Modular arithmetic

Question: What time will it be in 1 hour from now? In 2? In 10? In 20?

Modular arithmetic

Question: What time will it be in 1 hour from now? In 2? In 10? In 20?

Question: What time will it be in 5 hours? In 5 hours after that? In 5 hours after that? In 5 hours after that? In 5 hours after that?

Modular arithmetic

Question: What time will it be in 1 hour from now? In 2? In 10? In 20?

Question: What time will it be in 5 hours? In 5 hours after that? In 5 hours after that? In 5 hours after that? In 5 hours after that?

Question: If I run a computer program 30 times (in sequence) that takes 5 hours to run each time, when will it be done?

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\} (a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\}(a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, '$\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '$=$' instead of '$\equiv$'!*

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\}(a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, '$\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '=' instead of '≡'!*

Examples:

$14 \equiv 2 \pmod{12}$

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \dots, |n| - 1\}(a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, '$\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '=' instead of '$\equiv$'!*

Examples:

$$14 \equiv 2 \pmod{12}, \quad 26 \equiv 2 \pmod{12}$$

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\}(a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, '$\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '=' instead of '$\equiv$'!*

Examples:

$$14 \equiv 2 \pmod{12}, \quad 26 \equiv 2 \pmod{12}, \quad 14 \equiv 26 \pmod{12}$$

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\}(a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, '$\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '=' instead of '$\equiv$'!*

Examples:

$$14 \equiv 2 \pmod{12}, \quad 26 \equiv 2 \pmod{12}, \quad 14 \equiv 26 \pmod{12},$$
$$-10 \equiv 26 \pmod{12}$$

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = nq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\}(a = bq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, '$\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '=' instead of '$\equiv$'!*

Examples:

$$14 \equiv 2 \pmod{12}, \quad 26 \equiv 2 \pmod{12}, \quad 14 \equiv 26 \pmod{12},$$

$$-10 \equiv 26 \pmod{12}, \qquad -2 \not\equiv 2 \pmod{12}.$$

Modular arithmetic

Recall the division algorithm: For $a, n \in \mathbb{Z}$ with $n \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < |n|$ satisfying $a = bq + r$.

In logic:

$$\forall a \in \mathbb{Z}, n \in \mathbb{Z}_{\neq 0}, \exists! q \in \mathbb{Z}, r \in \{0, 1, \ldots, |n| - 1\}(a = nq + r).$$

($\exists!$ means "there exist(s) unique"—not only do they exist, but they're the only ones.)

We say q is the quotient and r is the remainder of n divided into a, also called the least residue of a modulo n.

If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

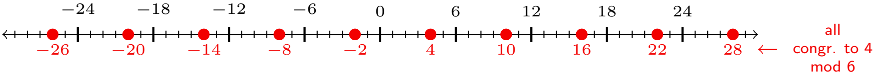
written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

LaTeX: '$\equiv$' is \equiv, ' $\pmod{b}$' is \pmod{b}

Warning: Even though the book does this, **DO NOT** *use '=' instead of '$\equiv$'!*

Example: The numbers that are equivalent to 4 modulo 6 are



If a and b have the same remainder when divided by n, we say

a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

Lemma. For $a, b, n \in \mathbb{Z}$ with $n \neq 0$, we have $a \equiv b \pmod{n}$ if and only if $n | a - b$.

If a and b have the same remainder when divided by n, we say

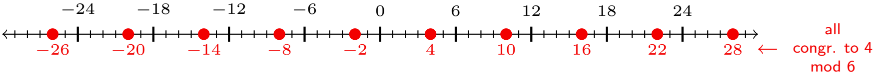
a is congruent to b modulo (mod) n

written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b.$$

Lemma. For $a, b, n \in \mathbb{Z}$ with $n \neq 0$, we have $a \equiv b \pmod{n}$ if and only if $n | a - b$.

Example: The numbers that are equivalent to 4 modulo 6 are



Lemma. For $a, b, n \in \mathbb{Z}$ with $n \neq 0$, we have $a \equiv b \pmod{n}$ if and only if $n | a - b$.

Proof. Fix $a, b \in \mathbb{Z}$. By the division algorithm, there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leqslant r_1, r_2 < |n|$ satisfying

$$a = q_1 n + r_1 \quad \text{and} \quad b = q_2 n + r_2.$$

If $a \equiv_n b$, then $r_1 = r_2$, so that

$$a - b = q_1 n + r_1 - (q_2 n + r_2) = (q_1 - q_2)n.$$

Since $q_1 - q_2 \in \mathbb{Z}$, we have $n | a - b$, as desired.

