

Modular Arithmetic

a and b are said to be congruent to each other under modulo N , if they leave same remainder when divided by N .

$$a \equiv b \pmod{N}$$

$$13 \equiv 41 \pmod{7}$$

$$13 \bmod 7 = 6$$

$$41 \bmod 7 = 6$$

$$\rightarrow (13 + 35 + 5) \% 7 = (6 + 0 + 5) \% 7 = (11) \% 7 = 4$$

$$(41 + 35 + 5) \% 7 = (6 + 0 + 5) \% 7 = (11) \% 7 = 4$$

$$\rightarrow (13 \times 4) \% 7 = (52) \% 7 = 3$$

$$(41 \times 4) \% 7 = (164) \% 7 = 3$$

$$\rightarrow \text{if } a \equiv b \pmod{N}$$

then

$$a - b \equiv 0 \pmod{N}$$

$a - b$ is divisible by N .

Proof:

$$a = N * K_1 + R$$

$$b = N * K_2 + R$$

$$a - b = N * (K_1 - K_2)$$

Ex: $13 \equiv 41 \pmod{7}$

$$13 - 41 = -28$$

$$41 - 13 = 28$$

$$a - b = N * K$$

$$a = N * K + b$$

↓

K can be +ve or -ve.

$$13 = 7 * (-4) + 41$$

$$41 = 7 * (4) + 13$$

→ If $a * b = c$
then

$$a \pmod{N} * b \pmod{N} \equiv c \pmod{N}$$
$$a \% N * b \% N \equiv c \% N$$

$$13 \equiv 3 \pmod{5} \quad \text{and} \quad 9 \equiv 4 \pmod{5}$$

$$13 * 9 = 117$$

$$(13 \% 5) * (9 \% 5) \equiv (117 \% 5)$$

$$3 * 4 \equiv 2 \pmod{5}$$

$$12 \equiv 2 \pmod{5}$$

If $a * b = c$
then

$$a \pmod{N} * b \pmod{N} \equiv c \pmod{N}$$

$$x_1 * x_2 \equiv x_3$$

$$(N * K_1 + x_1) * (N * K_2 + x_2) = (N * K_3 + x_3)$$

$$N * N * K_1 * K_2 + N * K_1 * x_2 + N * K_2 * x_1 + x_1 * x_2$$

$$= N * K_3 + x_3$$

$$N * N * K_1 * K_2 + N * K_1 * x_2 + N * K_2 * x_1 - N * K_3 = x_3 - (x_1 * x_2)$$

$$N * (N * K_1 * K_2 + K_1 * x_2 + K_2 * x_1 - K_3) = x_3 - (x_1 * x_2)$$

$$x_3 = a * b$$

$$= ((a \% N) * (b \% N)) \% N$$

Q: Find the last digit of $2573 * 34268$?

To find last digit

$$(2573 * 34268) \% 10$$

$$(3 * 8) \% 10$$

$$(24) \% 10 = 4$$

Q: $(142 + 453 + 324 + 781 + 523 + 250 + 313) \% 2 = ?$

$$(0+1+0+1+1+0+1) \% 2$$

$$(4) \% 2 = 0$$

→ Divisibility by 9 and 3:

check whether number 4819250393285 is divisible by 9.

Ex:

$$12345 \% 9 = (1 * 10^4 + 2 * 10^3 + 3 * 10^2 + 4 * 10^1 + 5 * 10^0) \% 9$$

$$= (1 * (9999+1) + 2 * (999+1) + 3 * (99+1) + 4 * (9+1) + 5 * (1)) \% 9$$

$$= (1 * (0+1) + 2 * (0+1) + 3 * (0+1) + 4 * (0+1) + 5 * (0)) \% 9$$

$$= (1+2+3+4+5) \% 9$$

$$= (15) \% 9$$

$$= 6$$

Remainder is not zero so not divisible by 9.

$$(142 + 453 + 324 + 781 + 533 + 250 + 714) \% 3 = ?$$

$$(1+0+0+1+2+1+0) \% 3$$

$$(5) \% 3 = 2$$

Not divisible by 3.

$$(7+3+0+7+2+7+3) \% 9$$

$$= 29 \% 9 = 2$$

Not divisible by 9.

→ Exponentiation in modular arithmetic:

If $a \equiv b \pmod{N}$
then

$$a^K \equiv b^K \pmod{N}$$

If $1b \equiv 1 \pmod{3}$

then

$$16^5 \equiv 1^5 \pmod{3}$$

Proof \rightarrow

$$a = N * p + b$$

$$a^K = (N * p + b)^K$$

$$(A+b)^K = \left[C(K,0) A^K + b^0 \right] + \left[C(K,1) A^{K-1} + b^1 \right] + \dots + \left[C(K,K) A^0 + b^K \right]$$

Q: Find $29^{10} \pmod{3}$.

$$29 \equiv 2 \pmod{3}$$

$$(2^{10}) \% 3 = (1024) \% 3$$

$$(7) \% 3 = 1$$

Q: Find $2^{123456789} \pmod{3}$.

$$123456789 \equiv 0 \pmod{3}$$

$$2^{123456789} = (2^3)^{41152263}$$

$$(8^{41152263}) \% 7$$

$$8 \equiv 1 \pmod{7}$$

$$(1^{41152263}) \% 7 = 1$$