Number Theory Exercises 4

Jason Sass

July 17, 2023

Congruences

Exercise 1. Write up justifications for the basic examples of congruence modulo definition.

a. $3 \equiv 24 \pmod 7$.
b. $-31 \equiv 11 \pmod 7$.
c. $-15 \equiv -64 \pmod 7$.
d. $25 \not\equiv 12 \pmod 7$.

Proof. Since $7(-3) = -21 = 3 - 24$, then 7 divides $3 - 24$, so 3 is congruent to 24 modulo 7.

Therefore, $3 \equiv 24 \pmod 7$. ☐

Proof. Since $7(-6) = -42 = -31 - 11$, then 7 divides $-31 - 11$, so -31 is congruent to 11 modulo 7.

Therefore, $-31 \equiv 11 \pmod 7$. ☐

Proof. Since $7(7) = 49 = -15 - (-64)$, then 7 divides $-15 - (-64)$, so -15 is congruent to -64 modulo 7.

Therefore, $-15 \equiv -64 \pmod 7$. ☐

Proof. Since 7 does not divide $13 = 25 - 12$, then 25 is not congruent to 12 modulo 7.

Therefore, $25 \not\equiv 12 \pmod 7$. ☐

Exercise 2. Any two integers are congruent modulo 1

Let $a, b \in \mathbb{Z}$.

Then $a \equiv b \pmod 1$.

Proof. Since 1 divides any integer, then 1 divides the difference $a - b$, so $a \equiv b \pmod 1$. ☐

Exercise 3. Two integers are congruent modulo 2 **when they are both even or both odd**

Let $a, b \in \mathbb{Z}$.

Then $a \equiv b \pmod 2$ iff a and b are either both even or both odd.

Proof. We first prove if a and b are both even or both odd, then $a \equiv b \pmod 2$.

Suppose a and b are both even or both odd.

Then either a and b are both even or a and b are both odd.

We consider these cases separately.

Case 1: Suppose a and b are both even.

Then $a = 2m$ and $b = 2n$ for some integers m and n.

Thus, $a - b = 2m - 2n = 2(m - n)$, so $2|(a - b)$.

Therefore, $a \equiv b \pmod 2$.

Case 2: Suppose a and b are both odd.

Then $a = 2m + 1$ and $b = 2n + 1$ for some integers m and n.

Thus, $a - b = (2m + 1) - (2n + 1) = 2m + 1 - 2n - 1 = 2m - 2n = 2(m - n)$, so $2|(a - b)$.

Therefore, $a \equiv b \pmod 2$. $\square$

Proof. Conversely, we prove if $a \equiv b \pmod 2$, then a and b are either both even or both odd.

We prove by contradiction.

Suppose $a \equiv b \pmod 2$ and neither a and b are both even nor both odd.

Then either a and b are not both even or a and b are not both odd, so either a is even and b is odd, or a is odd and b is even.

We consider these cases separately.

Case 1: Suppose a is even and b is odd.

Then $a = 2m$ and $b = 2n + 1$ for some integers m and n.

Thus, $a-b = 2m-(2n+1) = 2m-2n-1 = 2m-2n-2+1 = 2(m-n-1)+1$, so $2 \not| (a - b)$.

Therefore, $a \not\equiv b \pmod 2$.

But, this contradicts the assumption $a \equiv b \pmod 2$.

Case 2: Suppose a is odd and b is even.

Then $a = 2m + 1$ and $b = 2n$ for some integers m and n.

Thus, $a - b = (2m + 1) - 2n = 2m - 2n + 1 = 2(m - n) + 1$, so $2 \not| (a - b)$.

Therefore, $a \not\equiv b \pmod 2$.

But, this contradicts the assumption $a \equiv b \pmod 2$.

In all cases, we reach a contradiction.

Therefore, if $a \equiv b \pmod 2$, then a and b are either both even or both odd. $\square$

Exercise 4. Since $-56 = (-7)9 + 7$ and $-11 = (-2)9 + 7$, then -56 and -11 leave the same remainder 7 when divided by 9.

Therefore, $-56 \equiv -11 \pmod 9$.

Exercise 5. Show that 41 divides $2^{20} - 1$.

Solution. Since $41|32 - (-9)$, then $2^5 = 32 \equiv -9 \pmod{41}$.

Since $41 \cdot 2 = 82 = 81 - (-1)$, then 41 divides $81 - (-1)$, so $81 \equiv -1 \pmod{41}$.

Observe that

$$\begin{aligned} 2^{20} &= (2^5)^4 \\ &\equiv (-9)^4 \pmod{41} \\ &\equiv 9^4 \pmod{41} \\ &\equiv 81^2 \pmod{41} \\ &\equiv (-1)^2 \pmod{41} \\ &\equiv 1 \pmod{41}. \end{aligned}$$

Therefore, $2^{20} \equiv 1 \pmod{41}$, so $41|(2^{20}-1)$.

We observe the prime factorization is $2^{20} - 1 = 3 * 5^2 * 11 * 31 * 41$. $\square$

Exercise 6. Find the remainder when the sum $1! + 2! + 3! + 4! + ... + 99! + 100!$ is divided by 12.

Solution. Observe that $4! = 24 \equiv 0 \pmod{12}$.

Observe that $5! = 4! * 5$ and $6! = 4! * 5 * 6$ and $7! = 4! * 5 * 6 * 7$ and ... $k! = 4! * 5 * ... * (k-1) * k$, for any integer $k \geq 4$.

For any $k \geq 4$, we have

$$\begin{aligned} k! &= 4! * 5 * \ldots * (k-1) * k \\ &\equiv 0 * 5 * \ldots * (k-1) * k \pmod{12} \\ &\equiv 0 \pmod{12}.. \end{aligned}$$

Thus, $k! \equiv 0 \pmod{12}$ for any $k \geq 4$, so $4! \equiv 0 \pmod{12}$ and $5! \equiv 0 \pmod{12}$ and ... and $100! \equiv 0 \pmod{12}$.

Observe that

$$\begin{aligned} 1! + 2! + 3! + 4! + ... + 99! + 100! &= (1! + 2! + 3!) + (4! + 5! + \ldots + 100!) \\ &= 9 + (4! + 5! + \ldots + 100!) \\ &\equiv 9 + (0 + 0 + \ldots + 0) \pmod{12} \\ &\equiv 9 \pmod{12}. \end{aligned}$$

Hence, 12 divides $(1! + 2! + ... + 100!) - 9$, so $1! + 2! + ... + 100! - 9 = 12m$ for some integer m.

Thus, $1! + 2! + ... + 100! = 12m + 9$.

Therefore, by the division algorithm, when $1! + 2! + ... + 100!$ is divided by 12, the remainder is 9. $\square$

Exercise 7. What does $33 \equiv 15 \pmod{9}$ imply?

Solution. Since $9 \cdot 2 = 18 = 33 - 15$, then 9 divides $33 - 15$, so $33 \equiv 15 \pmod{9}$.

Thus, $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$.

Since $\gcd(9, 3) = 3$, then we conclude $11 \equiv 5 \pmod{\frac{9}{3}}$.

Therefore, $11 \equiv 5 \pmod{3}$.

Indeed, $3 * 2 = 6 = 11 - 5$, so 3 divides $11 - 5$.

Hence, $11 \equiv 5 \pmod{3}$. $\square$

Exercise 8. What does $-35 \equiv 45 \pmod 8$ imply?

Solution. Since $8(-10) = -80 = -35 - 45$, then 8 divides $-35 - 45$, so $-35 \equiv 45 \pmod 8$.

Thus, $(-7)5 \equiv 9(5) \pmod 8$.

Since $\gcd(8, 5) = 1$, then we may cancel to obtain $-7 \equiv 9 \pmod 8$.

Indeed, 8 divides the difference $-7 - 9 = -16 = 8(-2)$. $\square$

Exercise 9. Show that $ab \equiv 0 \pmod n$ does not imply $a \equiv 0 \pmod n$ or $b \equiv 0 \pmod n$.

Solution. Let $n = 12$ and $a = 4$ and $b = 3$.

Then $4 \cdot 3 \equiv 0 \pmod{12}$, but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$. $\square$

Proposition 10. *Let $n \in \mathbb{Z}^+$.*

Let $a, b \in \mathbb{Z}$.

If $ab \equiv 0 \pmod n$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod n$.

Proof. Suppose $ab \equiv 0 \pmod n$ and $\gcd(a, n) = 1$.

Since $ab \equiv 0 \pmod n$, then $n|ab - 0$, so $n|ab$.

Since $n|ab$ and $\gcd(n, a) = 1$, then $n|b$, so $n|b - 0$.

Therefore, $b \equiv 0 \pmod n$. $\square$

Proposition 11. *Let $p \in \mathbb{Z}^+$.*

Let $a, b \in \mathbb{Z}$.

If $ab \equiv 0 \pmod p$ and p is prime, then either $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$.

Proof. Suppose $ab \equiv 0 \pmod p$ and p is prime.

Since $ab \equiv 0 \pmod p$, then $p|ab$.

Since p is prime and $p|ab$, then either $p|a$ or $p|b$, by Euclid's lemma.

Therefore, either $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$. $\square$

Exercise 12. Let $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$.

Show that $ac \equiv bc \pmod n$ does not necessarily imply $a \equiv b \pmod n$.

Solution. Let $n = 6$ and $a = 10$ and $b = 7$ and $c = 2$.

Since $6 \cdot 1 = 6 = 20 - 14$, then 6 divides $20 - 14 = 10 \cdot 2 - 7 \cdot 2$, so 6 divides $10 \cdot 2 - 7 \cdot 2$.

Thus, $10 \cdot 2 \equiv 7 \cdot 2 \pmod 6$.

Since $6 \nmid 3$ and $3 = 10 - 7$, then 6 does not divide $10 - 7$, so $10 \not\equiv 7 \pmod 6$.

Therefore, $10 \cdot 2 \equiv 7 \cdot 2 \pmod 6$, but $10 \not\equiv 7 \pmod 6$. $\square$

Exercise 13. Let $m, n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$.

If $a \equiv b \pmod n$ and $m|n$, then $a \equiv b \pmod m$.

Proof. Suppose $a \equiv b \pmod n$ and $m|n$.

Since $a \equiv b \pmod n$, then $n|a - b$.

Since $m|n$ and $n|a - b$, then $m|a - b$

Therefore, $a \equiv b \pmod m$. $\square$

Proposition 14. *Let* $n, c \in \mathbb{Z}^+$ *and* $a, b, c \in \mathbb{Z}$.
If $a \equiv b \pmod{n}$, *then* $ac \equiv bc \pmod{nc}$.

Proof. Suppose $a \equiv b \pmod{n}$.
Then $n|a-b$.
Hence, $nc|(a-b)c$, so $nc|ac-bc$.
Therefore, $ac \equiv bc \pmod{nc}$. $\square$

Exercise 15. Let $n, d \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$.
If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by d, then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

Proof. Suppose $a \equiv b \pmod{n}$ and $d|a$ and $d|b$ and $d|n$.
Since $a \equiv b \pmod{n}$, then $n|a-b$, so $a-b = nk$ for some integer k.
Since $d|a$, then $a = dk_1$ for some integer k_1, so $k_1 = \frac{a}{d}$.
Therefore, $\frac{a}{d} \in \mathbb{Z}$.
Since $d|b$, then $b = dk_2$ for some integer k_2, so $k_2 = \frac{b}{d}$.
Therefore, $\frac{b}{d} \in \mathbb{Z}$.
Since $d|n$, then $n = dk_3$ for some integer k_3, so $k_3 = \frac{n}{d}$.
Therefore, $\frac{n}{d} \in \mathbb{Z}$.
Since $a-b = nk$, then we divide by $d > 0$ to obtain $\frac{a}{d} - \frac{b}{d} = \frac{a-b}{d} = \frac{nk}{d} = \frac{n}{d} \cdot k$.
Therefore, $\frac{n}{d}$ divides the difference $\frac{a}{d} - \frac{b}{d}$, so $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. $\square$

Exercise 16. Let $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$.
Show that $a^2 \equiv b^2 \pmod{n}$ does not necessarily imply $a \equiv b \pmod{n}$.

Solution. Let $n = 4$ and $a = 5$ and $b = 3$.
Since $16 = 4 \cdot 4 = 25 - 9$, then 4 divides $25 - 9$, so $25 \equiv 9 \pmod{4}$.
Since $4 \nmid 2$ and $2 = 5 - 3$, then 4 does not divide $5 - 3$, so $5 \not\equiv 3 \pmod{4}$.
Therefore, $25 \equiv 9 \pmod{4}$ does not imply $5 \equiv 3 \pmod{4}$. $\square$

Exercise 17. Let $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$.
If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

Proof. Suppose $a \equiv b \pmod{n}$.
Then $n|a-b$, so $a-b = nk$ for some integer k.
Let $d = \gcd(a, n)$.
Then $d|a$ and $d|n$ and if any integer c divides both a and n, then $c|d$.
Since $d|a$ and $d|n$, then d divides any linear combination of a and n.
Since $b = a - nk$ is a linear combination of a and n, then $d|b$.
Since $d|b$ and $d|n$, then d is a common divisor of b and n.

Let c be any common divisor of b and n.
The $c|b$ and $c|n$, so c divides any linear combination of b and n.
Since $a = b + nk$ is a linear combination of b and n, then $c|a$.
Since $c|a$ and $c|n$, then we conclude $c|d$.
Therefore, any common divisor of b and n divides d.

Since d is a common divisor of b and n and any common divisor of b and n divides d, then $d = \gcd(b, n)$.

Therefore, $\gcd(a, n) = \gcd(b, n)$. $\square$

Exercise 18. What is the remainder when 2^{50} is divided by 7?

Solution. Since $2^5 = 32 \equiv 4 \pmod 7$, then $2^{10} = (2^5)^2 \equiv 4^2 \pmod 7 \equiv 16 \pmod 7 \equiv 2 \pmod 7$, so $2^{10} \equiv 2 \pmod 7$.

Observe that

$$\begin{aligned} 2^{50} &= (2^{10})^5 \\ &\equiv 2^5 \pmod 7 \\ &\equiv 32 \pmod 7 \\ &\equiv 4 \pmod 7. \end{aligned}$$

Hence, $2^{50} \equiv 4 \pmod 7$, so $7 | 2^{50} - 4$.

Therefore, $2^{50} - 4 = 7k$ for some integer k, so $2^{50} = 7k + 4$.

By the division algorithm, the remainder is 4. $\square$

Exercise 19. What is the remainder when 41^{65} is divided by 7?

Solution. Observe that $41 \equiv -1 \pmod 7$.

