Chinese Remainder Theorem (CRT)

↳ CRT helps us to solve system of linear congruence.

$x \bmod 2 = 1$

$x \equiv 1 \pmod 2$ ← congruency

Ex

$$x \equiv 1 \pmod 2$$
$$x \equiv 5 \pmod 7$$
$$x \equiv 2 \pmod 3$$

} System of linear congruences

Find x → $x = 5$

$5 \bmod 2 = 1$
$5 \bmod 7 = 5$
$5 \bmod 3 = 2$

$x = 47$ →

$47 \bmod 2 = 1$
$47 \bmod 7 = 5$
$47 \bmod 3 = 2$

How can we solve using chinese remainder theorem ?:

Is gives a generalized formula to solve set of linear congruence.

numbers → $[n_1, n_2, n_3 \dots\dots n_k]$
remainders → $[r_1, r_2, r_3, \dots\dots r_k]$

$x \equiv n_1 = r_1$
$x \equiv n_2 = r_2$
$\vdots$
$\vdots$

The value of x which satisfies the system

$$x = \left(\sum_{i=0}^{k-1} (r_i \times z(i) \times inv(i)) \right) \% \text{ product}$$

$$\text{product} \rightarrow \prod_{i=0}^{k-1} n_i$$

$$z(i) = \frac{\text{product}}{n_i}$$

$inv(i)$ = multiplicative modulo inverse of $z(i)$ w.r.t n_i

$z(i) = 4$ $\quad\quad$ $n_i = 7$

$(4 \times \boxed{y}) \bmod 7 = 1$

y → multiplicative modulo inverse of 4 co.r.t 7

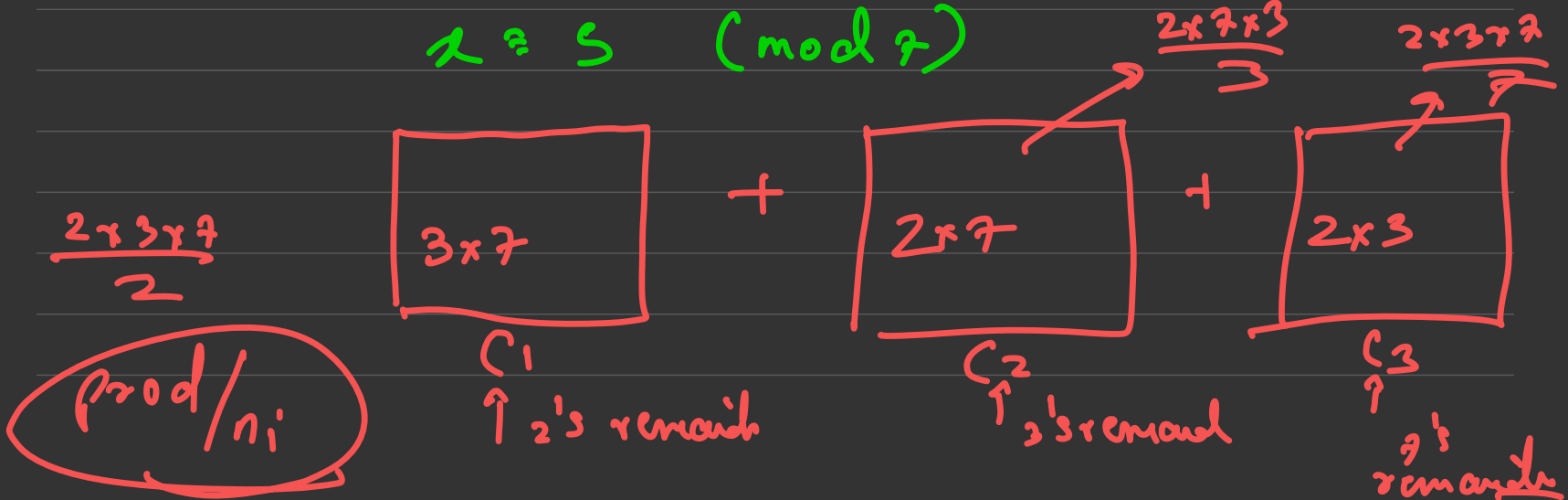
Some intuition proof for CRT

$x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 5 \pmod 7$

Find x



$(6 \times y) \% 7 = 5$

$(6 \times y') \% 7 = 1$

y' → inv module of 6 w.r.t 7

$a^{b^{exp}} \mod p$

$p \to 10^9 + 7$
↳ prime no.