Conversely, if $n | a - b$, then $a - b = kn$ for some $k \in \mathbb{Z}$. Thus,

$$kn = a - b = q_1 n + r_1 - (q_2 n + r_2) = (q_1 - q_2)n + (r_1 - r_2).$$

Therefore,

$$r_1 - r_2 = (k - q_1 + q_2)n, \quad \text{so that} \quad n | r_1 - r_2.$$

But since $0 \leqslant r_1, r_2 < |n|$, we have $-|n| < r_1 - r_2 < |n|$.
Therefore, $r_1 - r_2 = 0$, so that $a \equiv b \pmod{n}$, as desired. □

For the rest of today, fix $n \in \mathbb{Z}_{\geqslant 1}$, and assume all other variables are integers.

Proposition. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

For the rest of today, fix $n \in \mathbb{Z}_{\geqslant 1}$, and assume all other variables are integers.

Proposition. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Proof outline. Recall that

$$a \equiv_n b \quad \Leftrightarrow \quad n | a - b \quad \Leftrightarrow \quad a - b = kn$$

for some $k \in \mathbb{Z}$.

For the rest of today, fix $n \in \mathbb{Z}_{\geqslant 1}$, and assume all other variables are integers.

Proposition. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Proof outline. Recall that

$$a \equiv_n b \quad \Leftrightarrow \quad n | a - b \quad \Leftrightarrow \quad a - b = kn$$

for some $k \in \mathbb{Z}$. So since $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, we have

$$a_1 - b_1 = k_1 n \quad \text{and} \quad a_2 - b_2 = k_2 n$$

for some $k_1, k_2 \in \mathbb{Z}$.

For the rest of today, fix $n \in \mathbb{Z}_{\geqslant 1}$, and assume all other variables are integers.

Proposition. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Proof outline. Recall that

$$a \equiv_n b \quad \Leftrightarrow \quad n | a - b \quad \Leftrightarrow \quad a - b = kn$$

for some $k \in \mathbb{Z}$. So since $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, we have

$$a_1 - b_1 = k_1 n \quad \text{and} \quad a_2 - b_2 = k_2 n$$

for some $k_1, k_2 \in \mathbb{Z}$. To prove the lemma, show (by direct computation) that

$$(a_1 + a_2) - (b_1 + b_2) = kn \quad \text{and } a_1 a_2 - b_1 b_2 = \ell n$$

for some $k, \ell \in \mathbb{Z}$.

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Either $b/a \in \mathbb{Z}$, or there is no solution.

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Either $b/a \in \mathbb{Z}$, or there is no solution.

In modular arithmetic, there are three possibilities:

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Either $b/a \in \mathbb{Z}$, or there is no solution.

In modular arithmetic, there are three possibilities:
The equation $ax \equiv b \pmod{n}$ either

1. has no solutions;
2. has one solution (up to congruence);
3. has multiple solutions (up to congruence).

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Either $b/a \in \mathbb{Z}$, or there is no solution.

In modular arithmetic, there are three possibilities:
The equation $ax \equiv b \pmod{n}$ either

1. has no solutions;
2. has one solution (up to congruence);
3. has multiple solutions (up to congruence).

Here, up to congruence means that we consider two solutions $x_1 \neq x_2$ to be the "same" if $x_1 \equiv x_2 \pmod{n}$.
For example, $x = 2$ is a solution to $3x \equiv 6 \pmod{10}$.

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Either $b/a \in \mathbb{Z}$, or there is no solution.

In modular arithmetic, there are three possibilities:
The equation $ax \equiv b \pmod{n}$ either

1. has no solutions;
2. has one solution (up to congruence);
3. has multiple solutions (up to congruence).

Here, up to congruence means that we consider two solutions $x_1 \neq x_2$ to be the "same" if $x_1 \equiv x_2 \pmod{n}$.
For example, $x = 2$ is a solution to $3x \equiv 6 \pmod{10}$. But so are

$$12,\ 22,\ 31,\ \ldots, \quad \text{as well as} \quad -8,\ -18,\ -28,\ \ldots.$$

Division

Homework: If $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \quad \text{implies} \quad a \equiv b \pmod{n}.$$

Division

Homework: If $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \quad \text{implies} \quad a \equiv b \pmod{n}.$$

This can be strengthened into an if and only if statement!

