Modular Arithmetic

Al-Tarazi Assaubay

Senior Lecturer

Department of Computational and Data Sciences

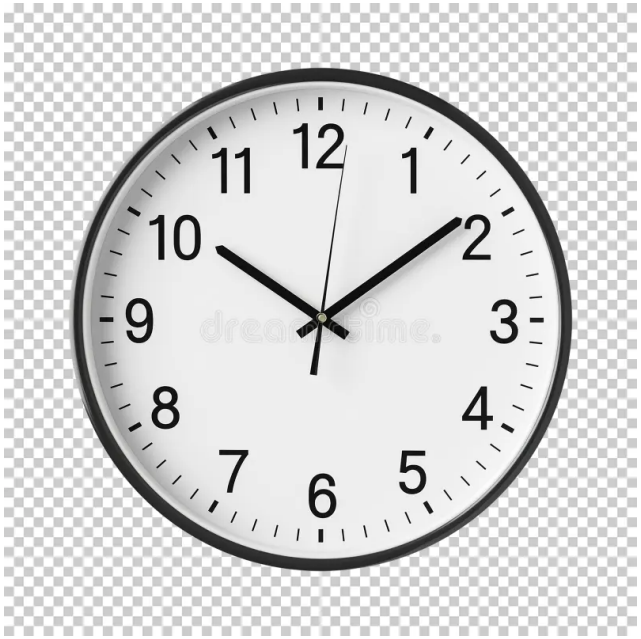
Department of Intelligent Systems and Cybersecurity

Basic concept

Modular arithmetic is a system of arithmetic for integers where numbers follow cyclic continuation rather than linear because of the **modulus**.

For example, consider a clock.

- Hour marks follow a system with modulus 12,
- Minute marks follow a system with modulus 60.



Basic properties

For a, b integers and n a positive integer we have the following

- $\left[a \pmod n + b \pmod n\right] \pmod n = (a+b) \pmod n$
- $\left[a \pmod n - b \pmod n\right] \pmod n = (a-b) \pmod n$
- $\left[a \pmod n \times b \pmod n\right] \pmod n = (a \times b) \pmod n$

Examples

1. Sum Property:

$$(17+5) \pmod{12} = 22 \pmod{12} = 10$$

$$[17 \pmod{12} + 5 \pmod{12}] \pmod{12} = (5+5) \pmod{12} = 10$$

2. Difference Property:

$$(17-5) \pmod{12} = 12 \pmod{12} = 0$$

$$[17 \pmod{12} - 5 \pmod{12}] \pmod{12} = (5-5) \pmod{12} = 0$$

3. Product Property:

$$(17 \cdot 5) \pmod{12} = 85 \pmod{12} = 1$$

$$[17 \pmod{12} \cdot 5 \pmod{12}] \pmod{12} = (5 \cdot 5) \pmod{12} = 1$$

Other properties

Property	Example (mod n)
Commutative	$(a+b) \mod n = (b+a) \mod n$ $(a \cdot b) \mod n = (b \cdot a) \mod n$
Associative	$((a+b)+c) \mod n = (a+(b+c)) \mod n$ $((a \cdot b) \cdot c) \mod n = (a \cdot (b \cdot c)) \mod n$
Distributive	$(a \cdot (b+c)) \mod n = ((a \cdot b)+(a \cdot c)) \mod n$
Identity (Additive)	$(a+0) \mod n = a \mod n$
Identity (Multiplicative)	$(a \cdot 1) \mod n = a \mod n$
Additive Inverse	$(a+(-a)) \mod n = 0$

Modular Exponentiation

Use congruence:

$$\begin{aligned}
89^{16} \pmod{100} &= (-11)^{16} \pmod{100} = \left[(-11)^2\right]^8 \pmod{100} \\
&= 121^8 \pmod{100} = 21^8 \pmod{100} = \\
&= (21^2)^4 \pmod{100} = 441^4 \pmod{100} \\
&= 41^4 \pmod{100} = (41^2)^2 \pmod{100} \\
&= 1681^2 \pmod{100} = 81^2 \pmod{100} \\
&= (-19)^2 \pmod{100} = 361 \pmod{100} \\
&= 61.
\end{aligned}$$

Try: $17^8 \pmod{14}$, $34^{15} \pmod{41}$.

Solution 1

$$\begin{aligned} 17^8 \pmod{14} &= 3^8 \pmod{14} = 3^{(2\cdot 4)} \pmod{14} \\ &= 9^4 \pmod{14} = (-5)^4 \pmod{14} = \\ &= 25^2 \pmod{14} = 11^2 \pmod{14} \\ &= (-3)^2 \pmod{14} = 9 \pmod{14} \\ &= 9. \end{aligned}$$

Solution 2

$$34^{15} \pmod{41} = 7^{15} \pmod{41} = 7^{1+2+4+8} \pmod{41} = 7^1 \cdot 7^2 \cdot 7^4 \cdot 7^8 \pmod{41}$$

- $7^2 \pmod{41} = 49 \pmod{41} = -8 \pmod{41}$
- $7^4 \pmod{41} = (7^2)^2 \pmod{41} = (-8)^2 \pmod{41} = 64 \pmod{41} = 23 \pmod{41}$
- $7^8 \pmod{41} = (7^4)^2 \pmod{41} = 23^2 \pmod{41} = 529 \pmod{41} = 37 \pmod{41} = -4 \pmod{41}$.

