Mathematics 2 **Number Theory 3**

Q1. For each of the following Diophantine equations find the general solution in standard form.

i. $256x - 64y = 128$

ii. $751x + 391y = 37$

iii. $6429x + 23573y = 12858$

iv. $28761x - 59333y = 311$

Q2. Show the following

(a) $13 \equiv 1 \pmod 2$ (b) $22 \equiv 7 \pmod 5$ (c) $91 \equiv 0 \pmod{13}$

(d) $69 \equiv 62 \pmod 7$ (e) $-2 \equiv 1 \pmod 3$ (f) $-3 \equiv 30 \pmod{11}$

(d) $111 \equiv -9 \pmod{40}$ (e) $666 \equiv 0 \pmod{37}$

Q3. Which of the following pairs of integers are congruent modulo 7?

(a) $1, 15$ (b) $0, 42$ (c) $2, 99$

(d) $-1, 8$ (e) $-9, 5$ (f) $-1, 699$

Q4. For which $m \in \mathbb{Z}_+$ are the following true?

(a) $27 \equiv 5 \pmod m$ (b) $1000 \equiv 1 \pmod m$ (c) $1331 \equiv 0 \pmod m$

Q5. Show that if $a \in \mathbb{Z}$ is even then $a^2 \equiv 0 \pmod 4$ and if $a \in \mathbb{Z}$ is odd then $a^2 \equiv 1 \pmod 4$.

Q6. Show that if $a \in \mathbb{Z}$ is odd then $a^2 \equiv 1 \pmod 8$.

Q7. Find the residue modulo 28 of

(a) 99 (b) 1100 (c) 12345

(d) -1 (e) -1000 (f) -54321

Q8. Construct a table for addition modulo 6.

Q9. Construct a table for subtraction modulo 6.

Q10. Construct a table for multiplication modulo 6. Which residues have multiplicative inverses?

Q11. Find a solution to the linear congruence equations

i. $3x \equiv 1 \pmod 5$

ii. $5x \equiv 4 \pmod 9$

iii. $980x \equiv 1500 \pmod{1600}$

Answers start on next page. Please try the questions before looking at the answers!

Answers:

Q1.

i. $x = 0 + k, y = -2 + 4k, k \in \mathbb{Z}$.

ii. $x = 188 + 391k, y = -361 - 751k, k \in \mathbb{Z}$.

iii. $x = 2 + 11k, y = 0 - 3k, k \in \mathbb{Z}$.

iv. $x = 36104 + 59333k, y = 17501 + 28761k, k \in \mathbb{Z}$.

Q3.

(a)	Yes	(b)	Yes	(c)	No
(d)	No	(e)	Yes	(f)	Yes

Q4.

(a) $1, 2, 11, 22$ (b) $1, 3, 9, 27, 37, 111, 333, 999$ (c) $1, 11, 121, 1331$

Q7.

(a)	15	(b)	8	(c)	25
(d)	27	(e)	8	(f)	27

Q8.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Q9.

$-$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4		2	1	0	5
5	5	4	3	2	1	

Q10.

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Q11.

i. 2

ii. 8

iii. 875