(What *is* the converse?)

Division

Homework: If $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \quad \text{implies} \quad a \equiv b \pmod{n}.$$

This can be strengthened into an if and only if statement!

(What *is* the converse?)

Prop. If $\gcd(c, n) \neq 1$, then there are a and b such that

$$ac \equiv bc \pmod{n} \quad \text{but} \quad a \not\equiv b \pmod{n}.$$

Division

Homework: If $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \quad \text{implies} \quad a \equiv b \pmod{n}.$$

This can be strengthened into an if and only if statement!

(What *is* the converse?)

Prop. If $\gcd(c, n) \neq 1$, then there are a and b such that

$$ac \equiv bc \pmod{n} \quad \text{but} \quad a \not\equiv b \pmod{n}.$$

Proof. Letting $\gcd(n, c) = g > 1$, there are $2 \leqslant k < n$ and $2 \leqslant \ell < c$ such that $kg = n$ and $\ell g = c$. So $ck = \ell gk = \ell n$. Therefore

$$ck \equiv_n 0 \equiv_n c \cdot 0.$$

But since $2 \leqslant k < n$, $k \not\equiv 0 \pmod{0}$.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving addition problems involves subtraction, which is straightforward:

If $a + x \equiv b \pmod{n}$, then

$$x \equiv_n a + x - a \equiv_n b - a.$$

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving addition problems involves subtraction, which is straightforward:

If $a + x \equiv b \pmod{n}$, then

$$x \equiv_n a + x - a \equiv_n b - a.$$

For example, if $2 + x \equiv_5 3$

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving addition problems involves subtraction, which is straightforward:

If $a + x \equiv b \pmod{n}$, then

$$x \equiv_n a + x - a \equiv_n b - a.$$

For example, if $2 + x \equiv_5 3$, then

$$x \equiv_5 2 - 3 = -1 \equiv_5 \boxed{4}.$$

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

Example: $4x \equiv 1 \pmod{7}$.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

Example: $4x \equiv 1 \pmod{7}$.
Since $\gcd(4, 7) = 1$, there will be a unique solution (up to congruence).
And since $1 \equiv_7 8 = 4 \cdot 2$, we have $x \equiv 2 \pmod{7}$ is that solution.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

Example: $4x \equiv 1 \pmod{7}$.
Since $\gcd(4, 7) = 1$, there will be a unique solution (up to congruence).
And since $1 \equiv_7 8 = 4 \cdot 2$, we have $x \equiv 2 \pmod{7}$ is that solution.

Example: $4x \equiv 8 \pmod{10}$.

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

Example: $4x \equiv 1 \pmod{7}$.
Since $\gcd(4, 7) = 1$, there will be a unique solution (up to congruence).
And since $1 \equiv_7 8 = 4 \cdot 2$, we have $x \equiv 2 \pmod{7}$ is that solution.

Example: $4x \equiv 8 \pmod{10}$.
Since $\gcd(4, 10) = 2$, we end up having more than one solution...

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

Example: $4x \equiv 1 \pmod{7}$.
Since $\gcd(4, 7) = 1$, there will be a unique solution (up to congruence).
And since $1 \equiv_7 8 = 4 \cdot 2$, we have $x \equiv 2 \pmod{7}$ is that solution.

Example: $4x \equiv 8 \pmod{10}$.
Since $\gcd(4, 10) = 2$, we end up having more than one solution...

x	0	1	2	3	4	5	6	7	8	9
$4x$	0	4	8	12	16	20	24	28	32	36
least residue	0	4	8	2	6	0	4	8	2	6

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

And if $\gcd(n, c) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Solving congruences.

Solving multiplication problems involves division, which is less straightforward.

Example: $4x \equiv 1 \pmod{7}$.
Since $\gcd(4, 7) = 1$, there will be a unique solution (up to congruence).
And since $1 \equiv_7 8 = 4 \cdot 2$, we have $x \equiv 2 \pmod{7}$ is that solution.

Example: $4x \equiv 8 \pmod{10}$.
Since $\gcd(4, 10) = 2$, we end up having more than one solution...

x	0	1	$\boxed{2}$	3	4	5	6	$\boxed{7}$	8	9
$4x$	0	4	8	12	16	20	24	28	32	36
least residue	0	4	$\boxed{8}$	2	6	0	4	$\boxed{8}$	2	6

Division

Example: Solve $4x \equiv 3 \pmod{19}$.