Thus,

$$\begin{aligned} 41^{65} &\equiv (-1)^{65} \pmod 7 \\ &\equiv -1 \pmod 7 \\ &\equiv 6 \pmod 7. \end{aligned}$$

Consequently, $41^{65} \equiv 6 \pmod 7$, so 7 divides $41^{65} - 6$.

Hence, $41^{65} - 6 = 7k$ for some integer k, so $41^{65} = 7k + 6$.

Therefore, by the division algorithm, when 41^{65} is divided by 7 the remainder is 6. $\square$

Exercise 20. What is the remainder when the sum $1^5 + 2^5 + 3^5 + ... + 99^5 + 100^5$ is divided by 4?

Solution. TODO

We observe that

$1^5 \equiv 1 \pmod 4$

$2^5 \equiv 0 \pmod 4$

$3^5 \equiv 3 \pmod 4$

$4^5 \equiv 0 \pmod 4$

$5^5 \equiv 1 \pmod 4$

$6^5 \equiv 0 \pmod 4$

$7^5 \equiv 3 \pmod 4$

$8^5 \equiv 0 \pmod 4$

$9^5 \equiv 1 \pmod 4$

Do we see a pattern or patterns?

Maybe if $k \equiv 1 \pmod 4$, then $k^5 \equiv 1 \pmod 4$. Can we prove this?
If k is even, then $k^5 \equiv 0 \pmod 4$. Can we prove this?
If $k \equiv 3 \pmod 4$, then $k^5 \equiv 3 \pmod 4$. Can we prove this?
So, if k is even, then adding doesn't change the sum.
So, if k is odd, then either $k \equiv 1 \pmod 4$ or $k \equiv 3 \pmod 4$.
So, how many k are between 1 and 100 and congruent to 1?
So, how many k are between 1 and 100 and congruent to 3?
Let c_1 be the number of k between 1 and 100 that are congruent to 1.
Then $c_1 = 25$ since $S_4^1 = \{4k + 1 : 1 \leq 4k + 1 \leq 100\}$.
Let c_2 be the number of k between 1 and 100 that are congruent to 3.
Then $c_2 = 25$ since $S_4^3 = \{4k + 3 : 1 \leq 4k + 3 \leq 100\}$.
Then $c_1 * 1 + c_2 * 3 = 25 * 1 + 25 * 3 = 25 * 4 = 100$ is the sum.
So, we think the sum will be congruent to 0 modulo 4.
This means the remainder is zero. $\square$

Proposition 21. *Let* $n_1, n_2 \in \mathbb{Z}^+$.
Let $a, b \in \mathbb{Z}$.
If $a \equiv b \pmod{n_1}$ *and* $a \equiv b \pmod{n_2}$, *then* $a \equiv b \pmod{lcm(n_1, n_2)}$.
Hence, whenever $\gcd(n_1, n_2) = 1$, *then* $a \equiv b \pmod{n_1 n_2}$.

Proof. Suppose $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$.
Then $n_1 | (a - b)$ and $n_2 | (a - b)$, so $a - b$ is a multiple of n_1 and n_2.
Hence, $a - b$ is a multiple of the least common multiple of n_1 and n_2, by definition of least common multiple.
Thus, $lcm(n_1, n_2)$ divides $a - b$, so a is congruent to b modulo $lcm(n_1, n_2)$.
Therefore, $a \equiv b \pmod{lcm(n_1, n_2)}$. $\square$

Proof. We prove: if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$ and $\gcd(n_1, n_2) = 1$, then $a \equiv b \pmod{n_1 n_2}$.

Suppose $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$ and $\gcd(n_1, n_2) = 1$.
Since $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod{lcm(n_1, n_2)}$.
Since $lcm(n_1, n_2) \cdot \gcd(n_1, n_2) = n_1 n_2$ and $\gcd(n_1, n_2) = 1$, then $n_1 n_2 = lcm(n_1, n_2) \cdot 1 = lcm(n_1, n_2)$.
Therefore, $a \equiv b \pmod{n_1 n_2}$. $\square$

Exercise 22. Give an example to show that $a^k \equiv b^k \pmod n$ and $k \equiv j \pmod n$ does not imply $a^j \equiv b^j \pmod n$.

Solution. Let $a = 7$ and $b = 5$ and $n = 3$ and $j = 5$ and $k = 2$.
Since $3 \cdot 8 = 24 = 49 - 25 = 7^2 - 5^2$, then 3 divides $7^2 - 5^2$, so $7^2 \equiv 5^2 \pmod 3$.
Since $3(-1) = -3 = 2 - 5$, then 3 divides $2 - 5$, so $2 \equiv 5 \pmod 3$.
Since $7^5 - 5^5 = 13682 = 3 \cdot 4560 + 2$, then $3 \nmid (7^5 - 5^5)$, so $7^5 \not\equiv 5^5 \pmod 3$.
Therefore, $7^2 \equiv 5^2 \pmod 3$ and $2 \equiv 5 \pmod 3$, but $7^5 \not\equiv 5^5 \pmod 3$. $\square$

Lemma 23. *Let* $a \in \mathbb{Z}$.
If a *is odd, then* $a^2 \equiv 1 \pmod 8$.

Proof. Suppose a is odd.

Then $a = 2k + 1$ for some integer k.

Thus, $a^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k = 4k(k + 1)$.

Since k and $k+1$ are consecutive integers, then the product $k(k+1)$ is even.

Hence, $k(k + 1) = 2m$ for some integer m.

Consequently, $a^2 - 1 = 4(2m) = 8m$, so $8|(a^2 - 1)$.

Therefore, $a^2 \equiv 1 \pmod 8$. ☐

Proof. Suppose a is odd.

By the division algorithm, there exist unique integers q and r such that $a = 4q + r$ and $0 \leq r < 4$, so either $a = 4q$ or $a = 4q + 1$ or $a = 4q + 2$ or $a = 4q + 3$.

Since $4q = 2(2q)$ is even and a is odd, then $a \neq 4q$.

Since $4q + 2 = 2(2q + 1)$ is even and a is odd, then $a \neq 4q + 2$.

Thus, either $a = 4q + 1$ or $a = 4q + 3$.

We consider these cases separately.

Case 1: Suppose $a = 4q + 1$.

Then $a^2 - 1 = (4q + 1)^2 - 1 = 16q^2 + 8q + 1 - 1 = 16q^2 + 8q = 8q(2q + 1)$.

Hence, 8 divides $a^2 - 1$, so $a^2 \equiv 1 \pmod 8$.

Case 2: Suppose $a = 4q + 3$.

Then $a^2 - 1 = (4q + 3)^2 - 1 = 16q^2 + 24q + 9 - 1 = 16q^2 + 24q + 8 = 8(2q^2 + 3q + 1)$.

Hence, 8 divides $a^2 - 1$, so $a^2 \equiv 1 \pmod 8$.

Therefore, in all cases, $a^2 \equiv 1 \pmod 8$. ☐

Exercise 24. Let $a \in \mathbb{Z}$.

Then either $a^3 \equiv 0 \pmod 9$ or $a^3 \equiv 1 \pmod 9$ or $a^3 \equiv 8 \pmod 9$.

Proof. By the division algorithm, there exist unique integers q and r such that $a = 3q + r$ and $0 \leq r < 3$, so either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.

We consider these cases separately.

Case 1: Suppose $a = 3q$.

Then $a^3 = (3q)^3 = 3^3q^3 = (3^2)3q^3 = 9(3q^3)$.

Hence, 9 divides a^3, so $a^3 \equiv 0 \pmod 9$.

Case 2: Suppose $a = 3q + 1$.

Then $a^3 = (3q + 1)^3 = 27q^3 + 27q^2 + 9q + 1$, so $a^3 - 1 = 27q^3 + 27q^2 + 9q = 9q(3q^2 + 3q + 1)$.

Hence, 9 divides $a^3 - 1$, so $a^3 \equiv 1 \pmod 9$.

Case 3: Suppose $a = 3q + 2$.

Then $a^3 = (3q+2)^3 = 27q^3 + 54q^2 + 36q + 8$, so $a^3 - 8 = 27q^3 + 54q^2 + 36q = 9q(3q^2 + 6q + 4)$.

Hence, 9 divides $a^3 - 8$, so $a^3 \equiv 8 \pmod 9$.

In all cases, either $a^3 \equiv 0 \pmod 9$ or $a^3 \equiv 1 \pmod 9$ or $a^3 \equiv 8 \pmod 9$. $\square$

Exercise 25. Let $a \in \mathbb{Z}$.
Then $a^3 \equiv a \pmod 6$.

Proof. The product of three consecutive integers is divisible by 6.
Thus, the product $(a-1)a(a+1) = a(a^2-1) = a^3 - a$ is divisible by 6, so 6 divides $a^3 - a$.
Therefore, $a^3 \equiv a \pmod 6$. $\square$

Proof. By the division algorithm, there exist unique integers q and r such that $a = 6q + r$ and $0 \leq r < 6$, so either $a = 6q$ or $a = 6q+1$ or $a = 6q+2$ or $a = 6q+3$ or $a = 6q+4$ or $a = 6q+5$.
We consider these cases separately.
Case 1: Suppose $a = 6q$.
Then

$$\begin{aligned} a^3 - a &= (6q)^3 - 6q \\ &= 6^3q^3 - 6q \\ &= 6q(36q^2 - 1). \end{aligned}$$

Hence, 6 divides $a^3 - a$, so $a^3 \equiv a \pmod 6$.
Case 2: Suppose $a = 6q+1$.
Then

$$\begin{aligned} a^3 - a &= (6q+1)^3 - (6q+1) \\ &= (216q^3 + 108q^2 + 18q + 1) - (6q+1) \\ &= 216q^3 + 108q^2 + 12q \\ &= 6q(36q^2 + 18q + 2). \end{aligned}$$

Hence, 6 divides $a^3 - a$, so $a^3 \equiv a \pmod 6$.
Case 3: Suppose $a = 6q+2$.
Then

$$\begin{aligned} a^3 - a &= (6q+2)^3 - (6q+2) \\ &= (216q^3 + 216q^2 + 72q + 8) - (6q+2) \\ &= 216q^3 + 216q^2 + 66q + 6 \\ &= 6(36q^3 + 36q^2 + 11q + 1). \end{aligned}$$

Hence, 6 divides $a^3 - a$, so $a^3 \equiv a \pmod 6$.
Case 4: Suppose $a = 6q+3$.
Then

$$\begin{aligned} a^3 - a &= (6q+3)^3 - (6q+3) \\ &= (216q^3 + 324q^2 + 162q + 27) - (6q+3) \\ &= 216q^3 + 324q^2 + 156q + 24 \\ &= 6(36q^3 + 54q^2 + 26q + 4). \end{aligned}$$

Hence, 6 divides $a^3 - a$, so $a^3 \equiv a \pmod 6$.
Case 5: Suppose $a = 6q + 4$.
Then

$$\begin{aligned} a^3 - a &= (6q+4)^3 - (6q+4) \\ &= (216q^3 + 432q^2 + 288q + 64) - (6q+4) \\ &= 216q^3 + 432q^2 + 282q + 60 \\ &= 6(36q^3 + 72q^2 + 47q + 12). \end{aligned}$$

Hence, 6 divides $a^3 - a$, so $a^3 \equiv a \pmod 6$.
Case 6: Suppose $a = 6q + 5$.
Then

$$\begin{aligned} a^3 - a &= (6q+5)^3 - (6q+5) \\ &= (216q^3 + 540q^2 + 450q + 125) - (6q+5) \\ &= 216q^3 + 540q^2 + 444q + 120 \\ &= 6(36q^3 + 90q^2 + 74q + 20). \end{aligned}$$

Hence, 6 divides $a^3 - a$, so $a^3 \equiv a \pmod 6$.

Therefore, in all cases, $a^3 \equiv a \pmod 6$. $\square$

Exercise 26. If an integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

Proof. Let $a \in \mathbb{Z}$.
We must prove: If $2 \nmid a$ and $3 \nmid a$, then $a^2 \equiv 1 \pmod{24}$.
Suppose $2 \nmid a$ and $3 \nmid a$.
Since $2 \nmid a$, then a is not even, so a is odd.
If a is odd, then $a^2 \equiv 1 \pmod 8$, by lemma 23.
Therefore, we conclude $a^2 \equiv 1 \pmod 8$.

We next show that $a^2 \equiv 1 \pmod 3$.
By the division algorithm, there exist unique integers q and r such that $a = 3q + r$ and $0 \leq r < 3$, so either $a = 3q$ or $a = 3q + 1$ or $a = 3q + 2$.
Since $3 \nmid a$ and 3 divides $3q$, then $a \neq 3q$.
Thus, either $a = 3q + 1$ or $a = 3q + 2$.
We consider these cases separately.
Case 1: Suppose $a = 3q + 1$.
Then

$$\begin{aligned} a^2 - 1 &= (3q+1)^2 - 1 \\ &= 9q^2 + 6q + 1 - 1 \\ &= 9q^2 + 6q \\ &= 3q(3q+2). \end{aligned}$$

Hence, 3 divides $a^2 - 1$, so $a^2 \equiv 1 \pmod 3$.
Case 2: Suppose $a = 3q + 2$.
Then

$$\begin{aligned} a^2 - 1 &= (3q+2)^2 - 1 \\ &= 9q^2 + 12q + 4 - 1 \\ &= 9q^2 + 12q + 3 \\ &= 3(3q^2 + 4q + 1). \end{aligned}$$

Hence, 3 divides $a^2 - 1$, so $a^2 \equiv 1 \pmod 3$.
Therefore, in all cases, $a^2 \equiv 1 \pmod 3$.

Since $a^2 \equiv 1 \pmod 3$ and $a^2 \equiv 1 \pmod 8$ and $lcm(3, 8) = 24$, then $a^2 \equiv 1 \pmod{24}$, by proposition 21. ◻

Exercise 27. If an integer a is both a square and a cube, then $a \equiv 0, 1, 9, or 28 \pmod{36}$.

Proof. TODO ◻

Exercise 28. If a is an odd integer, then $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

Proof. TODO ◻

Exercise 29. Verify that $89|2^{44} - 1$.

Proof. Since $2^{11} \equiv 1 \pmod{89}$, then

$$\begin{aligned} 2^{44} - 1 &= (2^{11})^4 - 1 \\ &\equiv 1^4 - 1 \pmod{89} \\ &\equiv 0 \pmod{89}. \end{aligned}$$

Hence, $2^{44} - 1 \equiv 0 \pmod{89}$, so 89 divides $2^{44} - 1$.
Therefore, $89|2^{44} - 1$. ◻

Exercise 30. Verify that $97|2^{48} - 1$.

