Modular Arithmetic

Basic Concepts and Applications

None W., Pana W., Sean W.

Outline

Section 1

Basic Definitions

Congruence Modulo n

Definition

Let n be a positive integer. Two integers a and b are **congruent modulo n** if n divides $(a-b)$.
We write: $a \equiv b \pmod{n}$

Equivalent Definitions

The following are equivalent:

1. a and b have the same remainder when divided by n
2. $a - b = kn$ for some integer k
3. $n \mid (a-b)$
4. $a \equiv b \pmod{n}$

Examples of Congruence

Example

$$17 \equiv 5 \pmod{12} \quad \text{because } 17 - 5 = 12 = 1 \cdot 12 \tag{1}$$
$$-3 \equiv 9 \pmod{12} \quad \text{because } -3 - 9 = -12 = -1 \cdot 12 \tag{2}$$
$$25 \equiv 1 \pmod{12} \quad \text{because } 25 - 1 = 24 = 2 \cdot 12 \tag{3}$$

Verification by Division

- $17 = 1 \cdot 12 + 5$ (remainder 5)
- $5 = 0 \cdot 12 + 5$ (remainder 5)
- Since both have remainder 5, $17 \equiv 5 \pmod{12}$

Section 2

Properties of Congruence

Properties of Congruence

Theorem (Basic Properties)

Let n be a positive integer. Then congruence modulo n is:

1. **Reflexive:** $a \equiv a \pmod{n}$
2. **Symmetric:** *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$
3. **Transitive:** *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$

Arithmetic Properties

Theorem (Arithmetic with Congruences)

If $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then:*

1. $a + c \equiv b + d \pmod{n}$
2. $a - c \equiv b - d \pmod{n}$
3. $ac \equiv bd \pmod{n}$
4. $a^k \equiv b^k \pmod{n}$ *for any positive integer* k

Example

Since $17 \equiv 5 \pmod{12}$ and $13 \equiv 1 \pmod{12}$:

$$17 + 13 \equiv 5 + 1 \equiv 6 \pmod{12} \tag{4}$$

$$17 \cdot 13 \equiv 5 \cdot 1 \equiv 5 \pmod{12} \tag{5}$$

Section 3

Applications

Computing with Large Numbers

Example

Compute $2^{100} \pmod 7$.

Solution

First, let's find the pattern of powers of 2 modulo 7:

$$2^1 \equiv 2 \pmod 7 \tag{6}$$
$$2^2 \equiv 4 \pmod 7 \tag{7}$$
$$2^3 = 8 \equiv 1 \pmod 7 \quad \text{(loops back to 1)} \tag{8}$$
$$2^4 \equiv 2^3 \cdot 2^1 \equiv 1 \cdot 2 \equiv 2 \pmod 7 \quad \text{(back to 2!)} \tag{9}$$

The pattern repeats every 3 steps: $2, 4, 1, 2, 4, 1, \ldots$

Computing with Large Numbers (continued)

Solution (continued)

Since $100 = 3 \cdot 33 + 1$, we have:

$$
\begin{aligned}
2^{100} &= 2^{3 \cdot 33 + 1} && (10)\\
&= (2^3)^{33} \cdot 2^1 && (11)\\
&\equiv 1^{33} \cdot 2 \pmod 7 && (12)\\
&\equiv 1 \cdot 2 \equiv 2 \pmod 7 && (13)
\end{aligned}
$$

Finding Unit Digits

Example

Find the unit digit of 23^{343}.

Solution

To find the unit digit, we compute $23^{343} \pmod{10}$.
Since $23 \equiv 3 \pmod{10}$, we need to find $3^{343} \pmod{10}$.
First, let's find the pattern of powers of 3 modulo 10:

$$3^1 \equiv 3 \pmod{10} \tag{14}$$
$$3^2 \equiv 9 \pmod{10} \tag{15}$$
$$3^3 = 27 \equiv 7 \pmod{10} \tag{16}$$
$$3^4 = 3^3 \cdot 3^1 \equiv 7 \cdot 3 \equiv 21 \equiv 1 \pmod{10} \quad \text{(cycle complete!)} \tag{17}$$