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a, n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$$ka + \ell n = 1.$$

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a, n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$$ka + \ell n = 1. \quad \text{So } 1 - ka = \ell n$$

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a, n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$ka + \ell n = 1.$ So $1 - ka = \ell n,$ implying $ka \equiv_n 1.$

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a, n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$ka + \ell n = 1.$ So $1 - ka = \ell n,$ implying $ka \equiv_n 1.$

Therefore

if $ax \equiv b \pmod{n}$, then $x \equiv_n kax \equiv kb.$

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a, n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$$ka + \ell n = 1. \quad \text{So } 1 - ka = \ell n, \quad \text{implying } ka \equiv_n 1.$$

Therefore

$$\text{if } ax \equiv b \pmod{n}, \quad \text{then} \quad x \equiv_n kax \equiv kb.$$

In our example above, $5 \cdot 4 = 20 \equiv 1 \pmod{19}$.

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a, n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$$ka + \ell n = 1. \quad \text{So } 1 - ka = \ell n, \quad \text{implying } ka \equiv_n 1.$$

Therefore

$$\text{if } ax \equiv b \pmod{n}, \quad \text{then} \quad x \equiv_n kax \equiv kb.$$

In our example above, $5 \cdot 4 = 20 \equiv 1 \pmod{19}$. So

$$x \equiv_{19} 5 \cdot 4 \cdot x \equiv_{19} 5 \cdot 3 \equiv_{19} 15.$$

Division

Example: Solve $4x \equiv 3 \pmod{6}$.

Division

Example: Solve $4x \equiv 3 \pmod{6}$.

This is equivalent to $6|(4x - 3)$.

Division

Example: Solve $4x \equiv 3 \pmod{6}$.

This is equivalent to $6|(4x - 3)$. (This is not possible!)

Division

Example: Solve $4x \equiv 3 \pmod{6}$.

This is equivalent to $6|(4x-3)$. (This is not possible!)

Claim: If you want to solve congruences of the form

$$ax \equiv b \pmod{n},$$

you have two cases, based on $d = \gcd(a,n)$.

1. If $d \nmid b$, then there are no solutions.
2. If $d|b$, then there are exactly d solutions (mod n).

   To find them, compute $u, v \in \mathbb{Z}$ such that $ua + vn = d$. Then

   $$b = (b/d)d = (b/d)ua + (b/d)vn,$$

   so that $x = (b/d)u$ is one solution. For the rest, add n/d until you have a full set.

Division

Example: Solve $4x \equiv 3 \pmod{6}$.

This is equivalent to $6|(4x-3)$. (This is not possible!)

Claim: If you want to solve congruences of the form

$$ax \equiv b \pmod{n},$$

you have two cases, based on $d = \gcd(a, n)$.

1. If $d \nmid b$, then there are no solutions.
2. If $d|b$, then there are exactly d solutions (mod n).

   To find them, compute $u, v \in \mathbb{Z}$ such that $ua + vn = d$. Then

   $$b = (b/d)d = (b/d)ua + (b/d)vn,$$

   so that $x = (b/d)u$ is one solution. For the rest, add n/d until you have a full set.

(Very Important) Corollary. An integer b has a (unique) multiplicative inverse modulo n if and only if $\gcd(b, n) = 1$.
Namely, if p is prime, then b has a multiplicative inverse modulo p if and only if $b \not\equiv_p 0$.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \quad \text{for all primes } p.$$

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \quad \text{for all primes } p.$$

Therefore, if we can prove that the theorem holds for $x \geqslant 0$, then

$$(-x)^p \equiv_p -x^p = (-1)x^p \equiv (-1)x = -x$$

as well. So we may assume henceforth that $x \geqslant 0$.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \quad \text{for all primes } p.$$

Therefore, if we can prove that the theorem holds for $x \geqslant 0$, then

$$(-x)^p \equiv_p -x^p = (-1)x^p \equiv (-1)x = -x$$

as well. So we may assume henceforth that $x \geqslant 0$.

(Aside: we often do this in mathematics with conjectures. If we think a powerful statement is true, but we can't yet prove it, we can state it as conjecture. Then, we might use that conjecture to prove other things. This either sets us up for a potential disproof by contradiction, or queues up a bunch of results that will have been proven true as soon as someone actually proves the conjecture. Here, the useful conjecture is $x^p \equiv_p x$ for all $x \in \mathbb{Z}_{\geqslant 0}$.)