Proof. Since $2^{19} \equiv 3 \pmod{97}$, then

$$\begin{aligned} 2^{48} &= (2^{10})(2^{19})^2 \\ &\equiv 2^{10} \cdot 3^2 \pmod{97} \\ &\equiv (2^5 \cdot 3)^2 \pmod{97} \\ &\equiv 96^2 \pmod{97} \\ &\equiv 1 \pmod{97}. \end{aligned}$$

Therefore, $2^{48} \equiv 1 \pmod{97}$, so $97|2^{48} - 1$. ◻

Proposition 31. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.*
If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.

Proof. Suppose $a \equiv b \pmod{n}$.
Then $n|(a-b)$, by definition of congruence modulo, so $a - b = nk$ for $k \in \mathbb{Z}$.
Multiplying both sides by $a+b$ we get $(a-b)(a+b) = nk(a+b)$ so it follows that $a^2 - b^2 = nk(a+b)$.
Since $k(a+b) \in \mathbb{Z}$, then $n|a^2 - b^2$.
Therefore $a^2 \equiv b^2 \pmod{n}$, by definition of congruence modulo. $\square$

Exercise 32. Repeated squares computational technique for $b^e \pmod{m}$
Compute $271^{321} \pmod{481}$.

Solution. We use a repeated squares computational technique to quickly compute $b^e \pmod{m}$ for base b raised to exponent e modulo m.
We express the exponent 321 as a sum of powers of 2.
Thus, $321 = 2^8 + 2^6 + 2^0$.
Observe that

$$\begin{aligned} 271^{321} \pmod{481} &= 271^{2^0+2^6+2^8} \pmod{481} \\ &= (271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8}) \pmod{481}. \end{aligned}$$

We compute powers 2^i for $i = 0, 6, 8$.
$271^{2^1} = 271^2 \equiv 329 \pmod{481}$.
$271^{2^2} = (271^{2^1})^2 \equiv 329^2 \pmod{481} \equiv 16 \pmod{481}$.
$271^{2^3} = (271^{2^2})^2 \equiv 16^2 \pmod{481} \equiv 256 \pmod{481}$.
$271^{2^4} = (271^{2^3})^2 \equiv 256^2 \pmod{481} \equiv 120 \pmod{481}$.
$271^{2^5} = (271^{2^4})^2 \equiv 120^2 \pmod{481} \equiv 451 \pmod{481}$.
$271^{2^6} = (271^{2^5})^2 \equiv 451^2 \pmod{481} \equiv 419 \pmod{481}$.
$271^{2^7} = (271^{2^6})^2 \equiv 419^2 \pmod{481} \equiv 477 \pmod{481}$.
$271^{2^8} = (271^{2^7})^2 \equiv 477^2 \pmod{481} \equiv 16 \pmod{481}$.

Thus, we have
$271^{2^0} \equiv 271 \pmod{481}$
$271^{2^6} \equiv 419 \pmod{481}$
$271^{2^8} \equiv 16 \pmod{481}$

Multiplying we obtain
$(271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8}) \equiv 271 \cdot 419 \cdot 16 \pmod{481}$.

Observe that

$$\begin{aligned}
271^{321} \pmod{481} &= 271^{2^0+2^6+2^8} \pmod{481} \\
&= (271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8}) \pmod{481} \\
&\equiv 271 \cdot 419 \cdot 16 \pmod{481} \\
&\equiv 47 \pmod{481}.
\end{aligned}$$

Therefore, $271^{321} \pmod{481} \equiv 47 \pmod{481}$. $\square$

Exercise 33. Compute $292^{3171} \pmod{582}$.

Solution. We use a repeated squares computational technique to quickly compute $b^e \pmod{m}$ for base b raised to exponent e modulo m.

We express the exponent 3171 as a sum of powers of 2.

Thus, $3171 = 2^0 + 2^1 + 2^5 + 2^6 + 2^{10} + 2^{11}$.

Observe that

$$\begin{aligned}
292^{3171} \pmod{582} &= 292^{2^0+2^1+2^5+2^6+2^{10}+2^{11}} \pmod{582} \\
&= (292^{2^0} \cdot 292^{2^1} \cdot 292^{2^5} \cdot 292^{2^6} \cdot 292^{2^{10}} \cdot 292^{2^{11}}) \pmod{582}.
\end{aligned}$$

We compute powers 2^i for $i = 0, 1, 5, 6, 10, 11$.

$292^{2^1} = 292^2 \equiv 292 \pmod{582}$.

$292^{2^2} = (292^{2^1})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

$292^{2^3} = (292^{2^2})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

$292^{2^4} = (292^{2^3})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

$292^{2^5} = (292^{2^4})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

$292^{2^6} = (292^{2^5})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

$292^{2^7} = (292^{2^6})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

$292^{2^8} = (292^{2^7})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$

$292^{2^9} = (292^{2^7})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$

$292^{2^{10}} = (292^{2^7})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$

$292^{2^{11}} = (292^{2^7})^2 \equiv 292^2 \pmod{582} \equiv 292 \pmod{582}$.

Thus, we have

$292^{2^0} \equiv 292 \pmod{582}$

$292^{2^1} \equiv 292 \pmod{582}$

$292^{2^5} \equiv 292 \pmod{582}$

$292^{2^6} \equiv 292 \pmod{582}$

$292^{2^{10}} \equiv 292 \pmod{582}$

$292^{2^{11}} \equiv 292 \pmod{582}$

Multiplying we obtain

$(292^{2^0} \cdot 292^{2^1} \cdot 292^{2^5} \cdot 292^{2^6} \cdot 292^{2^{10}} \cdot 292^{2^{11}}) \equiv 292^6 \pmod{582}$.

Observe that

$$
\begin{aligned}
292^{3171} \pmod{582} &= 292^{2^0+2^1+2^5+2^6+2^{10}+2^{11}} \pmod{582} \\
&= (292^{2^0} \cdot 292^{2^1} \cdot 292^{2^5} \cdot 292^{2^6} \cdot 292^{2^{10}} \cdot 292^{2^{11}}) \pmod{582} \\
&\equiv 292^6 \pmod{582} \\
&\equiv 292 \pmod{582}.
\end{aligned}
$$

Therefore, $292^{3171} \pmod{582} \equiv 292 \pmod{582}$. $\square$

Exercise 34. Compute $2557^{341} \pmod{5681}$.

Solution. We use a repeated squares computational technique to quickly compute $b^e \pmod{m}$ for base b raised to exponent e modulo m.

We express the exponent 341 as a sum of powers of 2.

Thus, $341 = 2^8 + 2^6 + 2^4 + 2^2 + 2^0$.

Observe that

$$
\begin{aligned}
2557^{341} \pmod{5681} &= 2557^{2^0+2^2+2^4+2^6+2^8} \pmod{5681} \\
&= (2557^{2^0} \cdot 2557^{2^2} \cdot 2557^{2^4} \cdot 2557^{2^6} \cdot 2557^{2^8}) \pmod{5681}.
\end{aligned}
$$

We compute powers 2^i for $i = 0, 2, 4, 6, 8$.

$2557^{2^1} = 2557^2 \equiv 5099 \pmod{5681}$.

$2557^{2^2} = (2557^{2^1})^2 \equiv 5099^2 \pmod{5681} \equiv 3545 \pmod{5681}$.

$2557^{2^3} = (2557^{2^2})^2 \equiv 3545^2 \pmod{5681} \equiv 653 \pmod{5681}$.

$2557^{2^4} = (2557^{2^3})^2 \equiv 653^2 \pmod{5681} \equiv 334 \pmod{5681}$.

$2557^{2^5} = (2557^{2^4})^2 \equiv 334^2 \pmod{5681} \equiv 3617 \pmod{5681}$.

$2557^{2^6} = (2557^{2^5})^2 \equiv 3617^2 \pmod{5681} \equiv 5027 \pmod{5681}$.

$2557^{2^7} = (2557^{2^6})^2 \equiv 5027^2 \pmod{5681} \equiv 1641 \pmod{5681}$.

$2557^{2^8} = (2557^{2^7})^2 \equiv 1641^2 \pmod{5681} \equiv 87 \pmod{5681}$.

Thus, we have

$2557^{2^0} \equiv 2557 \pmod{5681}$

$2557^{2^2} \equiv 3545 \pmod{5681}$

$2557^{2^4} \equiv 334 \pmod{5681}$

$2557^{2^6} \equiv 5027 \pmod{5681}$

$2557^{2^8} \equiv 87 \pmod{5681}$

Multiplying we obtain

$(2557^{2^0} \cdot 2557^{2^2} \cdot 2557^{2^4} \cdot 2557^{2^6} \cdot 2557^{2^8}) \equiv 2557 \cdot 3545 \cdot 334 \cdot 5027 \cdot 87 \pmod{5681}$.

Observe that

$$\begin{aligned}
2557^{341} \pmod{5681} &= 2557^{2^0+2^2+2^4+2^6+2^8} \pmod{5681} \\
&= (2557^{2^0} \cdot 2557^{2^2} \cdot 2557^{2^4} \cdot 2557^{2^6} \cdot 2557^{2^8}) \pmod{5681} \\
&\equiv 2557 \cdot 3545 \cdot 334 \cdot 5027 \cdot 87 \pmod{5681} \\
&\equiv 2876 \pmod{5681}.
\end{aligned}$$

Therefore, $2557^{341} \pmod{5681} \equiv 2876 \pmod{5681}$. □

Exercise 35. Compute $2071^{9521} \pmod{4724}$.

Solution. We use a repeated squares computational technique to quickly compute $b^e \pmod{m}$ for base b raised to exponent e modulo m.

We express the exponent 9521 as a sum of powers of 2.

Thus, $9521 = 2^{13} + 2^{10} + 2^8 + 2^5 + 2^4 + 2^0$.

Observe that

$$\begin{aligned}
2071^{9521} \pmod{4724} &= 2071^{2^0+2^4+2^5+2^8+2^{10}+2^{13}} \pmod{4724} \\
&= (2071^{2^0} \cdot 2071^{2^4} \cdot 2071^{2^5} \cdot 2071^{2^8} \cdot 2071^{2^{10}} \cdot 2071^{2^{13}}) \pmod{4724}.
\end{aligned}$$

We compute powers 2^i for $i = 0, 4, 5, 8, 10, 13$.

$2071^{2^1} = 2071^2 \equiv 4373 \pmod{4724}$.

$2071^{2^2} = (2071^{2^1})^2 \equiv 4373^2 \pmod{4724} \equiv 377 \pmod{4724}$.

$2071^{2^3} = (2071^{2^2})^2 \equiv 377^2 \pmod{4724} \equiv 409 \pmod{4724}$.

$2071^{2^4} = (2071^{2^3})^2 \equiv 409^2 \pmod{4724} \equiv 1941 \pmod{4724}$.

$2071^{2^5} = (2071^{2^4})^2 \equiv 1941^2 \pmod{4724} \equiv 2453 \pmod{4724}$.

$2071^{2^6} = (2071^{2^5})^2 \equiv 2453^2 \pmod{4724} \equiv 3557 \pmod{4724}$.

$2071^{2^7} = (2071^{2^6})^2 \equiv 3557^2 \pmod{4724} \equiv 1377 \pmod{4724}$.

$2071^{2^8} = (2071^{2^7})^2 \equiv 1377^2 \pmod{4724} \equiv 1805 \pmod{4724}$.

$2071^{2^9} = (2071^{2^7})^2 \equiv 1805^2 \pmod{4724} \equiv 3189 \pmod{4724}$.

$2071^{2^{10}} = (2071^{2^7})^2 \equiv 3189^2 \pmod{4724} \equiv 3673 \pmod{4724}$.

$2071^{2^{11}} = (2071^{2^7})^2 \equiv 3673^2 \pmod{4724} \equiv 3909 \pmod{4724}$.

$2071^{2^{12}} = (2071^{2^7})^2 \equiv 3909^2 \pmod{4724} \equiv 2865 \pmod{4724}$.

$2071^{2^{13}} = (2071^{2^7})^2 \equiv 2865^2 \pmod{4724} \equiv 2637 \pmod{4724}$.

Thus, we have

$2071^{2^0} \equiv 2071 \pmod{4724}$

$2071^{2^4} \equiv 1941 \pmod{4724}$

$2071^{2^5} \equiv 2453 \pmod{4724}$

$2071^{2^8} \equiv 1805 \pmod{4724}$

$2071^{2^{10}} \equiv 3673 \pmod{4724}$

$2071^{2^{13}} \equiv 2637 \pmod{4724}$

Multiplying we obtain
$(2071^{2^0} \cdot 2071^{2^4} \cdot 2071^{2^5} \cdot 2071^{2^8} \cdot 2071^{2^{10}} \cdot 2071^{2^{13}}) \equiv 2071 \cdot 1941 \cdot 2453 \cdot 1805 \cdot 3673 \cdot 2637 \pmod{4724}$.

Observe that

$$\begin{aligned}
2071^{9521} \pmod{4724} &= 2071^{2^0+2^4+2^5+2^8+2^{10}+2^{13}} \pmod{4724} \\
&= (2071^{2^0} \cdot 2071^{2^4} \cdot 2071^{2^5} \cdot 2071^{2^8} \cdot 2071^{2^{10}} \cdot 2071^{2^{13}}) \pmod{4724} \\
&\equiv 2071 \cdot 1941 \cdot 2453 \cdot 1805 \cdot 3673 \cdot 2637 \pmod{4724} \\
&\equiv 1523 \pmod{4724}.
\end{aligned}$$

Therefore, $2071^{9521} \pmod{4724} \equiv 1523 \pmod{4724}$. □

Exercise 36. Compute $971^{321} \pmod{765}$.

Solution. We use a repeated squares computational technique to quickly compute $b^e \pmod{m}$ for base b raised to exponent e modulo m.
We express the exponent 321 as a sum of powers of 2.
Thus, $321 = 2^8 + 2^6 + 2^0$.
Observe that

$$\begin{aligned}
971^{321} \pmod{765} &= 971^{2^0+2^6+2^8} \pmod{765} \\
&= (971^{2^0} \cdot 971^{2^6} \cdot 971^{2^8}) \pmod{765}.
\end{aligned}$$

We compute powers 2^i for $i = 0, 6, 8$.
$971^{2^1} = 971^2 \equiv 361 \pmod{765}$.
$971^{2^2} = (971^{2^1})^2 \equiv 361^2 \pmod{765} \equiv 271 \pmod{765}$.
$971^{2^3} = (971^{2^2})^2 \equiv 271^2 \pmod{765} \equiv 1 \pmod{765}$.
$971^{2^4} = (971^{2^3})^2 \equiv 1^2 \pmod{765} \equiv 1 \pmod{765}$.
$971^{2^5} = (971^{2^4})^2 \equiv 1^2 \pmod{765} \equiv 1 \pmod{765}$.
$971^{2^6} = (971^{2^5})^2 \equiv 1^2 \pmod{765} \equiv 1 \pmod{765}$.
$971^{2^7} = (971^{2^6})^2 \equiv 1^2 \pmod{765} \equiv 1 \pmod{765}$.
$971^{2^8} = (971^{2^7})^2 \equiv 1^2 \pmod{765} \equiv 1 \pmod{765}$.

