Chiness Remainder Theorem

Chinese Remainder Theorem

Given pairwise coprime positive integers $n_1, n_2, \ldots, n_k$ and arbitrary integers $a_1, a_2, \ldots, a_k$, the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution, and the solution is unique modulo $N = n_1 n_2 \cdots n_k$.

A consequence of the CRT is that the equation

$$x \equiv a \pmod{p}$$

is equivalent to the system of equations

$$x \equiv a_1 \pmod{p_1}$$

$$\cdots$$

$$x \equiv a_k \pmod{p_k}$$

(As above, assume that $p = p_1 p_2 \cdots p_k$ and p_i are pairwise relatively prime).

Divide and Conquer Trick

Sum of x^i

$$f(n) = f(\frac{n}{2}) + x^{\frac{n}{2}} \times f(\frac{n}{2}) \qquad \text{for even n}$$

$$f(n) = f(n-1) + x^n \qquad \text{for odd n}$$

Sum of x^i

$$f(x, n) = 1 + x^1 + x^2 + x^3 + ... + x^{n-1}$$

$$f(x, n) = (1 + x) \times f(x^2, \frac{n}{2})$$ for even n

$$f(x, n) = 1 + x \times f(x, n - 1)$$ for odd n

nCr % m