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \quad \text{for all primes } p.$$

Therefore, if we can prove that the theorem holds for $x \geqslant 0$, then

$$(-x)^p \equiv_p -x^p = (-1)x^p \equiv (-1)x = -x$$

as well. So we may assume henceforth that $x \geqslant 0$.

(Aside: we often do this in mathematics with conjectures. If we think a powerful statement is true, but we can't yet prove it, we can state it as conjecture. Then, we might use that conjecture to prove other things. This either sets us up for a potential disproof by contradiction, or queues up a bunch of results that will have been proven true as soon as someone actually proves the conjecture. Here, the useful conjecture is $x^p \equiv_p x$ for all $x \in \mathbb{Z}_{\geqslant 0}$.)

We will prove the theorem for $x \geqslant 0$ by induction on x.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \quad \text{for all primes } p.$$

Therefore, if we can prove that the theorem holds for $x \geqslant 0$, then

$$(-x)^p \equiv_p -x^p = (-1)x^p \equiv (-1)x = -x$$

as well. So we may assume henceforth that $x \geqslant 0$.

(Aside: we often do this in mathematics with conjectures. If we think a powerful statement is true, but we can't yet prove it, we can state it as conjecture. Then, we might use that conjecture to prove other things. This either sets us up for a potential disproof by contradiction, or queues up a bunch of results that will have been proven true as soon as someone actually proves the conjecture. Here, the useful conjecture is $x^p \equiv_p x$ for all $x \in \mathbb{Z}_{\geqslant 0}$.)

We will prove the theorem for $x \geqslant 0$ by induction on x. First, we have $0^p = 0 \equiv_p 0$, as desired.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \quad \text{for all primes } p.$$

Therefore, if we can prove that the theorem holds for $x \geqslant 0$, then

$$(-x)^p \equiv_p -x^p = (-1)x^p \equiv (-1)x = -x$$

as well. So we may assume henceforth that $x \geqslant 0$.

(Aside: we often do this in mathematics with conjectures. If we think a powerful statement is true, but we can't yet prove it, we can state it as conjecture. Then, we might use that conjecture to prove other things. This either sets us up for a potential disproof by contradiction, or queues up a bunch of results that will have been proven true as soon as someone actually proves the conjecture. Here, the useful conjecture is $x^p \equiv_p x$ for all $x \in \mathbb{Z}_{\geqslant 0}$.)

We will prove the theorem for $x \geqslant 0$ by induction on x. First, we have $0^p = 0 \equiv_p 0$, as desired. Next, fix $x \geqslant 0$, and assume $x^p \equiv_p x$.

Theorem. (Fermat's little theorem)
If p is prime, then $x^p \equiv_p x$ for all $x \in \mathbb{Z}$.

Proof. First note that either $p = 2$, or $(-x)^p = -x^p$. And for $p = 2$, then $-a \equiv_2 a$ for all $a \in \mathbb{Z}$, so that $(-x)^2 \equiv_2 -x^p$. So

$$(-x)^p \equiv_p -x^p \qquad \text{for all primes } p.$$

Therefore, if we can prove that the theorem holds for $x \geqslant 0$, then

$$(-x)^p \equiv_p -x^p = (-1)x^p \equiv (-1)x = -x$$

as well. So we may assume henceforth that $x \geqslant 0$.

(Aside: we often do this in mathematics with conjectures. If we think a powerful statement is true, but we can't yet prove it, we can state it as conjecture. Then, we might use that conjecture to prove other things. This either sets us up for a potential disproof by contradiction, or queues up a bunch of results that will have been proven true as soon as someone actually proves the conjecture. Here, the useful conjecture is $x^p \equiv_p x$ for all $x \in \mathbb{Z}_{\geqslant 0}$.)

We will prove the theorem for $x \geqslant 0$ by induction on x. First, we have $0^p = 0 \equiv_p 0$, as desired. Next, fix $x \geqslant 0$, and assume $x^p \equiv_p x$. Then, using the binomial theorem,

$$(x+1)^p \equiv_p \cdots \qquad \text{Homework!}$$

Wrapping up elementary number theory...

Chapters 27–29 in "How to think..." (on primes, divisors, gcd, Euclidean algorithm, modular arithmetic, etc.) are a *brief* introduction to elementary number theory.

To learn more: Take "Theory of Numbers" (Math 345).

Where else this is used: Modular arithmetic is a *Very Important Example* in "Modern Algebra" (a.k.a. "abstract algebra"), Math 347/A49.