Thus, we have
$971^{2^0} \equiv 971 \pmod{765}$
$971^{2^6} \equiv 1 \pmod{765}$
$971^{2^8} \equiv 1 \pmod{765}$

Multiplying we obtain
$(971^{2^0} \cdot 971^{2^6} \cdot 971^{2^8}) \equiv 971 \cdot 1 \cdot 1 \pmod{765}$.

Observe that

$$\begin{aligned} 971^{321} \pmod{765} &= 971^{2^0+2^6+2^8} \pmod{765} \\ &= (971^{2^0} \cdot 971^{2^6} \cdot 971^{2^8}) \pmod{765} \\ &\equiv 971 \cdot 1 \cdot 1 \pmod{765} \\ &\equiv 206 \pmod{765}. \end{aligned}$$

Therefore, $971^{321} \pmod{765} \equiv 206 \pmod{765}$. $\square$

Exercise 37. If $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$ and $\gcd(b,n) = 1$, then $a \equiv c \pmod{n}$.

Proof. Suppose $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$ and $\gcd(b,n) = 1$.

Observe that

$$\begin{aligned} b \equiv d \pmod{n} &\Rightarrow bc \equiv dc \pmod{n} \\ &\Rightarrow bc \equiv cd \pmod{n} \\ &\Rightarrow cd \equiv bc \pmod{n} \\ &\Rightarrow ab \equiv bc \pmod{n} \\ &\Rightarrow ab \equiv cb \pmod{n}. \end{aligned}$$

Since $ab \equiv cb \pmod{n}$ and $\gcd(n,b) = 1$, then by cancellation, we have $a \equiv c \pmod{n}$. $\square$

Exercise 38. If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$ and $n = \gcd(n_1, n_2)$, then $b \equiv c \pmod{n}$.

Proof. Suppose $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$ and $n = \gcd(n_1, n_2)$.

Then $n_1 | a - b$ and $n_2 | a - c$ and $n | n_1$ and $n | n_2$.

Since $n | n_1$ and $n_1 | a - b$, then $n | a - b$.

Since $n | n_2$ and $n_2 | a - c$, then $n | a - c$.

Since n is a common divisor of $a - b$ and $a - c$, then n divides any linear combination of $a - b$ and $a - c$.

Since $(-1)(a-b)+(1)(a-c) = -a+b+a-c = b-c$ is a linear combination of $a - b$ and $a - c$, then n divides $b - c$.

Therefore, $b \equiv c \pmod{n}$. $\square$

Linear Congruences

Exercise 39. Solve the linear congruence $3x \equiv 2 \pmod{7}$.

Solution. Let $d = \gcd(3, 7)$.

Since $d = 1$ and $1|2$, then a solution exists.

There are $d = 1$ distinct solutions modulo 7 and the solution is congruent modulo $\frac{7}{d} = \frac{7}{1} = 7$.

A particular solution is $x_0 = 3$.

The general solution x is in the set $3 + 7\mathbb{Z} = \{3 + 7k : k \in \mathbb{Z}\}$.

Let S be the solution set to the linear congruence.

Then $S = \{x \in \mathbb{Z} : 3x \equiv 2 \pmod 7\}$.

Let $x \in S$.

Then $x \in \mathbb{Z}$ and $3x \equiv 2 \pmod 7$, so $[3x] = [2]$.

Hence, $[3][x] = [2]$.

Since $\gcd(3, 7) = 1$, then $[3] \in \mathbb{Z}_7$ has a multiplicative inverse and $[3]^{-1} = [5]$, so $[3][5] = [5][3] = [1]$ modulo 7.

For convenience, we have $3x = 2$ and $3 * 5 = 5 * 3 = 1$.

Observe that

$$\begin{aligned} 3x &= 2 \\ 5 * 3x &= 5 * 2 \\ 1x &= 10 \\ x &= 3. \end{aligned}$$

Therefore, $[x] = [3]$, so $x \in [3]$.

Since $[3] = 3 + 7\mathbb{Z} = \{3 + 7k : k \in \mathbb{Z}\}$, then $x \in 3 + 7\mathbb{Z}$.

Thus, $x \in S$ implies $x \in 3 + 7\mathbb{Z}$, so S is a subset of $3 + 7\mathbb{Z}$.

We prove the set $3 + 7\mathbb{Z}$ is a subset of S.

Let $y \in 3 + 7\mathbb{Z}$.

Then $y = 3 + 7k$ for some integer k, so $y \in \mathbb{Z}$.

Observe that $3y - 2 = 3(3 + 7k) - 2 = 9 + 21k - 2 = 21k + 7 = 7(3k + 1)$.

Since $3k + 1 \in \mathbb{Z}$, then 7 divides the difference $3y - 2$, so $3y \equiv 2 \pmod 7$.

Since $y \in \mathbb{Z}$ and $3y \equiv 2 \pmod 7$, then $y \in S$, so $3 + 7\mathbb{Z}$ is a subset of S.

Since S is a subset of $3+7\mathbb{Z}$ and $3+7\mathbb{Z}$ is a subset of S, then $S = 3+7\mathbb{Z}$. $\square$

Exercise 40. Solve the linear congruence $5x + 1 \equiv 13 \pmod{23}$.

Solution. Suppose $5x + 1 \equiv 13 \pmod{23}$.

Then $5x \equiv 12$.

Let $d = \gcd(5, 23)$.

Since $d = 1$ and $1|12$, then a solution exists.

There are $d = 1$ distinct solutions modulo 23 and the solution is congruent modulo $\frac{23}{d} = \frac{23}{1} = 23$.

A particular solution is $x_0 = 7$.

The general solution x is in the set $7 + 23\mathbb{Z} = \{7 + 23k : k \in \mathbb{Z}\}$.

Let S be the solution set to the linear congruence.

Then $S = \{x \in \mathbb{Z} : 5x + 1 \equiv 13 \pmod{23}\}$.

Let $x \in S$.

Then $x \in \mathbb{Z}$ and $5x + 1 \equiv 13 \pmod{23}$, so $5x \equiv 12$

Thus, $[5x] = [12]$, so $[5[]x] = [12]$.

Since $\gcd(5, 23) = 1$, then $[5] \in \mathbb{Z}_{23}$ has a multiplicative inverse and $[5]^{-1} = [14]$, so $[5][14] = [14][5] = [1]$ modulo 23.

For convenience, we have $5x = 12$ and $5 * 14 = 14 * 5 = 1$.
Observe that

$$\begin{aligned} 5x &= 12 \\ 14 * 5x &= 14 * 12 \\ 1x &= 168 \\ x &= 7. \end{aligned}$$

Therefore, $[x] = [7]$, so $x \in [7]$.
Since $[7] = 7 + 23\mathbb{Z} = \{7 + 23k : k \in \mathbb{Z}\}$, then $x \in 7 + 23\mathbb{Z}$.
Thus, $x \in S$ implies $x \in 7 + 23\mathbb{Z}$, so S is a subset of $7 + 23\mathbb{Z}$.

We prove $7 + 23\mathbb{Z}$ is a subset of S.
Let $y \in 7 + 23\mathbb{Z}$.
Then $y = 7 + 23k$ for some integer k, so $y \in \mathbb{Z}$.
Observe that $(5y+1) - 13 = (5(7+23k)+1) - 13 = (35+115k+1) - 13 = 115k + 23 = 23(5k+1)$.
Since $5k + 1 \in \mathbb{Z}$, then 23 divides the difference $(5y+1) - 13$, so $5y + 1 \equiv 13 \pmod{23}$.
Since $y \in \mathbb{Z}$ and $5y + 1 \equiv 13 \pmod{23}$, then $y \in S$, so $7 + 23\mathbb{Z}$ is a subset of S.

Since S is a subset of $7+23\mathbb{Z}$ and $7+23\mathbb{Z}$ is a subset of S, then $S = 7+23\mathbb{Z}$.
$\square$

Exercise 41. Solve the linear congruence $5x + 1 \equiv 13 \pmod{26}$.

Solution. Suppose $5x + 1 \equiv 13 \pmod{26}$.
Then $5x \equiv 12$.
Let $d = \gcd(5, 26)$.
Since $d = 1$ and $1|12$, then a solution exists.
There are $d = 1$ distinct solutions modulo 26 and the solution is congruent modulo $\frac{26}{d} = \frac{26}{1} = 26$.
A particular solution is $x_0 = 18$.
The general solution x is in the set $18 + 26\mathbb{Z} = \{18 + 26k : k \in \mathbb{Z}\}$.

Let S be the solution set to the linear congruence.
Then $S = \{x \in \mathbb{Z} : 5x + 1 \equiv 13 \pmod{26}\}$.
Let $x \in S$.
Then $x \in \mathbb{Z}$ and $5x + 1 \equiv 13 \pmod{26}$, so $5x \equiv 12$.
Hence, $[5x] = [12]$, so $[5[]x] = [12]$.
Since $\gcd(5, 26) = 1$, then $[5] \in \mathbb{Z}_{26}$ has a multiplicative inverse and $[5]^{-1} = [21]$, so $[5][21] = [21][5] = [1]$ modulo 26.
For convenience, we have $5x = 12$ and $5 * 21 = 21 * 5 = 1$.

Observe that

$$\begin{aligned} 5x &= 12 \\ 21 * 5x &= 21 * 12 \\ 1x &= 252 \\ x &= 18. \end{aligned}$$

Therefore, $[x] = [18]$, so $x \in [18]$.
Since $[18] = 18 + 26\mathbb{Z} = \{18 + 26k : k \in \mathbb{Z}\}$, then $x \in 18 + 26\mathbb{Z}$.
Thus, $x \in S$ implies $x \in 18 + 26\mathbb{Z}$, so S is a subset of $18 + 26\mathbb{Z}$.

We prove $18 + 26\mathbb{Z}$ is a subset of S.
Let $y \in 18 + 26\mathbb{Z}$.
Then $y = 18 + 26k$ for some integer k, so $y \in \mathbb{Z}$.
Observe that $(5y+1) - 13 = [5(18+26k)+1] - 13 = (90+130k+1) - 13 = 130k + 78 = 26(5k+3)$.
Since $5k+3 \in \mathbb{Z}$, then 26 divides the difference $(5y+1) - 13$, so $5y+1 \equiv 13 \pmod{26}$.
Since $y \in \mathbb{Z}$ and $5y + 1 \equiv 13 \pmod{26}$, then $y \in S$, so $18 + 26\mathbb{Z}$ is a subset of S.

Since S is a subset of $18 + 26\mathbb{Z}$ and $18 + 26\mathbb{Z}$ is a subset of S, then $S = 18 + 26\mathbb{Z}$. $\square$

Exercise 42. Solve the linear congruence $9x \equiv 3 \pmod 5$.

Solution. Let S be the solution set of the linear congruence.
Then $S = \{x \in \mathbb{Z} : 9x \equiv 3 \pmod 5\}$.
Let $x \in S$.
Then $x \in \mathbb{Z}$ and $9x \equiv 3 \pmod 5$.
Since $9 \equiv 4 \pmod 5$, then $9x \equiv 4x \pmod 5$, so $4x \equiv 9x \pmod 5$.
Since $4x \equiv 9x \pmod 5$ and $9x \equiv 3 \pmod 5$, then $4x \equiv 3 \pmod 5$, so $[4x] = [3]$.
Hence, $[4][x] = [3]$.
Since $\gcd(4, 5) = 1$, then $[4] \in \mathbb{Z}_5$ has a multiplicative inverse and $[4]^{-1} = [4]$, so $[4][4] = [1]$.
For convenience, we have $4x = 3$ and $4 * 4 = 1$.
Observe that

$$\begin{aligned} 4x &= 3 \\ 4 * 4x &= 4 * 3 \\ 1x &= 12 \\ x &= 2. \end{aligned}$$

Therefore, $[x] = [2]$, so $x \in [2]$.
Since $[2] = 2 + 5\mathbb{Z} = \{2 + 5k : k \in \mathbb{Z}\}$, then $x \in 2 + 5\mathbb{Z}$.
Thus, $x \in S$ implies $x \in 2 + 5\mathbb{Z}$, so S is a subset of $2 + 5\mathbb{Z}$.

We prove $2+5\mathbb{Z}$ is a subset of S.
Let $y \in 2+5\mathbb{Z}$.
Then $y = 2+5k$ for some integer k, so $y \in \mathbb{Z}$.
Observe that

$$\begin{aligned} 9y-3 &= 9(2+5k)-3 \\ &= 18+45k-3 \\ &= 45k+15 \\ &= 5(9k+3). \end{aligned}$$

Since $9k+3 \in \mathbb{Z}$, then 5 divides the difference $9y-3$, so $9y \equiv 3 \pmod 5$.
Since $y \in \mathbb{Z}$ and $9y \equiv 3 \pmod 5$, then $y \in S$, so $2+5\mathbb{Z}$ is a subset of S.

Since S is a subset of $2+5\mathbb{Z}$ and $2+5\mathbb{Z}$ is a subset of S, then $S = 2+5\mathbb{Z}$. $\square$

Exercise 43. Solve the linear congruence $5x \equiv 1 \pmod 6$.

Solution. Let S be the solution set of the linear congruence.
Then $S = \{x \in \mathbb{Z} : 5x \equiv 1 \pmod 6\}$.
Let $x \in S$.
Then $x \in \mathbb{Z}$ and $5x \equiv 1 \pmod 6$, so $[5x] = [1]$.
Hence, $[5][x] = [1]$.
Since $\gcd(5,6) = 1$, then $[5] \in \mathbb{Z}_6$ has a multiplicative inverse and $[5]^{-1} = [5]$, so $[5][5] = [1]$.
For convenience, we have $5x = 1$ and $5 * 5 = 1$.
Observe that

$$\begin{aligned} 5x &= 1 \\ 5 * 5x &= 5 * 1 \\ 1x &= 5 \\ x &= 5. \end{aligned}$$

Therefore, $[x] = [5]$, so $x \in [5]$.
Since $[5] = 5+6\mathbb{Z} = \{5+6k : k \in \mathbb{Z}\}$, then $x \in 5+6\mathbb{Z}$.
Thus, $x \in S$ implies $x \in 5+6\mathbb{Z}$, so S is a subset of $5+6\mathbb{Z}$.

