Modular Arithmetic (Congruence also covered)

Modular Arithmetic

- ★ System of arithmetic for integers.
- ★ Wrap around after reaching a certain value called modulus.
- ★ Central mathematical concept in cryptography.

Congruence

★ In cryptography, congruence(≡) instead of equality(=).

Examples:

$15 \equiv 3 \pmod{12}$

$$\begin{array}{r|l} & 1 \\ \hline 12 & 15 \\ & 12 \\ \hline & 3 \end{array}$$

Congruence

★ In cryptography, congruence($\equiv$) instead of equality($=$).

Examples:

$15 \equiv 3 \pmod{12}$

$23 \equiv 11 \pmod{12}$

$33 \equiv 3 \pmod{10}$

$10 \equiv -2 \pmod{12}$

$\therefore a \equiv b \pmod{m}$

i.e. $a = km + b$

$$\begin{array}{r|l} & 1 \\ 12 & 15 \\ & 12 \\ \hline & 3 \end{array} \qquad \begin{array}{r|l} & 1 \\ 12 & 23 \\ & 12 \\ \hline & 11 \end{array} \qquad \begin{array}{r|l} & 3 \\ 10 & 33 \\ & 30 \\ \hline & 3 \end{array}$$

$$\begin{array}{r|l} & 0 \\ 12 & 10 \\ & 0 \\ \hline & 10 \\ & (-2) \end{array} \qquad \begin{array}{r|l} & k \\ m & a \\ & \\ \hline & b \end{array}$$

Valid or Invalid

- $38 \equiv 2 \pmod{12}$ ✓
- $38 \equiv 14 \pmod{12}$ ✓
- $5 \equiv 0 \pmod{5}$ ✓
- $10 \equiv 2 \pmod{6}$ ✗
- $13 \equiv 3 \pmod{13}$ ✗
- $2 \equiv -3 \pmod{5}$ ✓

One more analogy

Circumference: 10

Length: 35

No. of Wraps (Quotient)	Remaining thread (Remainder)	Congruence
1	25	$35 \equiv 25 \bmod 10$
2	15	$35 \equiv 15 \bmod 10$
3	5	$35 \equiv 5 \bmod 10$

Properties of Modular Arithmetic

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Properties of Modular Arithmetic

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Example:

$$[(15 \bmod 8) + (11 \bmod 8)] \bmod 8 = (15 + 11) \bmod 8$$
$$= 26 \bmod 8$$
$$= 2$$

Properties of Modular Arithmetic

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Example:

$$[(15 \bmod 8) - (11 \bmod 8)] \bmod 8 = (15 - 11) \bmod 8$$
$$= 4 \bmod 8$$
$$= 4$$

Properties of Modular Arithmetic

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Example:

$$
\begin{aligned}
[(15 \bmod 8) \times (11 \bmod 8)] \bmod 8 &= (15 \times 11) \bmod 8 \\
&= 165 \bmod 8 \\
&= 5
\end{aligned}
$$

Properties of Modular Arithmetic

Property	Expression
Commutative Laws	$(a + b) \bmod n = (b + a) \bmod n$ $(a \times b) \bmod n = (b \times a) \bmod n$
Associative Laws	$[(a + b) + c] \bmod n = [a + (b + c)] \bmod n$ $[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$
Distributive Laws	$[a \times (b + c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$
Identities	$(0 + a) \bmod n = a \bmod n$ $(1 \times a) \bmod n = a \bmod n$
Additive Inverse	For each $a \in Z_n$, there exists a '$-a$' such that $a + (-a) \equiv 0 \bmod n$

Fast Modular Arithmetic (Modular exponentiation)

Modular Exponentiation

- It is a type of exponentiation performed over a modulus.
- a^b mod m or a^b (mod m).

Examples:

2^{33} mod 30

3^{100} mod 29

Example 1

Solve 23^3 mod 30.