$a, b, n \leq 10^5$

↳ $exp \to {}^nC_0^2 + {}^nC_1^2 + {}^nC_2^2 \dots\dots {}^nC_n^2$

$\to {}^{2n}C_n$

$a^{b^{enc_n}}$ dop

↳ Reduces the problem

assume $b^{enc_n} = y$

a^y d.p

$\phi(p) = p-1$

$$y = kx\,\phi(p) + y\,q_0\,\phi(p)$$

$$\phi(p) = \underline{\underline{p-1}}$$

$$a^{\phi(p)} \equiv_p 1 \quad \text{or} \quad a^{p-1} \equiv_p 1 \Rightarrow \underline{\underline{\text{Fermat's theorem}}}$$

$a^y \mod p$

$\hookrightarrow a^{k\phi(p)} \times a^{y \bmod \phi(p)} \mod p$

$$\left(a^{y \bmod \phi(p)} \mod p\right)$$

$\phi(p) = p-1$

$p = 10^9+7$

$p-1 \rightarrow 10^9+6$

$a^{y\, d_0 (10^9+6)}$ d_0 p

$y\, d_0\, 10^9+6$

b^{2nC_n} $d_0(10^9+6)$

composite number

$b^{2nC_n} \cdot 9 \cdot (10^9+6)$

$b \to$ odd

$b \to$ even

factorise in the form of coprime

$b^{2nC_n} \cdot 9 \cdot (10^9+6)$

$10^9+6 = (2)(5\times10^8+3)$

2 → coprimes

$b^{2^{n}+1}\, d_0(10^9+6) \rightarrow b^{2^{n}+1}\, \phi(10^9+6)\, d_0 10^9+6$

$\phi(10^9+6) = \phi(2) \times \phi(5 \times 10^8+3)$

↳ 1×500000000 ✓

$\phi(10^9+6) = 2 \times 41^2 \times 148271$

$$b^{2nc_n} q_0 (2 \times (5 \times 10^8 + 3))$$

$$\phi(ab) = \phi(a)\phi(b)$$

↳ $b^{2nc_1} q_0 2$

$b^{2nc_n} q_0 (5 \times 10^8 + 3)$

$$b^{2nC_n}\ q_0\ (5\times10^8+3)$$

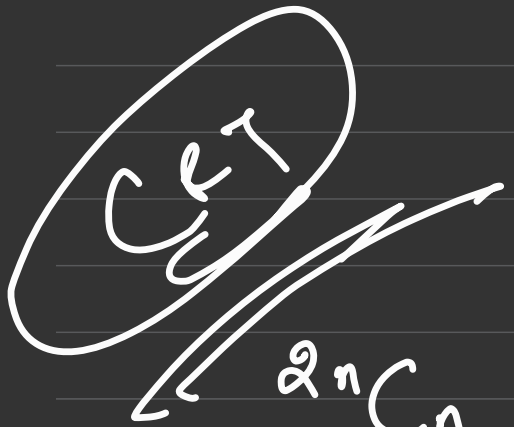
$$\left(b^{2nC_n\ q_0\ (5\times10^8+2)}\right)\ q_0\ (5\times10^8+3)$$

$^{2n}C_n$ q_0 $(5\times10^8+2)$

large Number

not prime

$^{2n}C_n$ $\%$ $(5 \times 10^8 + 2)$



$2 \times 41^2 \times 148721$

$^{2n}C_n \bmod 2 = ?$

$^{2n}C_n \bmod 1681 = ?$

$^{2n}C_n \bmod 148721 = ?$

Remainder

$$^nC_r = \frac{n!}{r!(n-r)!}$$

$$= \frac{(n-r+1)(n-r+2)\cdots}{r!}$$

^nC_r of m

$m = 2$

↳ 16वां

↳ 1248721

$nCr \% m$

$\hookrightarrow \left(\frac{(n-r+1)\%m \times (n-r+2)\%m \cdots}{(r!)} \right) \%m$

$\left(\frac{1}{r!}\right) \%m$

m → composite → Brut force

m → prime

$(r!^{m-2}) \%m \rightarrow$ inv modulo

1 → 4

$m > n$

$$ax_1 + by_1 = m$$

$$ax_2 + by_2 = m+1$$

$$a(x_2 - x_1) + b(y_2 - y_1) = 1$$

$$aX + bY = 1$$

$\gcd(a,b) \mid 1$

$\gcd(a,b) = 1$

-1