The pattern repeats every 4 steps: $3, 9, 7, 1, 3, 9, 7, 1, \ldots$

Finding Unit Digits (continued)

Solution (continued)

Since $343 = 4 \cdot 85 + 3$, we have:

$$\begin{aligned}
3^{343} &= 3^{4\cdot 85+3} && (18)\\
&= (3^4)^{85} \cdot 3^3 && (19)\\
&\equiv 1^{85} \cdot 7 \pmod{10} && (20)\\
&\equiv 1 \cdot 7 \equiv 7 \pmod{10} && (21)
\end{aligned}$$

Therefore, the unit digit of 23^{343} is $\boxed{7}$.

Exercise

Problem 27, POSN Computer 2562

Find the remainder of $2018^{2019} + 2019^{2020} + 2020^{2021}$ when divided by 13.

Days of the Week

Day Calculation

We can use modular arithmetic to determine what day of the week a given date falls on.
Each day corresponds to a number modulo 7:

- Sunday = 0, Monday = 1, ..., Saturday = 6

Example

If today is Wednesday (day 3), what day will it be in 100 days?
$3 + 100 = 103$
$103 = 14 \cdot 7 + 5$, so $103 \equiv 5 \pmod 7$
Day 5 corresponds to Friday.

Section 4

GCD and LCM

Greatest Common Divisor (GCD)

Definition

The **greatest common divisor** of two integers a and b (not both zero) is the largest positive integer that divides both a and b.
We write: $\gcd(a, b)$ or (a, b)

Properties

- $\gcd(a, 0) = |a|$ for any non-zero integer a
- $\gcd(a, b) = \gcd(b, a)$ (symmetry)
- $\gcd(a, b) = \gcd(a, b \bmod a)$ if $a > 0$

Euclidean Algorithm

Example

Find $\gcd(252, 105)$:

$$
\begin{aligned}
gcd(252,105) &= \gcd(105, 252 \mod 105) && (22)\\
&= \gcd(105, 42) && (23)\\
&= \gcd(42, 105 \mod 42) && (24)\\
&= \gcd(42, 21) && (25)\\
&= \gcd(21, 42 \mod 21) && (26)\\
&= \gcd(21, 0) && (27)\\
&= 21 && (28)
\end{aligned}
$$

Therefore, $\gcd(252, 105) = 21$.

Bézout's Identity

Theorem (Bézout's Identity)

For any integers a and b (not both zero), there exist integers x and y such that:

$$ax + by = \gcd(a, b)$$

These integers x and y are called **Bézout coefficients**.

Extended Euclidean Algorithm

We can find the Bézout coefficients by working backwards through the Euclidean algorithm.

Bézout's Identity Example

Example

Find integers x and y such that $252x + 105y = \gcd(252, 105) = 21$.

Solution

Working backwards from our Euclidean algorithm:

$$
\begin{aligned}
21 &= 105 - 2 \cdot 42 && (29) \\
&= 105 - 2 \cdot (252 - 2 \cdot 105) && (30) \\
&= 105 - 2 \cdot 252 + 4 \cdot 105 && (31) \\
&= 5 \cdot 105 - 2 \cdot 252 && (32) \\
&= (-2) \cdot 252 + 5 \cdot 105 && (33)
\end{aligned}
$$

Therefore, $x = -2$ and $y = 5$.
Verification: $252(-2) + 105(5) = -504 + 525 = 21$ ✓

Least Common Multiple (LCM)

Definition

The **least common multiple** of two positive integers a and b is the smallest positive integer that is divisible by both a and b.
We write: $\text{lcm}(a, b)$ or $[a, b]$

Theorem (Fundamental Relationship)

For any positive integers a and b:

$$\gcd(a, b) \times \mathit{lcm}(a, b) = a \times b$$

GCD and LCM Example

Example

If two number a and b have $\gcd(a,b) = 10$ and $\mathsf{lcm}(a,b) = 100$, find $a \times b$.

Solution

We know that $\gcd(a,b) \times \mathsf{lcm}(a,b) = a \times b$.
Therefore, $a \times b = 10 \times 100 = 1000$.