3) if $a = b \pmod N$, $c = d \pmod N$ $\Longrightarrow$ $a+c = b+d \pmod N$

proof: $a-b = k_1 N$, $c-d = k_2 N$ $\Big\} \downarrow +$ $(a+c)-(b+d) = N(k_1-k_2)$

$\Longrightarrow$ $a+c = b+d \pmod N$

e.g: $50 + 148 \overset{24}{\equiv} 2 + 4 \overset{24}{\equiv} 6$

if $a \overset{N}{\equiv} b$, $c \overset{N}{\equiv} d$ $\Big\} \Longrightarrow ac \overset{N}{\equiv} bd$

proof: $a-b = k_1 N$, $c-d = k_2 N$,

$ac - bd = ac - bc + bc - bd$

$= c(a-b) + b(c-d)$

$= c k_1 N + b k_2 N$

$= N(ck_1 + bk_2)$

$\Longrightarrow ac - bd = N(ck_1 + bk_2)$

$\Longrightarrow ac = bd \pmod N$

e.g: $8 \times 16 \times 43 \times 71 \overset{7}{\equiv} 1 \times 2 \times 1 \times 1 = 2$

★ if $a \overset{N}{\equiv} b \Longrightarrow a^k \overset{N}{\equiv} b^k$

e.g: $3^{20} \overset{4}{\equiv} (-1)^{20} \overset{4}{\equiv} 1$

$3^{22} \overset{7}{\equiv} 3 \times 3^{21} \overset{7}{\equiv} 3 \times (3^3)^7 \overset{7}{\equiv} 3 \times (27)^7 \overset{7}{\equiv}$

$3 \times (-1)^7 \overset{7}{\equiv} -3 \overset{7}{\equiv} \boxed{4}$

4) Find the Bézout coefficients of 533 and 195 using Euclidean algorithm:

→ step 1: finding gcd(533, 195)

$$195\overset{2}{\overline{)533}}$$
$$-390$$

$$143\overset{1}{\overline{)195}}$$
$$-143$$

$$52\overset{2}{\overline{)143}}$$
$$-104$$

$$39\overset{1}{\overline{)52}}$$
$$-39$$

$$13\overset{3}{\overline{)39}}$$
$$-39$$
$$0$$

→ $533 = 195 \times 2 + 143$ IV

→ $195 = 143 \times 1 + 52$ III

→ $143 = 52 \times 2 + 39$ II

→ $52 = 39 \times 1 + 13$ I

→ $39 = 13 \times 3 + \underline{\underline{0}}$

$\Longrightarrow \gcd(533, 195) = \boxed{13}$

→ step 2: using substitutions and writing 13 as a linear combination of 195 and 533.

I → $13 = 52 - 39$

II ↓ $13 = 52 - (143 - 2 \times 52) = -1 \times 143 + 3 \times 52$

III ↓ $13 = -1 \times 143 + 3 \times (195 - 143) = 3 \times 195 - 4 \times 143$

IV ↓ $13 = 3 \times 195 - 4 \times (533 - 2 \times 195) = -4 \times 533 + 11 \times 195$

→ $13 = \boxed{-4} \times 533 + \boxed{11} \times 195$ ✓

Scanned by CamScanner