We prove $5+6\mathbb{Z}$ is a subset of S.
Let $y \in 5+6\mathbb{Z}$.
Then $y = 5+6k$ for some integer k, so $y \in \mathbb{Z}$.
Observe that

$$\begin{aligned} 5y-1 &= 5(5+6k)-1 \\ &= 25+30k-1 \\ &= 30k+24 \\ &= 6(5k+4). \end{aligned}$$

Since $5k+4 \in \mathbb{Z}$, then 6 divides the difference $5y-1$, so $5y \equiv 1 \pmod 6$.
Since $y \in \mathbb{Z}$ and $5y \equiv 1 \pmod 6$, then $y \in S$, so $5+6\mathbb{Z}$ is a subset of S.

Since S is a subset of $5+6\mathbb{Z}$ and $5+6\mathbb{Z}$ is a subset of S, then $S = 5+6\mathbb{Z}$. $\square$

Exercise 44. Solve the linear congruence $3x \equiv 1 \pmod 6$.

Solution. Let S be the solution set of the linear congruence.

Then $S = \{x \in \mathbb{Z} : 3x \equiv 1 \pmod 6\}$.

Let $x \in S$.

Then $x \in \mathbb{Z}$ and $3x \equiv 1 \pmod 6$, so $[3x] = [1]$.

Hence, $[3][x] = [1]$.

Since $\gcd(3, 6) = 3 \neq 1$, then $[3] \in \mathbb{Z}_6$ does not have a multiplicative inverse in $\mathbb{Z}_6$.

Thus, there is no solution to $[3][x] = [1]$, so there is no solution to the linear congruence.

Therefore, $S = \emptyset$. $\square$

Exercise 45. Solve the linear congruence $18x \equiv 30 \pmod{42}$.

Solution. Since $\gcd(18, 42) = 6$ and $6|30$, then the linear congruence has a solution and there are exactly 6 distinct solutions modulo 42 and these solutions are congruent modulo $\frac{42}{6} = 7$.

A particular solution is $x_0 = 4$.

The 6 distinct solutions are given by $x = 4 + \frac{-42}{6}t = 4 - 7t$ for some integer t.

Equivalently, the 6 solutions modulo 42 are in the solution set $\{4, 11, 18, 25, 32, 39\}$ $\square$

Exercise 46. Solve the linear congruence $9x \equiv 21 \pmod{30}$.

Solution. Since $\gcd(9, 30) = 3$ and $3|21$, then the linear congruence has a solution and there are exactly 3 distinct solutions modulo 30 and these solutions are congruent modulo $\frac{30}{3} = 10$.

A particular solution is $x_0 = 9$.

The 3 distinct solutions are given by $x = 9 + 10t$ for some integer t.

Equivalently, the 3 solutions modulo 30 are in the solution set $\{9, 19, 29\}$. $\square$

Exercise 47. Solve the linear congruence $25x \equiv 15 \pmod{29}$.

Solution. Since $\gcd(25, 29) = 1$ and $1|15$, then the linear congruence has a solution and there is exactly 1 distinct solution modulo 29 and the solution is congruent modulo $\frac{29}{1} = 29$.

Since $5 \cdot 5x \equiv 5 \cdot 3 \pmod{29}$ and $\gcd(29, 5) = 1$, then we may cancel 5 to obtain $5x \equiv 3 \pmod{29}$.

Since $\gcd(5, 29) = 1$ and $1|15$, then the linear congruence has a solution and there is exactly 1 distinct solution modulo 29 and the solution is congruent modulo $\frac{29}{1} = 29$.

Since $5 * 6 \equiv 1 \pmod{29}$, then we multiply by 6 to obtain $6(5x) \equiv 6 * 3 \pmod{29}$, so $1x \equiv 18 \pmod{29}$.

Therefore, $x \equiv 18 \pmod{29}$.

A particular solution is $x_0 = 18$.

The 1 distinct solution is given by $x = 18 + 29t$ for some integer t.

Equivalently, the 1 solution modulo 29 is in the solution set $\{18\}$. $\square$

Exercise 48. Solve the linear congruence $5x \equiv 2 \pmod{26}$.

Solution. Since $\gcd(5, 26) = 1$ and $1|2$, then the linear congruence has a solution and there is exactly 1 distinct solution modulo 26 and the solution is congruent modulo $\frac{26}{1} = 26$.

Since $5 * 21 \equiv 1 \pmod{26}$, then we multiply by 21 to obtain $21(5x) \equiv 21 * 2 \pmod{26}$, so $x \equiv 21 * 2 \pmod{26}$.

Therefore, $x \equiv 42 \pmod{26} \equiv 16 \pmod{26}$.

A particular solution is $x_0 = 16$.

The 1 distinct solution is given by $x = 16 + 26t$ for some integer t.

Equivalently, the 1 solution modulo 26 is in the solution set $\{16\}$. $\square$

Exercise 49. Solve the linear congruence $6x \equiv 15 \pmod{21}$.

Solution. Since $\gcd(6, 21) = 3$ and $3|15$, then the linear congruence has a solution and there are exactly 3 distinct solutions modulo 21 and the solutions are congruent modulo $\frac{21}{3} = 7$.

Since $6x = 3 * 2 * x \equiv 3 * 5 \pmod{21}$ and $\gcd(21, 3) = 3$, then $2x \equiv 5 \pmod{\frac{21}{3}}$, so $2x \equiv 5 \pmod{7}$.

Since $\gcd(2, 7) = 1$ and $1|5$, then the linear congruence has a solution and there is exactly 1 distinct solution modulo 7 and the solution is congruent modulo $\frac{7}{1} = 7$.

Since $2 * 4 \equiv 1 \pmod{7}$, then we multiply by 4 to obtain $4(2x) \equiv 4 * 5 \pmod{7}$, so $x \equiv 20 \pmod{7}$.

Therefore, $x \equiv 6 \pmod{7}$.

A particular solution is $x_0 = 6$.

The 3 distinct solutions are given by $x = 6 + 7t$ for some integer t.

Equivalently, the 3 solutions modulo 21 are in the solution set $\{6, 13, 20\}$. $\square$

Exercise 50. Solve the linear congruence $36x \equiv 8 \pmod{102}$.

Solution. Since $\gcd(36, 102) = 6$ and $6 \nmid 8$, then the linear congruence does not have a solution. $\square$

Exercise 51. Solve the linear congruence $34x \equiv 60 \pmod{98}$.

Solution. Since $\gcd(34, 98) = 2$ and $2|60$, then the linear congruence has a solution and there are exactly 2 distinct solutions modulo 98 and the solutions are congruent modulo $\frac{98}{2} = 49$.

Since $34x \equiv 60 \pmod{98}$ implies $2 * 17x \equiv 2 * 30 \pmod{98}$ and $\gcd(98, 2) = 2$, then we cancel to obtain $17x \equiv 30 \pmod{49}$.

Since $\gcd(17, 49) = 1$ and $1|30$, then the linear congruence has a solution and there is exactly 1 distinct solution modulo 49 and the solution is congruent modulo $\frac{49}{1} = 49$.

The multiplicative inverse of 17 is 26 modulo 49, so $17 * 26 \equiv 1 \pmod{49}$.

Thus, $17 * 26x \equiv x \pmod{49}$ and $26 * 17x \equiv 26 * 30 \pmod{49}$.

Since $17 * 26x \equiv x \pmod{49}$, then $x \equiv 17 * 26x \pmod{49}$.

Since $x \equiv 17*26x \pmod{49}$ and $26*17x \equiv 26*30 \pmod{49}$, then $x \equiv 26*30 \pmod{49} \equiv 780 \pmod{49} \equiv 45 \pmod{49}$.

Therefore, $x \equiv 45 \pmod{49}$.

A particular solution is $x_0 = 45$.

The 2 distinct solutions are given by $x = 45 + 49t$ for some integer t.

Equivalently, the 2 solutions modulo 98 are in the solution set $\{45, 94\}$. $\square$

Exercise 52. Solve the linear congruence $140x \equiv 133 \pmod{301}$.

Solution. Since $\gcd(140, 301) = 7$ and $7|133$, then the linear congruence has a solution and there are exactly 7 distinct solutions modulo 301 and the solutions are congruent modulo $\frac{301}{7} = 43$.

Since $140x \equiv 133 \pmod{301}$ implies $7*20x \equiv 7*19 \pmod{301}$ and $\gcd(301, 7) = 7$, then we cancel to obtain $20x \equiv 19 \pmod{43}$.

Since $\gcd(20, 43) = 1$ and $1|19$, then the linear congruence has a solution and there is exactly 1 distinct solution modulo 43 and the solution is congruent modulo $\frac{43}{1} = 43$.

The multiplicative inverse of 20 is 28 modulo 43, so $20 * 28 \equiv 1 \pmod{43}$.

Thus, $20 * 28x \equiv x \pmod{43}$ and $28 * 20x \equiv 28 * 19 \pmod{43}$.

Since $20 * 28x \equiv x \pmod{43}$, then $x \equiv 20 * 28x \pmod{43}$.

Since $x \equiv 20*28x \pmod{43}$ and $28*20x \equiv 28*19 \pmod{43}$, then $x \equiv 28*19 \pmod{43} \equiv 532 \pmod{43} \equiv 16 \pmod{43}$.

Therefore, $x \equiv 16 \pmod{43}$.

A particular solution is $x_0 = 16$.

The 7 distinct solutions are given by $x = 16 + 43t$ for some integer t.

Equivalently, the 7 solutions modulo 301 are in the solution set $\{16, 59, 102, 145, 188, 231, 274\}$. $\square$

Exercise 53. Solve the linear Diophantine equation using congruences : $4x + 51y = 9$.

Solution. Since $\gcd(4, 51) = 1$ and $1|9$, then the linear Diophantine equation has a solution.

Since $4x + 51y = 9$, then $4x = 9 - 51y$, so $4|(9 - 51y)$.

Hence, $9 \equiv 51y \pmod{4}$, so $51y \equiv 9 \pmod{4}$.

Since $\gcd(51, 4) = 1$ and $1|9$, then the linear congruence has exactly one solution modulo 4.

Since $51 * 3 \equiv 1 \pmod{4}$, then $51 * 3y \equiv y \pmod{4}$ and $3 * 51y \equiv 3 * 9 \pmod{4}$, so $y \equiv 3 * 9 \pmod{4} \equiv 27 \pmod{4} \equiv 3 \pmod{4}$.

Hence, $y_0 = 3$ is a solution and $x_0 = \frac{9-51*3}{4} = -36$ is a solution.

The general solution of the linear Diophantine equation is given by $x = -36 + \frac{51}{\gcd(4,51)} * t = -36 + 51t$ and $y = 3 - \frac{4}{\gcd(4,51)} * t = 3 - 4t$ for some integer t.

Therefore, the solution set to the linear Diophantine equation is $\{(-36 + 51t, 3 - 4t) : t \in \mathbb{Z}\}$. $\square$

Solution. Since $4x + 51y = 9$, then $4x = 9 - 51y$, so $4|(9 - 51y)$.

Hence, $9 \equiv 51y \pmod 4$, so $51y \equiv 9 \pmod 4$.

Since $\gcd(51,4) = 1$ and $1|9$, then the linear congruence has exactly one solution modulo 4 and the solution is congruent modulo $\frac{4}{1} = 4$.

Since $51 * 3 \equiv 1 \pmod 4$, then $51 * 3y \equiv y \pmod 4$ and $3 * 51y \equiv 3 * 9 \pmod 4$, so $y \equiv 3 * 9 \pmod 4 \equiv 27 \pmod 4 \equiv 3 \pmod 4$.

Hence, $y = 3 + 4s$ is a solution to the linear congruence for some integer s.

Since $4x + 51y = 9$, then $51y = 9 - 4x$, so $51|9 - 4x$.

Hence, $9 \equiv 4x \pmod{51}$, so $4x \equiv 9 \pmod{51}$.

Since $\gcd(4,51) = 1$ and $1|9$, then the linear congruence has exactly one solution modulo 51 and the solution is congruent modulo $\frac{51}{1} = 51$.

Since $4 * 13 \equiv 1 \pmod{51}$, then $4 * 13x \equiv x \pmod{51}$ and $13 * 4x \equiv 13 * 9 \pmod{51}$, so $x \equiv 13 * 9 \pmod{51} \equiv 117 \pmod{51} \equiv 15 \pmod{51}$.

Thus, $x = 15 + 51t$ is a solution to the linear congruence for some integer t.

Since $x = 15 + 51t$ and $y = 3 + 4s$ and $4x + 51y = 9$, then we substitute to get $4(15 + 51t) + 51(3 + 4s) = 9$, or equivalently, $t + s = -1$.

Since $t = -1 - s$ and $x = 15 + 51t$, then $x = 15 + 51(-1 - s) = -36 - 51s$.

Hence, $x = -36 - 51s$ and $y = 3 + 4s$ for some integer s.

Therefore, the solution set to the linear Diophantine equation is $\{(-36 - 51s, 3 + 4s) : s \in \mathbb{Z}\}$. $\square$

Exercise 54. Solve the linear Diophantine equation using congruences : $12x + 25y = 331$.

Solution. Since $\gcd(12,25) = 1$ and $1|331$, then the linear Diophantine equation has a solution.

Since $12x + 25y = 331$, then $12x = 331 - 25y$, so $12|(331 - 25y)$.

Hence, $331 \equiv 25y \pmod{12}$, so $25y \equiv 331 \pmod{12}$.

Since $\gcd(25,12) = 1$ and $1|331$, then the linear congruence has exactly one solution modulo 4 and the solution is congruent modulo $\frac{4}{1} = 4$.

Since $25 * 1 \equiv 1 \pmod{12}$, then $25 * 1y \equiv 1 * y \pmod{12}$, so $25y \equiv y \pmod{12}$.

Hence, $y \equiv 25y \pmod{12}$.

Since $25y \equiv 331 \pmod{12}$, then $y \equiv 331 \pmod{12} \equiv 7 \pmod{12}$.

Hence, $y_0 = 7$ is a solution and $x_0 = \frac{331 - 25*7}{12} = 13$ is a solution.

The general solution of the linear Diophantine equation is given by $x = 13 + \frac{25}{\gcd(12,25)} * t = 13 + 25t$ and $y = 7 - \frac{12}{\gcd(12,25)} * t = 7 - 12t$ for some integer t.

Therefore, the solution set to the linear Diophantine equation is $\{(13 + 25t, 7 - 12t) : t \in \mathbb{Z}\}$. $\square$

Solution. Since $12x + 25y = 331$, then $12x = 331 - 25y$, so $12|(331 - 25y)$.

