Chinese Remainder Theorem

Dr. Amol Sonawane

Assistant Professor
Department of Mathematics
Government College of Arts and Science
Aurangabad

Chinese Remainder Theorem

Theorem

Let $n_1, n_2, \cdots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

has a simultaneous solution,

Proof of Chinese Remainder Theorem

Proof: Let $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \cdots, r$, let $N_k = \frac{n}{n_k}$.
Since $\gcd(n_i, n_j) = 1$ for $i \neq j$, $\gcd(N_k, n_k) = 1$ for each $k = 1, 2, \cdots, r$.
$\implies$ The linear congruence $N_k x \equiv 1 \pmod{n_k}$ has a unique solution, say x_k.
Let $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$.
Note that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$. ($\because n_k \mid N_i$ for $i \neq k$).
$\implies a_i N_i x_i \equiv 0 \pmod{n_k}$ for $i \neq k$.
$\implies \bar{x} \equiv a_k N_k x_k \pmod{n_k}$ for $k = 1, 2, \cdots, r$.
$\implies \bar{x} \equiv a_k \pmod{n_k}$ for $k = 1, 2, \cdots, r$. ($\because N_k x_k \equiv 1 \pmod{n_k}$.)
$\implies \bar{x}$ is a solution of the given system of linear congruences.
Now we prove that $\bar{x}$ is unique solution of the given system of linear congruences modulo n.

Proof of Chinese Remainder Theorem

Suppose that $\bar{y}$ is also a solution of the given system of linear congruences.

Then $\bar{y} \equiv a_k \pmod{n_k}$ for $k = 1, 2, \cdots, r$.

$\implies \bar{x} \equiv \bar{y} \pmod{n_k}$ for $k = 1, 2, \cdots, r$. ($\because \bar{x} \equiv a_k \pmod{n_k}$)

$\implies n_k \,|\, (\bar{x} - \bar{y})$ for $k = 1, 2, \cdots, r$.

But $\gcd(n_i, n_j) = 1$ for $i \neq j$.

$\implies n_1 n_2 \cdots n_r \,|\, (\bar{x} - \bar{y})$.

$\implies n \,|\, (\bar{x} - \bar{y})$.

$\implies \bar{x} \equiv \bar{y} \pmod{n}$.

Hence the given system of linear congruences has unique simultaneous solution modulo $n = n_1 n_2 \cdots n_r$.

Example

Example

Solve the system of linear congruences:
$x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.

Solution: Let $n = 3 \cdot 5 \cdot 7 = 105$.
Let $N_1 = \frac{n}{3} = 35$, $N_2 = \frac{n}{5} = 21$ and $N_3 = \frac{n}{7} = 15$.
The linear congruences $35x \equiv 1 \pmod{3}$, $21x \equiv 1 \pmod{5}$, $15x \equiv 1 \pmod{7}$ are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectively.
Take $\bar{x} = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 70 + 42 + 45 = 157$.
But $\bar{x} = 157 \equiv 52 \pmod{105}$.
Hence 52 is the required solution of the given system of linear congruences.

Thank You!