23^3 mod 30 $= -7^3$ mod 30 || 23 mod 30 can be 23 or -7.

$= -7^3$ mod 30

$= -7^2 \times -7$ mod 30

$= 49 \times -7$ mod 30

$= -133$ mod 30

$= -13$ mod 30

$= 17$ mod 30

23^3 mod 30 $= 17$

Example 2

Solve 31^{500} mod 30.

$$
\begin{aligned}
31^{500} \bmod 30 &= 1^{500} \bmod 30 \\
&= 1 \bmod 30 \\
&= 1
\end{aligned}
$$

$31^{500} \bmod 30 = 1$

Example 3

Solve 242^{329} mod 243.

$$
\begin{aligned}
242^{329} \bmod 243 &= -1^{329} \bmod 243 \\
&= -1^{329} \bmod 243 \;||\; -1^{328} \times -1^{1} \\
&= -1 \bmod 243 \\
&= 242
\end{aligned}
$$

242^{329} mod 243 = 242

Example 4

Solve 11^7 mod 13.

11^7 mod 13 = 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13

= -2 x -2 x -2 x -2 x -2 x -2 x -2 mod 13

= -128 mod 13

= -11 mod 13

= 2

11^7 mod 13 = 2

Example 1

Solve 88^7 mod 187.

88^1 mod 187 $= 88$

88^2 mod 187 $= 88^1 \times 88^1$ mod 187 $= 88 \times 88 = 7744$ mod 187 $= 77$

88^4 mod 187 $= 88^2 \times 88^2$ mod 187 $= 77 \times 77 = 5929$ mod 187 $= 132$

88^7 mod 187 $= 88^4 \times 88^2 \times 88^1$ mod 187 $= (132 \times 77 \times 88)$ mod 187

$= 894{,}432$ mod 187

88^7 mod 187 $= 11$

Example 2

What is "the last two digits" of 29^5?

$29^1 \bmod 100 = 29$ or -71

$29^2 \bmod 100 = 29^1 \times 29^1 \bmod 100 = 29 \times 29 = 841 \bmod 100 = 41$ or -59

$29^4 \bmod 100 = 29^2 \times 29^2 \bmod 100 = 41 \times 41 = 1681 \bmod 100 = 81$ or -19

$29^5 \bmod 100 = 29^4 \times 29^1 \bmod 100$

$= -19 \times 29 \bmod 100$

$= -551 \bmod 100$

$= -51 \bmod 100$

$= 49$

$88^7 \bmod 187 = 49$

Example 3

Solve $3^{100} \bmod 29$.

$3^1 \bmod 29 = 3 \bmod 29 = 3$ or -26.

$3^2 \bmod 29 = 3^1 \times 3^1 \bmod 29 = 3 \times 3 \bmod 29 = 9 \bmod 29 = 9$ or -20.

$3^4 \bmod 29 = 3^2 \times 3^2 \bmod 29 = 9 \times 9 \bmod 29 = 81 \bmod 29 = 23$ or -6.

$3^8 \bmod 29 = 3^4 \times 3^4 \bmod 29 = -6 \times -6 \bmod 29 = 36 \bmod 29 = 7$ or -22.

$3^{16} \bmod 29 = 3^8 \times 3^8 \bmod 29 = 7 \times 7 \bmod 29 = 49 \bmod 29 = 20$ or -9.

$3^{32} \bmod 29 = 3^{16} \times 3^{16} \bmod 29 = -9 \times -9 \bmod 29 = 81 \bmod 29 = 23$ or -6.

$3^{64} \bmod 29 = 3^{32} \times 3^{32} \bmod 29 = -6 \times -6 \bmod 29 = 36 \bmod 29 = 7$ or -22.

$3^{100} \bmod 29 = 3^{64} \times 3^{32} \times 3^4 \bmod 29.$

$= 7 \times -6 \times -6 \bmod 29$

$= 252 \bmod 29$

$3^{100} \bmod 29 = 20$