Hence, $331 \equiv 25y \pmod{12}$, so $25y \equiv 331 \pmod{12}$.

Since $\gcd(25,12) = 1$ and $1|331$, then the linear congruence has exactly one solution modulo 12 and the solution is congruent modulo $\frac{12}{1} = 12$.

Since $25 * 1 \equiv 1 \pmod{12}$, then $25 * 1y \equiv 1 * y \pmod{12}$, so $25y \equiv y \pmod{12}$.

Hence, $y \equiv 25y \pmod{12}$.

Since $y \equiv 25y \pmod{12}$ and $25y \equiv 331 \pmod{12}$, then $y \equiv 331 \pmod{12} \equiv 7 \pmod{12}$.

Thus, $y = 7 + 12s$ is a solution to the linear congruence for some integer s.

Since $12x + 25y = 331$, then $25y = 331 - 12x$, so $25|331 - 12x$.

Hence, $331 \equiv 12x \pmod{25}$, so $12x \equiv 331 \pmod{25}$.

Since $\gcd(12, 25) = 1$ and $1|331$, then the linear congruence has exactly one solution modulo 25 and the solution is congruent modulo $\frac{25}{1} = 25$.

Since $12*23 \equiv 1 \pmod{25}$, then $12*23x \equiv x \pmod{25}$ and $23*12x \equiv 23*331 \pmod{25}$, so $x \equiv 23 * 331 \pmod{25} \equiv 7613 \pmod{25} \equiv 13 \pmod{25}$.

Thus, $x = 13 + 25t$ is a solution to the linear congruence for some integer t.

Since $x = 13 + 25t$ and $y = 7 + 12s$ and $12x + 25y = 331$, then we substitute to get $12(13 + 25t) + 25(7 + 12s) = 331$, or equivalently, $t + s = 0$.

Since $t + s = 0$, then $s = -t$, so $y = 7 + 12s = 7 + 12(-t) = 7 - 12t$.

Hence, $x = 13 + 25t$ and $y = 7 - 12t$ for some integer t.

Therefore, the solution set to the linear Diophantine equation is $\{(13 + 25t, 7 - 12t) : t \in \mathbb{Z}\}$. $\square$

Exercise 55. Solve the linear Diophantine equation using congruences : $5x - 53y = 17$.

Solution. Since $\gcd(5, -53) = 1$ and $1|17$, then the linear Diophantine equation has a solution.

Since $5x - 53y = 17$, then $5x = 53y + 17$, so $5|53y - (-17)$.

Hence, $53y \equiv -17 \pmod{5} \equiv 3 \pmod{5}$.

Since $\gcd(53, 5) = 1$ and $1|3$, then the linear congruence has exactly one solution modulo 5 and the solution is congruent modulo $\frac{5}{1} = 5$.

Since $53 * 2 \equiv 1 \pmod{5}$, then $53 * 2y \equiv 1 * y \pmod{5}$, so $53 * 2y \equiv y \pmod{5}$.

Hence, $y \equiv 53 * 2y \pmod{5}$.

Since $53y \equiv 3 \pmod{5}$, then $2 * 53y \equiv 2 * 3 \pmod{5}$.

Since $y \equiv 53 * 2y \pmod{5}$ and $2 * 53y \equiv 2 * 3 \pmod{5}$, then $y \equiv 2 * 3 \pmod{5} \equiv 6 \pmod{5} \equiv 1 \pmod{5}$.

Thus, $y_0 = 1$ is a solution and $x_0 = \frac{53(1)+17}{5} = 14$ is a solution.

The general solution of the linear Diophantine equation is given by $x = 14 + \frac{-53}{\gcd(5,-53)} * t = 14 - 53t$ and $y = 1 - \frac{5}{\gcd(5,-53)} * t = 1 - 5t$ for some integer t.

Therefore, the solution set to the linear Diophantine equation is $\{(14 - 53t, 1 - 5t) : t \in \mathbb{Z}\}$. $\square$

Solution. Since $5x - 53y = 17$, then $5x = 53y + 17$, so $5|53y - (-17)$.

Hence, $53y \equiv -17 \pmod{5} \equiv 3 \pmod{5}$.

Since $\gcd(53, 5) = 1$ and $1|3$, then the linear congruence has exactly one solution modulo 5 and the solution is congruent modulo $\frac{5}{1} = 5$.

Since $53 * 2 \equiv 1 \pmod{5}$, then $53 * 2y \equiv 1 * y \pmod{5}$, so $53 * 2y \equiv y \pmod{5}$.

Hence, $y \equiv 53 * 2y \pmod{5}$.

Since $53y \equiv 3 \pmod{5}$, then $2 * 53y \equiv 2 * 3 \pmod{5}$.

Since $y \equiv 53 * 2y \pmod{5}$ and $2 * 53y \equiv 2 * 3 \pmod{5}$, then $y \equiv 2 * 3 \pmod{5} \equiv 6 \pmod{5} \equiv 1 \pmod{5}$.

Thus, $y = 1 + 5s$ is a solution to the linear congruence for some integer s.

Since $5x - 53y = 17$, then $53y = 5x - 17$, so $53|5x - 17$.

Hence, $5x \equiv 17 \pmod{53}$.

Since $\gcd(5, 53) = 1$ and $1|17$, then the linear congruence has exactly one solution modulo 53 and the solution is congruent modulo $\frac{53}{1} = 53$.

Since $5 * 32 \equiv 1 \pmod{53}$, then $5 * 32x \equiv x \pmod{53}$ and $32 * 5x \equiv 32 * 17 \pmod{53}$, so $x \equiv 32 * 17 \pmod{53} \equiv 544 \pmod{53} \equiv 14 \pmod{53}$.

Thus, $x = 14 + 53t$ is a solution to the linear congruence for some integer t.

Since $x = 14 + 53t$ and $y = 1 + 5s$ and $5x - 53y = 17$, then we substitute to get $5(14 + 53t) - 53(1 + 5s) = 17$, or equivalently, $t = s$.

Hence, $x = 14 + 53t$ and $y = 1 + 5t$ for some integer t.

Therefore, the solution set to the linear Diophantine equation is $\{(14 + 53t, 1 + 5t) : t \in \mathbb{Z}\}$. □

Exercise 56. Solve the linear congruence : $3x - 7y \equiv 11 \pmod{13}$.

Solution. Let's try breaking up the congruence into two congruences.

One congruence is $3x \equiv 0 \pmod{13}$.

Second congruence is $-7y \equiv 11 \pmod{13}$.

Can we solve these independently?

Let's solve $3x \equiv 0 \pmod{13}$.

Since $3x \equiv 3*0 \pmod{13}$ and $\gcd(13, 3) = 1$, then we cancel to obtain $x \equiv 0 \pmod{13}$.

Thus, $x = 13s$ for some integer s.

Let's solve $-7y \equiv 11 \pmod{13}$.

Since $-7y \equiv 11 \pmod{13}$, then $7y \equiv -11 \pmod{13} \equiv 2 \pmod{13}$.

Since $\gcd(7, 13) = 1$ and $1|2$, then the linear congruence has a unique solution modulo 13 and the solution is congruent modulo $\frac{13}{1} = 13$.

Since $7 * 2 \equiv 1 \pmod{13}$, then $7 * 2y \equiv y \pmod{13}$ and $2 * 7y \equiv 2 * 2 \pmod{13}$, so $y \equiv 2 * 2 \pmod{13} \equiv 4 \pmod{13}$.

Thus, $y = 4 + 13t$ for some integer t.

So, we think the solution set is $\{(13s, 4+13t) : s,t \in \mathbb{Z}\}$. $\square$

Exercise 57. Solve the system of linear congruences:
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

Solution. Using the Chinese Remainder Theorem, we let $n = 3*5*7 = 105$ and let $N_k = \frac{n}{n_k}$, where $n_1 = 3$ and $n_2 = 5$ and $n_3 = 7$ and $a_1 = 2$ and $a_2 = 3$ and $a_3 = 2$.

For $N_1 = \frac{3*5*7}{3} = 35$, we solve the linear congruence $35x \equiv 1 \pmod 3$ which has solution $x_1 = 2$.

For $N_2 = \frac{3*5*7}{5} = 21$, we solve the linear congruence $21x \equiv 1 \pmod 5$ which has solution $x_2 = 1$.

For $N_3 = \frac{3*5*7}{7} = 15$, we solve the linear congruence $15x \equiv 1 \pmod 7$ which has solution $x_3 = 1$.

The solution is $x = \sum a_k N_k x_k = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 2(35)(2) + 3(21)(1) + 2(15)(1) = 233 \equiv 233 \pmod{105} \equiv 23 \pmod{105}$. $\square$

Exercise 58. Solve the system of linear congruence: $17x \equiv \pmod{276}$.

Solution. TODO Start here $\square$

Exercise 59. Let b, d, d', p be arbitrary integers.
If $bd \equiv bd' \pmod p$, where p is prime and $p \nmid b$, then $d \equiv d' \pmod p$.

Proof. Suppose $bd \equiv bd' \pmod p$ and p is prime and $p \nmid b$.
Then $p|(bd - bd')$, so $p|b(d-d')$.
Since p is prime, then the only positive divisors of p are 1 and p.
Since $p \nmid b$, then 1 is the only positive divisor of both p and b.
Therefore, p and b are relatively prime, so $\gcd(p,b) = 1$.
Since $\gcd(p,b) = 1$ and $p|b(d-d')$, then $p|d-d'$.
Hence, $d \equiv d' \pmod p$. $\square$

Exercise 60. Let a, b, k be arbitrary integers with $k > 0$.
If $|a| < \frac{k}{2}$ and $|b| < \frac{k}{2}$ and $a \equiv b \pmod k$, then $a = b$.

Proof. Suppose $|a| < \frac{k}{2}$ and $|b| < \frac{k}{2}$ and $a \equiv b \pmod k$.
Since $a \equiv b \pmod k$, then $k|a-b$, so $a - b = km$ for some integer m.
Observe that $0 \le |a-b| < \frac{k}{2}$.
Since $a - b = km$, then $|a-b| = |km| = k|m|$, so $\frac{|a-b|}{k} = |m|$.
Dividing by positive k, we obtain $0 \le \frac{|a-b|}{k} < \frac{1}{2}$.
Thus, $0 \le |m| < \frac{1}{2}$.
Since m is an integer, then this implies $|m| = 0$, so $m = 0$.
Therefore, $a - b = k(0) = 0$, so $a = b$. $\square$

Exercise 61. Let $S_2 = \{n \in \mathbb{Z} : n^2 \equiv -1 \pmod 2\}$.
Then $S_2 = [1]_2$.

Proof. Observe that $S_2 = \{n \in \mathbb{Z} : 2|n^2 + 1\}$ and $[1]_2 = \{n \in \mathbb{Z} : n \equiv 1 \pmod 2\} = \{n \in \mathbb{Z} : 2|n - 1\}$.

Let $a \in S_2$.
Then $a \in \mathbb{Z}$ and $2|a^2 + 1$.
Thus, $a^2 + 1 = 2k$ for some integer k.
Hence, $a^2 = 2k - 1 = 2(k - 1) + 1$, so a^2 is odd.
Since the integer a^2 is odd if and only if a is odd, then a is odd.
Thus, $a - 1$ is even, so $2|a - 1$.
Therefore, $a \in [1]_2$, so $S_2 \subset [1]_2$.
Let $b \in [1]_2$.
Then $b \in \mathbb{Z}$ and $2|(b - 1)$.
Thus, $b - 1 = 2m$ for some integer m.
Hence, $b^2 + 1 = (2m + 1)^2 + 1 = 2(2m^2 + 2m + 1)$.
Since $2m^2 + 2m + 1$ is an integer, then $2|(b^2 + 1)$.
Thus, $b \in S_2$, so $[1]_2 \subset S_2$.
Since $S_2 \subset [1]_2$ and $[1]_2 \subset S_2$, then $S_2 = [1]_2$, as desired. □

Exercise 62. Prove $[1]$ and $[n - 1]$ are units of $\mathbb{Z}_n$.

Solution. To prove $[1]$ is a unit of $\mathbb{Z}_n$ and $[n - 1]$ is a unit of $\mathbb{Z}_n$, we can use a variety of methods.

We know that $[1]$ is a unit of $\mathbb{Z}_n$ iff $\gcd(1, n) = 1$ and $[n - 1]$ is a unit of $\mathbb{Z}_n$ iff $\gcd(n - 1, n) = 1$.

Let $n \in \mathbb{Z}^+$.

To prove $[1]$ is a unit of $\mathbb{Z}_n$, we must show that $[1] \in \mathbb{Z}_n$ and $\gcd(1, n) = 1$.

To prove $[n - 1]$ is a unit of $\mathbb{Z}_n$, we must show that $[n - 1] \in \mathbb{Z}_n$ and $\gcd(1, n) = 1$.

We know that $(1 - n) * 1 + 1 * n = 1$, so 1 is a linear combination of 1 and n.

Hence, $\gcd(1, n) = 1$.

We know that $(-1)(n - 1) + 1 * n = 1$, so 1 is a linear combination of $n - 1$ and n.

Hence, $\gcd(n - 1, n) = 1$. □

Proof. Let $n \in \mathbb{Z}^+$.
Observe that $[1] \in \mathbb{Z}_n$ and $[1][1] = [1 * 1] = [1]$.
Hence, there exists $[1] \in \mathbb{Z}_n$ such that $[1][1] = [1]$.
Therefore, $[1]$ is a unit of $\mathbb{Z}_n$ and $[1]^{-1} = [1]$.
Since $n|n$, then $n|(n - 1 + 1)$, so $n|(n - 1) - (-1)$.
Hence, $n - 1 \equiv -1 \pmod n$, so $[n - 1] = [-1]$.
Observe that $[n - 1] \in \mathbb{Z}_n$ and $[n - 1][n - 1] = [-1][-1] = [-1 * -1] = [1]$.
Hence, there exists $[n - 1] \in \mathbb{Z}_n$ such that $[n - 1][n - 1] = [1]$.
Therefore, $[n - 1]$ is a unit of $\mathbb{Z}_n$ and $[n - 1]^{-1} = [n - 1]$. □

Exercise 63. Define $f : \mathbb{Z}_{12} \to \mathbb{Z}_8$ by $f([x]_{12}) = [2x]_8$ for all $[x]_{12} \in \mathbb{Z}_{12}$.
Define $g : \mathbb{Z}_{12} \to \mathbb{Z}_8$ by $g([x]_{12}) = [3x]_8$ for all $[x]_{12} \in \mathbb{Z}_{12}$.
Show that f is a function, but g is not a function.

