pmod{9}$ [2]

8

6 marks

- (a) Show that $2x \equiv 5 \pmod{8}$ has no integer solutions. [2]
 (b) Find all solutions of $5x \equiv 0 \pmod{10}$. [2]
 (c) How many $x \in \llbracket 12 \rrbracket$ satisfy $4x \equiv 8 \pmod{12}$? [2]

9

7 marks

- (a) Find the last digit of 7^{20} , by working modulo 10. [3]
- (b) Find $r \in \mathbb{[3]}$ with $5^{100} \equiv r \pmod{3}$. [2]
- (c) Use $10 \equiv 1 \pmod{9}$ to find $r \in \mathbb{[9]}$ with $123456 \equiv r \pmod{9}$. [2]

10

7 marks

- (a) Find every $x \in \mathbb{[7]}$ with $x^2 \equiv 2 \pmod{7}$. [2]
- (b) Find every $x \in \mathbb{[7]}$ with $x^2 \equiv 3 \pmod{7}$. [2]
- (c) Check whether $x^3 \equiv x \pmod{6}$ for every $x \in \mathbb{[6]}$, showing each cube modulo 6. [3]

11

9 marks

Exam style. Work modulo 12.

- (a) List $5x$ modulo 12 for each $x \in \mathbb{[12]}$, as an element of $\mathbb{[12]}$. [2]
- (b) Use your list to solve $5x \equiv 7 \pmod{12}$. [2]
- (c) List $4x$ modulo 12 for each $x \in \mathbb{[12]}$. Does $4x \equiv 6 \pmod{12}$ have a solution? [2]
- (d) Find all solutions of $4x \equiv 8 \pmod{12}$, as a union of classes modulo 12 and as a single class modulo 3. [3]

12

9 marks

Exam style.

- (a) Find 3^k modulo 7 for $k = 1, \dots, 6$, and use 3^6 to find $r \in \mathbb{[7]}$ with $3^{40} \equiv r \pmod{7}$. [4]
- (b) Today is a Sunday. What day of the week will it be in 100 days? [2]
- (c) Find the smallest positive integer x with $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$. [2]
- (d) Check that $x + 15$ also satisfies both congruences, for your x from (c). [1]

End of questions. Worked answers and the mark scheme are in the matching answers PDF.