Modular Arithmetic

Theorem 4.2.1

Fix a modulus m. Let a, b, c, d be integers such that

$$a \equiv c \pmod{m} \qquad \textit{and} \qquad b \equiv d \pmod{m}.$$

Then we have

$$a + b \equiv c + d \pmod{m} \qquad \textit{and} \qquad ab \equiv cd \pmod{m}.$$

Theorem 4.2.1

Fix a modulus m. Let a, b, c, d be integers such that

$$a \equiv c \pmod{m} \qquad \textit{and} \qquad b \equiv d \pmod{m}.$$

Then we have

$$a + b \equiv c + d \pmod{m} \qquad \textit{and} \qquad ab \equiv cd \pmod{m}.$$

Proof. (Product) Suppose $a - c = k_1 m$ and $b - d = k_2 m$. Then

$$ab = (c + k_1 m)(d + k_2 m) = cd + (k_1 d + k_2 c + k_1 k_2 m)m.$$

Hence, $m \mid ab - cd$. $\square$

The previous theorem tells us that the congruence class of the sum/product is independent of the choice of representatives. We thus are able to define the *addition* and *multiplication* of congruence classes.

Definition 4.2.2

The *sum* of two congruence classes $[a]_m$ and $[b]_m$ is $[a+b]_m$. The *product* of two congruence classes $[a]_m$ and $[b]_m$ is $[ab]_m$.

Definition 4.2.2

The *sum* of two congruence classes $[a]_m$ and $[b]_m$ is $[a+b]_m$. The *product* of two congruence classes $[a]_m$ and $[b]_m$ is $[ab]_m$.

Example 4.2.3

$[1234567]_{10} \cdot [20230208]_{10} =$

$[7]_{10} \cdot [8]_{10} = [56]_{10} = [6]_{10}$

Definition 4.2.4

The residue set $\mathbb{Z}/m$ together with the *addition* and *multiplication* of congruence classes and the neutral elements $\mathbf{0} := [0]_m$ and $\mathbf{1} := [1]_m$ of them respectively, is called the *residue ring modulo* m.

We have a *residue map*:

$$\pi_m : \mathbb{Z} \longrightarrow \mathbb{Z}/m : a \mapsto [a]_m$$

respecting their structures.

We can translate problems on $\mathbb{Z}$ through π_m. Note that this map is not bijective, hence solving problems on $\mathbb{Z}/m$ doesn't mean solving problems on $\mathbb{Z}$. However, since any solution in $\mathbb{Z}$ will *descend* to a solution in $\mathbb{Z}/m$, it is convenient to use modular arithmetic to disprove problems on $\mathbb{Z}$.

$a^2 + b^2 = 3c^2$ mod 4

We can translate problems on $\mathbb{Z}$ through π_m. Note that this map is not bijective, hence solving problems on $\mathbb{Z}/m$ doesn't mean solving problems on $\mathbb{Z}$. However, since any solution in $\mathbb{Z}$ will *descend* to a solution in $\mathbb{Z}/m$, it is convenient to use modular arithmetic to disprove problems on $\mathbb{Z}$.

Example 4.2.5

If $X^2 + Y^2 = 3Z^2$ has any integer solution, then it descends to a solution in $\mathbb{Z}/4$. But we can verify that there is no such a solution in $\mathbb{Z}/4$.

Definition 4.2.6

Fix a modulus m. A congruence class α is a *unit* in $\mathbb{Z}/m$ if there is a congruence class β such that $\alpha\beta = 1$. The class β is called the *multiplicative inverse* of α. Suppose a and b are representatives of α and β respectively. Then we say a is *(multiplicative) invertible modulo* m and b is a *multiplicative inverse of* a *modulo* m.

Definition 4.2.6

Fix a modulus m. A congruence class α is a *unit* in $\mathbb{Z}/m$ if there is a congruence class β such that $\alpha\beta = 1$. The class β is called the *multiplicative inverse* of α. Suppose a and b are representatives of α and β respectively. Then we say a is *(multiplicative) invertible modulo* m and b is a *multiplicative inverse of* a *modulo* m.

Example 4.2.7

$2 \cdot 3 \equiv 2 \cdot 8 \equiv 1 \pmod 5$. Hence, 2 is (multiplicative) invertible modulo 5, and 3 and 8 are two multiplicative inverse of 2 modulo 5.