Solution. Let $f : A \to B$ be a binary relation from A to B.

To prove $f : A \to B$ is a function, we must show that f is well defined.

Thus, we must prove if $a_1 = a_2$, then $f(a_1) = f(a_2)$ for all $a_1, a_2 \in A$.

To prove f is a function, we must prove if $[x]_{12} = [y]_{12}$, then $f([x]_{12}) = f([y]_{12})$ for all $[x]_{12}, [y]_{12} \in \mathbb{Z}_{12}$.

Thus, we must prove if $[x]_{12} = [y]_{12}$, then $[2x]_8 = [2y]_8$ for all $[x]_{12}, [y]_{12} \in \mathbb{Z}_{12}$.

To prove g is not a function, we need only show an example $[x]_{12}, [y]_{12} \in \mathbb{Z}_{12}$ such that $g([x]) \neq g([y])$. ☐

Proof. Let $[x], [y] \in \mathbb{Z}_{12}$ such that $[x] = [y]$.

Then $x \equiv y \pmod{12}$, so $12|(x - y)$.

Thus, $4 * 3|(x - y)$, so $4|(x - y)$.

Hence, $2 * 4|2(x - y)$, so $8|2x - 2y$.

Thus, $2x \equiv 2y \pmod{8}$, so $[2x] = [2y]$.

Therefore, $f([x]) = f([y])$.

Since $[x] = [y]$ implies $f([x]) = f([y])$, then f is well defined, so f is a function. ☐

Exercise 64. Let a be a fixed element of $\mathbb{Z}_{17}^*$.

Let $f : \mathbb{Z}_{17}^* \to \mathbb{Z}_{17}^*$ be defined by $f([x]) = [a][x]$ for all $x \in \mathbb{Z}_{17}^*$.

Determine if the inverse function exists.

Solution. We know that $\mathbb{Z}_{17}^* = \{[m] \in \mathbb{Z}17 : \gcd(m, 17) = 1\} = \{[1], [2], [3], ..., [16]\}$ and $|\mathbb{Z}_{17}^*| = \phi(17) = 16$.

Since $(\mathbb{Z}_n^*, *)$ is an abelian group, then $(\mathbb{Z}_{17}^*, *)$ is an abelian group.

Let $[x] \in \mathbb{Z}_{17}^*$.

Then $f([x]) = [a][x]$.

Since $(\mathbb{Z}_{17}^*, *)$ is a group, then $\mathbb{Z}_{17}^*$ is closed under multiplication modulo 17.

Thus, $[a][x] \in \mathbb{Z}_{17}^*$, so $f([x]) \in \mathbb{Z}_{17}^*$.

Hence, f is a binary relation from $\mathbb{Z}_{17}^*$ to $\mathbb{Z}_{17}^*$.

Is f a function(ie, well defined)?

Suppose $[x], [y] \in \mathbb{Z}_{17}^*$ such that $[x] = [y]$.

Then $f([x]) = [a][x] = [a][y] = f([y])$, so $f([x]) = f([y])$.

Thus, $[x] = [y]$ implies $f([x]) = f([y])$, so f is well defined.

Therefore, f is a function.

Is f injective?

Let $[x], [y] \in \mathbb{Z}_{17}^*$ such that $f[x] = f[y]$.

Then $[a][x] = [a][y]$, so $[ax] = [ay]$.

Thus, $ax \equiv ay \pmod{17}$.

Since $[a] \in \mathbb{Z}_{17}^*$, then $[a] \in \mathbb{Z}_{17}$ and $\gcd(a, 17) = 1$.

Since $\gcd(a, 17) = 1$, we may cancel to obtain $x \equiv y \pmod{17}$.

Thus, $[x] = [y] \pmod{17}$.

Hence, $f[x] = f[y]$ implies $[x] = [y]$, so f is injective.

Is f surjective?

Let $[z] \in \mathbb{Z}_{17}^*$.

Since $(\mathbb{Z}_{17}^*, *)$ is a group and $[a] \in \mathbb{Z}_{17}^*$, then $[a]^{-1} \in \mathbb{Z}_{17}^*$.

Let $[x] = [a]^{-1}[z]$.

Since $(\mathbb{Z}_{17}^*, *)$ is closed under multiplication modulo n, then $[a]^{-1}[z] \in \mathbb{Z}_{17}^*$, so $[x] \in \mathbb{Z}_{17}^*$.

Observe that $f[x] = [a][x] = [a]([a]^{-1}[z]) = ([a][a]^{-1})[z] = [1][z] = [z]$.

Hence, there exists $[x] \in \mathbb{Z}_{17}^*$ such that $f[x] = [z]$, so f is surjective.

Since f is injective and surjective, then f is bijective, so the inverse function exists.

Let $f^{-1} : \mathbb{Z}_{17}^* \mapsto \mathbb{Z}_{17}^*$ be the inverse function of f.

Then f^{-1} satisfies $f \circ f^{-1} = I = f^{-1} \circ f$, where I is the identity function.

Let $[x] \in \mathbb{Z}_{17}^*$.

Then $(f \circ f^{-1})[x] = [x]$, so $f(f^{-1}[x]) = [x]$.

Let $[y] = f^{-1}[x]$.

Then $f([y]) = [x]$, so $[a][y] = [x]$.

We multiply by $[a]^{-1}$ to obtain $[y] = [a]^{-1}[x]$.

Thus, we let the inverse function f^{-1} be defined by $f^{-1}[x] = [a]^{-1}[x]$.

We verify this is correct by confirming $f^{-1} \circ f = I$.

This means we must show $(f^{-1} \circ f)([x]) = [x]$ for all $[x] \in \mathbb{Z}_{17}^*$.

Let $[x] \in \mathbb{Z}_{17}^*$.

Then $(f^{-1} \circ f)([x]) = f^{-1}(f[x]) = f^{-1}([a][x]) = [a]^{-1}([a][x]) = ([a]^{-1}[a])[x] = [1][x] = [x]$. $\square$

Exercise 65. Let $m, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.

Let $f : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ be defined by $f([x]) = [mx + b]$.

Show that f is bijective iff $\gcd(m, n) = 1$ and find the inverse if $\gcd(m, n) = 1$.

Solution. Observe that f is a binary relation on $\mathbb{Z}_n$.

Let's first prove f is a function(ie, well defined).

Let $[x] \in \mathbb{Z}_n$.

Then $f([x]) = [mx + b]$.

Since $mx + b \in \mathbb{Z}$, then $[mx + b] \in \mathbb{Z}_n$, so $f([x]) \in \mathbb{Z}_n$.

Suppose $[x], [y] \in \mathbb{Z}_n$ such that $[x] = [y]$.

Then $x \equiv y \pmod{n}$.

We multiply by m to obtain $mx \equiv my \pmod{n}$.

We add b to obtain $mx + b \equiv my + b \pmod{n}$.

Thus, $[mx + b] = [my + b]$, so $f([x]) = f([y])$.

Hence, $[x] = [y]$ implies $f([x]) = f([y])$, so f is well defined.

Therefore, f is a function.

Suppose f is bijective.

Then f is injective and surjective.

Since f is surjective, then for every $[z] \in \mathbb{Z}_n$ there exists $[x] \in \mathbb{Z}_n$ such that $f([x]) = [z] = [mx + b]$.

Thus, for every $z \in \mathbb{Z}$ there exists $x \in \mathbb{Z}$ such that $mx + b \equiv z \pmod{n}$.
Let $z = b + 1$.
Then $z \in \mathbb{Z}$ and there exists $x \in \mathbb{Z}$ such that $mx + b \equiv b + 1 \pmod{n}$.
Hence, there exists $x \in \mathbb{Z}$ such that $mx \equiv 1 \pmod{n}$.
Thus, m has an inverse modulo n.
Since m has an inverse modulo n iff $\gcd(m, n) = 1$, then $\gcd(m, n) = 1$.
Therefore, if f is bijective, then $\gcd(m, n) = 1$.

Conversely, suppose $\gcd(m, n) = 1$.
Let $[x] \in \mathbb{Z}_n$.
Since $\gcd(m, n) = 1$, then there exists $m' \in \mathbb{Z}$ such that $mm' \equiv 1 \pmod{n}$.
Hence, m has an inverse modulo n, so $[m]^{-1} \in \mathbb{Z}_n$ and $[m][m]^{-1} = [1]$.
Let $[y] = [m]^{-1}[x - b]$.
Since multiplication modulo n is a binary operation on $\mathbb{Z}_n$, then $\mathbb{Z}_n$ is closed under multiplication modulo n.
Thus, $[m]^{-1}[x - b] \in \mathbb{Z}_n$, so $[y] \in \mathbb{Z}_n$.
Observe that $f([y]) = [my+b] = [my]+[b] = [m][y]+[b] = [m]([m]^{-1}[x-b])+[b] = ([m][m]^{-1})[x-b]+[b] = [1][x-b]+[b] = [x-b]+[b] = [x-b+b] = [x+0] = [x]$.
Hence, there exists $[y] \in \mathbb{Z}_n$ such that $f([y]) = [x]$, so f is surjective.

Let $[x], [y] \in \mathbb{Z}$ such that $f([x]) = f([y])$.
Then $[mx + b] = [my + b]$, so $mx + b \equiv my + b \pmod{n}$.
Thus, $mx \equiv my \pmod{n}$.
Since $\gcd(m, n) = 1$, then we may cancel to obtain $x \equiv y \pmod{n}$.
Hence, $[x] = [y]$.
Since $f([x]) = f([y])$ implies $[x] = [y]$, then f is injective.
Since f is injective and surjective, then f is bijective.
Hence, $\gcd(m, n) = 1$ implies f is bijective.

Suppose $\gcd(m, n) = 1$.
Then f is bijective.
Since f is bijective iff the inverse function f^{-1} exists, then f^{-1} exists.
Let $f^{-1} : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ be the inverse of f.
Then $f \circ f^{-1} = I$, where I is the identity function.
Thus, for every $[x] \in \mathbb{Z}_n$, $(f \circ f^{-1})[x] = [x]$.
Let $[x] \in \mathbb{Z}_n$.
Then $(f \circ f^{-1})[x] = [x]$, so $f(f^{-1})[x] = [x]$.
Let $[y] = f^{-1}[x]$.
Then $[x] = f([y]) = [my + b]$, so $[x] = [my] + [b]$.
Thus, $[x] - [b] = [my]$, so $[x - b] = [m][y]$.
Since $\gcd(m, n) = 1$, then the inverse of m exists modulo n.
Hence, $[m]^{-1} \in \mathbb{Z}_n$ and $[m]^{-1}[m] = [1]$.
We multiply by the inverse to obtain $[m]^{-1}[x - b] = [y]$.
Thus, $f^{-1}[x] = [m]^{-1}[x - b]$.
We verify that this is the correct inverse function by showing that $f^{-1} \circ f = I$.

Let $[x] \in \mathbb{Z}_n$.

Then $(f^{-1} \circ f)[x] = f^{-1}(f[x]) = f^{-1}([mx + b]) = [m]^{-1}[(mx + b) - b] = [m]^{-1}[mx] = [m]^{-1}[m][x] = [1][x] = [x]$. ☐

Exercise 66. Suppose $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod 6$ if and only if $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.

Proof. First we prove that if $a \equiv b \pmod 6$, then $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.

Suppose $a \equiv b \pmod 6$. This means $6|(a - b)$, so there is an integer n for which $a - b = 6n$.

From this equation we get $a - b = 2(3n)$, which implies $2|(a - b)$, so $a \equiv b \pmod 2$.

We also get $a - b = 3(2n)$, which implies $3|(a - b)$, so $a \equiv b \pmod 3$.

Therefore $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.

Conversely, we show that if $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$, then $a \equiv b \pmod 6$.

Suppose $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$.

Since $a \equiv b \pmod 2$ then $2|(a-b)$, so there is an integer k for which $a-b = 2k$.

Therefore $a - b$ is even.

Since $a \equiv b \pmod 3$ then $3|(a-b)$, so there is an integer l for which $a-b = 3l = 2k$.

Since $a-b$ is even, then $3l$ is even. Since $3l$ is even and 3 is odd, then l must be even, for if l were odd then $3l = a - b$ would be odd.

Hence $l = 2m$ for some integer m.

Thus $a - b = 3(2m) = 6m$.

This means $6|(a - b)$, so $a \equiv b \pmod 6$. ☐

Exercise 67. If $a \in \mathbb{Z}$, then $a^3 \equiv a \pmod 3$.

Proof. Suppose $a \in \mathbb{Z}$.

Then $a^3 - a = a(a^2 - 1) = a(a - 1)(a + 1) = (a - 1)a(a + 1)$.

This means $a^3 - a$ is the product of three consecutive integers.

Without loss of generality we shall assume a is nonnegative. A similar argument holds if a is negative.

We consider the integer a when it is divided by 3.

Suppose $a \geq 0$.

Then we know the remainder when a is divided by 3 is either 0,1, or 2.

Thus by the division algorithm $a = 3q + r$ for some integers q and r and $r = 0$ or $r = 1$ or $r = 2$.

We consider these cases separately.

Case 1: Suppose $r = 0$.

This means 3 evenly divides a, so $3|a$.

This implies $a = 3q$ for some $q \in \mathbb{Z}$.

Substituting we get

$(a-1)a(a+1) = (3q-1)(3q)(3q+1) = 3q(3q-1)(3q+1)$, so $3|(a-1)a(a+1)$.
Therefore $3|a^3 - a$.
Case 2: Suppose $r = 1$.
This means 1 is the remainder when a is divided by 3, so $a = 3q+1$ for some $q \in \mathbb{Z}$.
Substituting we get
$(a-1)a(a+1) = (3q)(3q+1)(3q+2) = 3q(3q+1)(3q+2)$, so $3|(a-1)a(a+1)$.
Therefore $3|a^3 - a$.
Case 3: Suppose $r = 2$.
This means 2 is the remainder when a is divided by 3, so $a = 3q+2$ for some $q \in \mathbb{Z}$.
Substituting we get
$(a-1)a(a+1) = (3q+1)(3q+2)(3q+3) = (3q+1)(3q+2)(3(q+1)) = 3(q+1)(3q+1)(3q+2)$, so $3|(a-1)a(a+1)$.
Therefore $3|a^3 - a$.

In each of these cases we always get $3|a^3 - a$.
Consequently $a^3 \equiv a \pmod 3$. □

Exercise 68. Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.
If $12a \not\equiv 12b \pmod n$, then $n \nmid 12$.

