

1. Construct a multiplication table for $\mathbb{Z}/6\mathbb{Z} := \{0, 1, 2, 3, 4, 5\}$.

\cdot	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	3	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2. Find the least positive residue of $1! + 2! + 3! + \cdots + 10!$ modulo each of the following integers

(a) 3

(c) 11

(b) 4

(d) 23

(a) Note that $3!, 4!, 5!, \dots, 10!$ are all multiples of 3 and hence, each is congruent to 0 mod 3. $1! \equiv 1 \pmod{3}$ and $2! \equiv 2 \pmod{3}$, so

$$1! + 2! + \cdots + 10! \equiv 1 + 2 + 0 + \cdots + 0 \equiv 0 \pmod{3}$$

(b) As in the previous part, $4!, 5!, \dots, 10!$ are all multiples of 4 and each is congruent to 0 mod 4. $1! \equiv 1 \pmod{4}$, $2! \equiv 2 \pmod{4}$, and $3! \equiv 2 \pmod{4}$, so

$$1! + 2! + \cdots + 10! \equiv 1 + 2 + 2 + 0 + \cdots + 0 \equiv 1 \pmod{4}$$

(c) There's no trick here beyond using a calculator to compute the least positive residue of $n!$ modulo 11 for each $1 \leq n \leq 10$, then adding them up at the end. You end up finding that

$$1! + 2! + \cdots + 10! \equiv 0 \pmod{11}$$

(d) As in the previous part, there's no trick. You end up finding that

$$1! + 2! + \cdots + 10! \equiv 10 \pmod{23}$$

3. Show that if a is an even integer, then

$$a^2 \equiv 0 \pmod{4}$$

and if a is an odd integer, then

$$a^2 \equiv 1 \pmod{4}$$

If a is even, then $a = 2s$ for some $s \in \mathbb{Z}$. Then $a^2 = 4s^2$ and since $4 \mid 4s^2$, $a^2 \equiv 4s^2 \equiv 0 \pmod{4}$. Similarly, if a is odd, then $a = 2s + 1$ for some $s \in \mathbb{Z}$. Then

$$a^2 = 4s^2 + 4s + 1 = 4(s^2 + s) + 1 \equiv 1 \pmod{4}$$

4. Show that $4^{3n+1} + 2^{3n+1} \equiv 6 \pmod{7}$ for all integers $n \geq 0$

Here, we use the fact that if $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ regularly. First observe that $2^{3n+1} = 2 \cdot 8^n \cdot 2$. Since $8 \equiv 1 \pmod{7}$, we conclude that $2^{3n+1} = 8^n \cdot 2 \equiv 2 \pmod{7}$. Likewise, $4^{3n+1} = 64^n \cdot 4$ and since $64 \equiv 1 \pmod{7}$, $4^{3n+1} = 64^n \cdot 4 \equiv 4 \pmod{7}$. Hence,

$$4^{3n+1} + 2^{3n+1} \equiv 4 + 2 = 6 \pmod{7}$$

5. Find all solutions to each of the following linear congruences:

(a) $3x \equiv 2 \pmod{7}$

$3x \equiv 2 \pmod{7}$ if and only if there exists $y \in \mathbb{Z}$ so that $3x - 2 = 7y$, i.e. $3x - 7y = 2$. Since $(3, 7) = 1$ and since $3 \cdot 3 - 7 \cdot 1 = 2$, every x and y which solve $3x - 7y = 2$ are of the form $x = 3 + 7k$ and $y = 1 + 3k$ for some $k \in \mathbb{Z}$. Hence, the only solution to $3x \equiv 2 \pmod{7}$ is $x \equiv 3 \pmod{7}$.

(b) $17x \equiv 14 \pmod{21}$

$17x \equiv 14 \pmod{21}$ if and only if there exists $y \in \mathbb{Z}$ so that $17x - 14 = 21y$, i.e. $17x - 21y = 14$. Since $(17, 21) = 1$ and $17 \cdot 7 - 21 \cdot 5 = 14$, every x and y which solve $17x - 21y = 14$ are of the form $x = 7 + 21k$ and $y = 5 + 17k$ for some integer k . Hence, the only solution to $17x \equiv 14 \pmod{21}$ is $x \equiv 7 \pmod{21}$.

(c) $15x \equiv 9 \pmod{25}$

$15x \equiv 9 \pmod{25}$ if and only if there exists $y \in \mathbb{Z}$ so that $15x - 9 = 25y$, i.e. $15x - 25y = 9$. But $(15, 25) = 5$ which doesn't divide 9. Therefore, $15x \equiv 9 \pmod{25}$ has no solutions.