Modular Arithmetic

Wednesday, January 26, 2022 12:44 PM

Recall : gcd

1] Thrm:

$$a \cdot b = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$$

e.g. if a and are coprime, then $\mathrm{lcm}(a,b) = a \cdot b$

2] Euclidean Algorithm

Thrm: $\gcd(a,b) = \gcd(b, a \bmod b)$

e.g. $\gcd(414, 248)$

$$414 = \underline{1} \cdot 248 + \underline{166}$$
$$248 = \underline{1} \cdot 166 + \underline{82}$$
$$166 = \underline{2} \cdot 82 + \underline{2}$$
$$82 = \underline{41} \cdot 2 + \underline{0}$$

gcd

3] Thrm:

① $\gcd(a, 0) = a \quad \forall a \in \mathbb{Z}^+$

② if $\gcd(a,b) = d$, then

(i) $d \mid a$, and $d \mid b$

(ii) $\forall c$, if $c \mid a$ and $c \mid b$, then $c \mid d$

③ $\gcd(0,0) = 0$ by def^n.

4] Extended Euclidean Algorithm

if $a, b \in \mathbb{Z}^+$, then $\exists\, x, y$ s.t. $\gcd(a,b) = xa + yb$

i.e. $\gcd(a,b)$ can be expressed as a linear combination of a and b.

5] e.g. Express the $\gcd(252, 198)$ as linear combination of 252 and 198.

$$252 = \underline{1} \cdot 198 + \underline{54} \quad \text{——— (1)}$$
$$198 = 3 \cdot 54 + 36 \quad \text{——— (2)}$$
$$54 = 1 \cdot 36 + 18 \quad \text{——— (3)}$$
$$36 = 2 \cdot 18 + 0 \quad \text{gcd}$$

From (3) $\quad 18 = 54 - 1 \cdot 36$

From (2) $\quad = 54 - 1(198 - 3 \cdot 54)$

$\quad = -1 \cdot 198 + 4 \cdot 54$

From (1) $\quad = -1 \cdot 198 + 4(252 - 1 \cdot 198)$

$\quad = +4 \cdot 252 - 5 \cdot 198$

$$\therefore x = 4, \quad y = -5$$

6] Modular Arithmetic

Def^n. $a, b, m \in \mathbb{Z}$, $m > 0$

a is congruent to b modulo - m if $m \mid (a - b)$

Notation:

$a \equiv b \pmod{m}$ denotes congruent

$a \not\equiv b \pmod{m}$ " not congruent.

$a \equiv b \pmod{m}$ denotes congruent

$a \not\equiv b \pmod{m}$ " not congruent.

7] Thrm: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

iff $a = b + k \cdot m$ for some k.

8] e.g. $23 \equiv 13 \pmod{5}$

$-2 \equiv 17 \pmod{19}$

9] Thrm: if $a \equiv b \pmod{m}$

and $c \equiv d \pmod{m}$

then

$$a \pm c \equiv b \pm d \pmod{m}$$

$$a \cdot c \equiv b \cdot d \pmod{m}$$

e.g. $137 \cdot 23 \pmod{5}$

$\equiv 2 \cdot 3$

$\equiv 6$

$\equiv 1 \pmod{5}$

e.g. $703525 \times 2140 \pmod{7}$

$\equiv (700000 + 3500 + 21 + 4)(2100 + 42 - 2)$

$\equiv (4)(-2) \equiv 6 \pmod{7}$

10] Exer

(2838 * 34999) mod 7

Sol.

= 3 * (-1) = -3 = 4 (mod 7)