Theorem 4.2.8

Fix a modulus m. An integer a is invertible modulo m if and only if a is coprime to m.

Theorem 4.2.8

Fix a modulus m. An integer a is invertible modulo m if and only if a is coprime to m.

Proof. a is invertible modulo m

$\iff$ there is $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$

Theorem 4.2.8

Fix a modulus m. An integer a is invertible modulo m if and only if a is coprime to m.

Proof. a is invertible modulo m

$\iff$ there is $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$

$\iff$ there is $b \in \mathbb{Z}$ such that $m \mid ab - 1$

Theorem 4.2.8

Fix a modulus m. An integer a is invertible modulo m if and only if a is coprime to m.

Proof. a is invertible modulo m

$\iff$ there is $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$

$\iff$ there is $b \in \mathbb{Z}$ such that $m \mid ab - 1$ $\quad ab-1 = -mk$

$\iff$ the Diophantine equation $aX + mY = 1$ has integer solutions.

$ab + mk = 1$

Theorem 4.2.8

Fix a modulus m. An integer a is invertible modulo m if and only if a is coprime to m.

Proof. a is invertible modulo m

$\iff$ there is $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$

$\iff$ there is $b \in \mathbb{Z}$ such that $m \mid ab - 1$

$\iff$ the Diophantine equation $aX + mY = 1$ has integer solutions.

The last is equivalent to $\gcd(a, m) = 1$ by the Bézout's identity. $\square$

Question (Linear congruent equation)

Find integer $x \in \mathbb{Z}$ *such that*

$a X =$

$$ax \equiv b \pmod{m}.$$

Equivalently, find congruence class $X \in \mathbb{Z}/m$ *such that*

$$[a]_m \cdot X = [b]_m.$$

$X = [a]^{-1} \cdot [b]$

Question (Linear congruent equation)

Find integer $x \in \mathbb{Z}$ *such that*

$$ax \equiv b \pmod{m}.$$

Equivalently, find congruence class $X \in \mathbb{Z}/m$ *such that*

$$[a]_m \cdot X = [b]_m.$$

Theorem 4.2.9 (Cancelling)

If a *is invertible modulo* m, *then*

$$a \cdot x \equiv a \cdot y \pmod{m} \implies x \equiv y \pmod{m}.$$

Example 4.2.10

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

Example 4.2.10

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

1. Verify if 15 is coprime to 37.

Example 4.2.10

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

1. Verify if 15 is coprime to 37.

$$\begin{aligned} 37 &= 2 \cdot 15 + 7 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned}$$

Example 4.2.10

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

1. Verify if 15 is coprime to 37.

$$\begin{aligned} 37 &= 2 \cdot 15 + 7 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 15 - 2 \cdot 7 \\ &= 15 - 2 \cdot (37 - 2 \cdot 15) \\ &= 5 \cdot 15 - 2 \cdot 37. \end{aligned}$$

Example 4.2.10

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

1. Verify if 15 is coprime to 37.

$$\begin{aligned} 37 &= 2 \cdot 15 + 7 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 15 - 2 \cdot 7 \\ &= 15 - 2 \cdot (37 - 2 \cdot 15) \\ &= 5 \cdot 15 - 2 \cdot 37. \end{aligned}$$

2. Find a multiplicative inverse of 15 modulo 37.

Example 4.2.10

Solve: $15 \cdot x \equiv 4 \pmod{37}$.

1. Verify if 15 is coprime to 37.

$$37 = 2 \cdot 15 + 7 \qquad 1 = 15 - 2 \cdot 7$$
$$15 = 2 \cdot 7 + 1 \qquad = 15 - 2 \cdot (37 - 2 \cdot 15)$$
$$7 = 7 \cdot 1 + 0 \qquad = 5 \cdot 15 - 2 \cdot 37.$$

2. Find a multiplicative inverse of 15 modulo 37.
3. Cancelling:

$$15 \cdot x \equiv 4 \pmod{37} \Longrightarrow x \equiv 5 \cdot 4 \equiv 20 \pmod{37}.$$

$$x \equiv \text{“}15\text{”}^{-1} \cdot 4$$