Solution. Direct proof doesn't seem to work. So we'll try proof by contrapositive since we can get rid of the negatives. □

Proof. Suppose $n|12$.
Then there is an integer k for which $12 = nk$.
Multiply the equation by $a - b$ to get

$$\begin{aligned} 12(a-b) &= nk(a-b) \\ 12a - 12b &= n(ka - kb) \end{aligned}$$

Since $ka - kb \in \mathbb{Z}$, the equation $12a - 12b = n(ka - kb)$ implies that $n|(12a - 12b)$.
This in turn means that $12a \equiv 12b \pmod n$. □

Exercise 69. If $n \in \mathbb{N}$, then $12|(n^4 - n^2)$.

Solution. Note that the statement is equivalent to $n^4 \equiv n^2 \pmod{12}$.
The equivalent universal quantified statement is $\forall n \in \mathbb{N}, 12|(n^4 - n^2)$.
We prove by induction.
Note that $n^4 - n^2 = n^2(n^2 - 1) = n^2(n-1)(n+1)$.
The statement S_n is $12|n^2(n-1)(n+1)$.
The statement S_k is $12|k^2(k-1)(k+1)$.
The statement S_{k+1} is $12|(k+1)^2(k)(k+2)$.
We try weak induction.
Basis:

If $n = 1$ then the statement S_1 is $12|1^2(1-1)(1+1)$. This simplifies to $12|0$, which is true because $0 = 12 * 0$.

Induction:

We must prove $S_k \to S_{k+1}$ for $k \geq 1$.

This means we must prove $12|k^2(k-1)(k+1)$ implies $12|(k+1)^2(k)(k+2)$ for any integer $k \geq 1$.

We use direct proof.

Suppose $12|k^2(k-1)(k+1)$ for any integer $k \geq 1$.

Then $k^2(k-1)(k+1) = 12a$ for $a \in \mathbb{Z}$, by definition of divisibility.

Our goal is to prove $12|(k+1)^2(k)(k+2)$, so this implies we must prove $(k+1)^2(k)(k+2) = 12b, b \in \mathbb{Z}$.

If we subtract we get

$$\begin{aligned}
(k+1)^2(k)(k+2) - k^2(k-1)(k+1) &= k(k+1)[(k+1)(k+2) - k(k-1)] \\
&= k(k+1)(k^2 + 3k + 2 - k^2 + k) \\
&= k(k+1)(4k+2) \\
&= 2k(k+1)(2k+1)
\end{aligned}$$

This implies we must prove $12|2k(k+1)(2k+1)$ in order to prove our main goal.

This implies $2k(k+1)(2k+1) = 12c, c \in \mathbb{Z}$ which implies $k(k+1)(2k+1) = 6c$.

Of course, we've already proved that $6|n(n+1)(2n+1)$, so we know this is true.

However, we will use strong induction instead.

Since $k(k+1)(2k+1)$ must be divisible by 6 for $k \geq 1$, then we can show that it is sufficient to show that $k(k+1)(2k+1)$ is divisible by 6 for the first 6 natural numbers in order to use strong induction. We can do this because the Division Algorithm says that for any integer n divided by 6, $n = 6q + r, 0 \leq r < 6$.

Thus we have a partition of $\mathbb{N}$ under the equivalence relation $a \equiv b \pmod 6$:

If $r = 0$,then $n = 6q$ which implies $n \in \{6q\} = [0]_6$.

If $r = 1$,then $n = 6q + 1$ which implies $n \in \{6q + 1\} = [1]_6$.

If $r = 2$,then $n = 6q + 2$ which implies $n \in \{6q + 2\} = [2]_6$.

If $r = 3$,then $n = 6q + 3$ which implies $n \in \{6q + 3\} = [3]_6$.

If $r = 4$,then $n = 6q + 4$ which implies $n \in \{6q + 4\} = [4]_6$.

If $r = 5$,then $n = 6q + 5$ which implies $n \in \{6q + 5\} = [5]_6$.

Each of these congruence classes(equivalence classes) are disjoint sets and $\mathbb{N} = \cup_{i=0}^{5} [i]_6$.

Thus we only have to choose the first 6 natural numbers since any integer greater than 6 will be congruent modulo 6 to one of the first 6 natural numbers.

Thus for strong induction we simply prove $S_1 \wedge S_2 \wedge ... \wedge S_6 \wedge S_k \to S_{k+1}, k \geq 6$.

Thus for the basis step we must prove $S_1 \wedge S_2 \wedge ... \wedge S_6$.

For the induction step we must prove $S_1 \wedge S_2 \wedge ... \wedge S_6 \wedge S_k \rightarrow S_{k+1}, k \geq 6$.

This implies we must prove $S_{k-5} \wedge S_{k-4} \wedge ... \wedge S_k \rightarrow S_{k+1}$ for $k \geq 6$. □

Proof. We prove by induction(strong).

Basis:

If $n = 1$ then the statement is $12|(1^4 - 1^2)$. This simplifies to $12|0$, which is true.

If $n = 2$ then the statement is $12|(2^4 - 2^2)$. This simplifies to $12|12$, which is true.

If $n = 3$ then the statement is $12|(3^4 - 3^2)$. This simplifies to $12|72$, which is true.

If $n = 4$ then the statement is $12|(4^4 - 4^2)$. This simplifies to $12|240$, which is true.

If $n = 5$ then the statement is $12|(5^4 - 5^2)$. This simplifies to $12|600$, which is true.

If $n = 6$ then the statement is $12|(6^4 - 6^2)$. This simplifies to $12|1260$, which is true.

Induction: We must prove $S_1 \wedge S_2 \wedge ... \wedge S_6 \wedge S_k \rightarrow S_{k+1}, k \geq 6$.

This implies we must prove $S_{k-5} \wedge S_{k-4} \wedge ... \wedge S_k \rightarrow S_{k+1}$ for $k \geq 6$.

For simplicity, let $m = k - 5$.

Then $S_{k-5} \wedge S_{k-4} \wedge ... \wedge S_k \rightarrow S_{k+1}$ for $k \geq 6$ becomes $S_m \wedge S_{m+1} \wedge ... \wedge S_{m+5} \rightarrow S_{m+6}$ for $m \geq 1$.

We prove the latter statement using direct proof.

Suppose $S_m \wedge S_{m+1} \wedge ... \wedge S_{m+5}$ for $m \geq 1$.

We must prove that these assumptions together imply S_{m+6}.

Since $S_m \wedge S_{m+1} \wedge ... \wedge S_{m+5}$ is true by assumption, then S_m is true.

This implies $12|m^4 - m^2$.

Thus $m^4 - m^2 = 12a, a \in \mathbb{Z}$ by definition of divisibility.

Observe the following equalities:

$$\begin{aligned}
(m+6)^4 - (m+6)^2 &= (m^4 + 24m^3 + 216m^2 + 864m + 1296) - (m^2 + 12m + 36) \\
&= m^4 + 24m^3 + 215m^2 + 852m + 1260 \\
&= (m^4 - m^2) + (24m^3 + 216m^2 + 852m + 1260) \\
&= 12a + (24m^3 + 216m^2 + 852m + 1260) \\
&= 12(a + 2m^3 + 18m^2 + 71m + 105)
\end{aligned}$$

Since $a + 2m^3 + 18m^2 + 71m + 105 \in \mathbb{Z}$, then by definition of divisibility $12|(m+6)^4 - (m+6)^2$.

Thus S_{m+6} is true.

Hence $S_m \wedge S_{m+1} \wedge ... \wedge S_{m+5} \rightarrow S_{m+6}$ for $m \geq 1$.

Thus, $S_{k-5} \wedge S_{k-4} \wedge ... \wedge S_k \rightarrow S_{k+1}$ for $k \geq 6$.

It follows by strong induction that $12|(n^4 - n^2)$ for all natural numbers n. □

Proposition 70. *Each set of seven distinct natural numbers contains a pair of numbers whose sum or difference is divisible by 10.*

Solution. We first translate the English statement into logical symbols in order to better understand what the statement means.

The statement in logical symbols is something like: $\forall S, P$ where S is a set of 7 distinct natural numbers and P is $\exists a_i, a_j \in S, 10|a_i + a_j \vee 10|a_i - a_j$.

We can represent a set S of 7 distinct natural numbers as follows.

Let $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$.

Then $|S| = 7$.

How many pairs of distinct elements exist?

To answer this question, we realize this is really asking how many combinations are there which is the same as asking how many sets of size 2 from a set of size 7 are there?

This is simply 7 choose 2 = 21 since this is a selection without repetition(ie, combination).

Now to better understand this proposition we should try some concrete examples.

If we have a set of 7 distinct natural numbers, then we would need to compute the sum and differences of each of the 21 pairs, and then determine whether any of the results is divisible by 10. We can write a Java program or use some other math software (like GAP) to investigate whether this proposition appears to be true.

We do try some examples and the examples do suggest the conjecture is true.

Let's analyze statement P.

Statement P is telling us that there exist distinct $a_i, a_j \in S$, such that some statement is true concerning the sum or difference: $\exists a_i, a_j \in S, P(a_i + a_j, a_i - a_j)$.

Let's translate this logical statement into math symbols. We should think about the sums and differences of any distinct $a_i, a_j \in S$. We consider a set of sums and differences of distinct $a_i, a_j \in S$. Let T be a set of distinct sums and differences of distinct pairs $a_i, a_j \in S$. We observe that there could be some pairs whose sum may be the same. For example, if $2, 3, 4, 5 \in S$, then $2 + 5 = 3 + 4$. Since we want to guarantee that any sum(or difference) of distinct pairs is distinct, then we must devise set T in such a way that this holds true. Otherwise, T would have duplicate sums(or differences) and would therefore not be a true set!

What facts do we know that can help us to devise set T?

We know $S \subseteq N$ and S is not empty, so by the Well Ordering Principle, we know S has a smallest element, say a_1.

With some insight we realize that a way to devise set T would be to consider the set of sums and differences of the smallest element of S.

Let $T = \{a_1 - a_2, a_1 - a_3, a_1 - a_4, a_1 - a_5, a_1 - a_6, a_1 - a_7, a_1 + a_2, a_1 + a_3, a_1 + a_4, a_1 + a_5, a_1 + a_6, a_1 + a_7\}$.

We observe that each element of set T is distinct from any other element in T, so T is truly a set.

Consider the statement $10|n$.

This means some natural number $n \in \{10, 20, 30, 40, 50, ...\} = A$.

Observe that set A consists of numbers that end with the digit zero.

Thus, $\exists a_i, a_j \in S, P(a_i + a_j, a_i - a_j)$ is the same as $\exists a_i, a_j \in S, 10|a_i + a_j \vee 10|a_i - a_j$ and can be interpreted to mean $\exists a_i, a_j \in S, a_i + a_j$ ends with a zero or $a_i - a_j$ ends with a zero.

How do we prove the existence of a number that has this property of ending with the digit zero?

Since we can't devise a concrete example, we must try another approach to devise that such an element must exist.

We consider the property of a number ending with a specific digit.

Since every number ends with one of the digits 0 to 9, then there is a natural mapping from each number n to the digit that it ends with.

Thus, let us define a function $f : T \mapsto D$ where $f(n) =$ the digit that a number n ends with and D is the set of digits 0 to 9.

For example, $f(803) = 3$ since the number 803 ends with the digit 3.

What properties or relationships can we deduce about function f?

Well, we know that $|T| = 12$ and $|D| = 10$. By the Pigeonhole principle, this implies f is not injective.

Thus, there exist distinct $x, y \in T$ for which $f(x) = f(y)$.

This means there exist distinct $x, y \in T$ which end with the same digit.

In other words, there exist distinct $a_1 \pm a_i, a_1 \pm a_j \in T$ for which $f(a_1 \pm a_i) = f(a_1 \pm a_j)$ where $a_i, a_j \in S$.

So we have deduced that there exist distinct $a_1 \pm a_i, a_1 \pm a_j \in T$ and $a_1 \pm a_i$ has the same last digit as $a_1 \pm a_j$.

We know that the difference between any two numbers that end in the same digit is a number that ends with the digit zero.

Thus, we take the difference between $a_1 \pm a_i, a_1 \pm a_j \in T$ to get $(a_1 \pm a_i) - (a_1 \pm a_j) = \pm a_i \mp a_j = \pm a_i \pm a_j$.

This implies $a_i + a_j$ or $a_i - a_j$ ends with the digit zero.

Hence $a_i + a_j$ or $a_i - a_j$ is divisible by 10. $\square$

Proof. Let $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ be a set of seven distinct natural numbers.

We must prove $\exists a_i, a_j \in S, 10|a_i + a_j \vee 10|a_i - a_j$

Since $S \subseteq N$ and S is not empty, then it follows by the Well Ordering Principle that S has a smallest element.

Without loss of generality, let a_1 be the smallest element of S.

Let $T = \{a_1 - a_2, a_1 - a_3, a_1 - a_4, a_1 - a_5, a_1 - a_6, a_1 - a_7, a_1 + a_2, a_1 + a_3, a_1 + a_4, a_1 + a_5, a_1 + a_6, a_1 + a_7\}$ be a set of sums and differences of a_1. It is obvious that T is a set since each sum or difference in T is different from any other sum or difference in T.

Let $f : T \mapsto D$ be a function where $f(n) =$ the digit that a number n ends with and D is the set of digits 0 to 9.

Observe that $|T| = 12$ and $|D| = 10$.

Since $|T| > |D|$, then by the pigeonhole principle, f is not injective.

Thus, there exist distinct $x, y \in T$ for which $f(x) = f(y)$.

This means there exist distinct $x, y \in T$ which end with the same digit.

Thus, there exist distinct $a_1 \pm a_i, a_1 \pm a_j \in T$ and $a_1 \pm a_i$ has the same last digit as $a_1 \pm a_j$ where $a_i, a_j \in S$.

We know that the difference between any two numbers that end in the same digit is a number that ends with the digit zero.

Thus, we take the difference between $a_1 \pm a_i, a_1 \pm a_j \in T$ to get $(a_1 \pm a_i) - (a_1 \pm a_j) = \pm a_i \mp a_j = \pm a_i \pm a_j$.

This implies $a_i + a_j$ or $a_i - a_j$ ends with the digit zero.

Since any number is divisible by 10 if and only if it ends with the digit zero, then this implies $a_i + a_j$ or $a_i - a_j$ is divisible by 10. $\square$

Exercise 71. Prove that for every $n \in \mathbb{Z}^+$

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Exercise 72. Euler conjecture is false

The equation $a^4 + b^4 + c^4 = d^4$ has no solution when a, b, c, d are positive integers.

Show that this statement is false

Proof. Let $a = 95800$ and $b = 217519$ and $c = 414560$ and $d = 422481$.

Then $a^4 + b^4 + c^4 = 31858749840007945920321 = d^4$.

Therefore, the conjecture is false. $\square$