Then, we have: $7^1 \cdot (-8) \cdot 23 \cdot (-4) \cdot \pmod{41} = (-56) \cdot (-92) \pmod{41}$

$$= (-15) \cdot (-10) \pmod{41} = 150 \pmod{41} = 27.$$

Modular Exponentiation example

What are the last two digits of 14^8?

Hint: $\pmod{100}$ provides last two digits, $\pmod{1000}$ provides last three digits etc.

$$\begin{aligned} 14^8 \pmod{100} &= (14^2)^4 \pmod{100} = 196^4 \pmod{100} \\ &= (-4)^4 \pmod{100} = 16^2 \pmod{100} \\ &= 256 \pmod{100} = 56. \end{aligned}$$

Answer: "56" are the last two digits of 14^8.

Fermat's little theorem

Theorem (Fermat's little theorem)

If p is a prime number. and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{or} \quad a^p \equiv a \pmod{p}.$$

Example:

$$24^{10} \pmod{11} = 24^{11-1} \pmod{11} = 1.$$

$$24^{10} \pmod{11} = 2^{10} \pmod{11} = (2^5)^2 \pmod{11}$$

$$= 32^2 \pmod{11} = (10)^2 \pmod{11} = 100 \pmod{11} = 1.$$

Multiplicative inverse: Definition

We cannot technically divide in modular arithmetic, since modular arithmetic is a system of integers and division often results in decimal numbers. That is why we use multiplicative inversion as an alternative operation for division. Reminder:

Definition

Suppose $a \in \mathbb{Z}_n$. Then $a^{-1} \pmod{n}$ is called the multiplicative inverse of a modulo n if and only if

$$a \cdot a^{-1} \pmod{n} = a^{-1} \cdot a \pmod{n} = 1$$

Multiplicative inverse: Solution

Multiplicative inverse a^{-1} of a modulo n exists if and only if $\gcd(a,n) = 1$.

- Use Euclidean Algorithm to find that $\gcd(a,n) = 1$.
- Rewrite the equations of Euclidean Algorithm as a linear combination $\gcd(a,n) = 1 = a \cdot x + n \cdot y$.
- x is multiplicative inverse of a.

Multiplicative Inverse: Example

Find $19^{-1} \pmod{26}$. First, let's use Euclidean Algorithm:

$$\begin{aligned} 26 &= 1 \cdot 19 + 7 & 7 &= 26 - 19 \\ 19 &= 2 \cdot 7 + 5 & 5 &= 19 - 2 \cdot 7 \\ 7 &= 1 \cdot 5 + 2 & 2 &= 7 - 5 \\ 5 &= 2 \cdot 2 + 1 & \mathbf{1} &= \mathbf{5} - \mathbf{2} \cdot \mathbf{2} \end{aligned}$$

Then, trace back the equation on the second column and leave 19 and 26 intact.

Multiplicative Inverse: Example cont.

$$
\begin{aligned}
7 &= 26 - 19 \\
5 &= 19 - 2 \cdot 7 \\
2 &= 7 - 5 \\
\mathbf{1} &= \mathbf{5} - \mathbf{2} \cdot \mathbf{2}
\end{aligned}
$$

$$
\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2(7 - 5) \\
&= 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 \\
&= 3 \cdot 19 - 8 \cdot 7 \\
&= 3 \cdot 19 - 8 \cdot (26 - 19) \\
&= \mathbf{11} \cdot \mathbf{19} - 8 \cdot 26
\end{aligned}
$$

$$11 = 19^{-1} \pmod{26} \quad \Longleftarrow$$

Practice: $31^{-1} \pmod{121}$

Solution

1. Find $\gcd(31, 121)$:

$$\begin{aligned} 121 &= 3 \cdot 31 + 28 & \qquad 28 &= 121 - 3 \cdot 31 \\ 31 &= 1 \cdot 28 + 3 & \qquad 3 &= 31 - 28 \\ 28 &= 9 \cdot 3 + 1 & \qquad \mathbf{1} &= \mathbf{28 - 9 \cdot 3} \end{aligned}$$

2. Find inverse:

$$\begin{aligned} 1 &= 28 - 9 \cdot 3 = 28 - 9 \cdot (31 - 28) \\ &= 10 \cdot 28 - 9 \cdot 31 = 10 \cdot (121 - 3 \cdot 31) - 9 \cdot 31 \\ &= 10 \cdot 121 - \mathbf{39} \cdot \mathbf{31} \end{aligned}$$

Thus, inverse is: $-39 \pmod{121} = 82 = 31^{-1} \pmod{121}$

Co-prime numbers, Euler totient function

Recall:

Definition

Suppose $a \geq 1, m \geq 2$ are integers. Then a, m are co-prime if and only if $\gcd(a,m) = 1$.

Now, we define Euler totient function:

Definition

Euler totient function $\phi(n)$ is a number of positive integers that are less than n and are co-prime to n.

Euler totient function formula

Table of formula for Euler totient function:

Type of Number n	Formula for $\phi(n)$
$n = p$	$\phi(p) = p - 1$
$n = pq$	$\phi(n) = (p-1)(q-1)$
$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$	$\phi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$

Euler totient function: examples

1. $n = 79, \ \phi(79) = 79 - 1 = 78.$
2. $n = 77 = 11 \cdot 7, \ \phi(77) = (7-1)(11-1) = 6 \cdot 10 = 60$
3. $n = 273 = 3 \cdot 7 \cdot 13$

$$\begin{aligned}\phi(273) &= 273 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{13}\right) \\ &= 3 \cdot 7 \cdot 13 \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{12}{13} \\ &= 2 \cdot 6 \cdot 12 = 144.\end{aligned}$$