Chinese Remainder Theorem

If $n_1, n_2, \ldots, n_k$ are prime numbers then,

for any $1 \leq i \leq k$, n_i and $n_{\bar{i}} = \prod_{j \neq i} n_j$ are relative prime.

Chinese Remainder Theorem

If $n_1, n_2, \ldots, n_k$ are prime numbers then,

for any $1 \leq i \leq k$, n_i and $n_{\bar{i}} = \prod_{j \neq i} n_j$ are relative prime.

That means there exists r_i and s_i such that $r_i * n_i + s_i * n_{\bar{i}} = 1$.

The numbers r_i and s_i can be found using the GCD algorithm.

Chinese Remainder Theorem

If $n_1, n_2, \ldots, n_k$ are prime numbers then,

for any $1 \leq i \leq k$, n_i and $n_{\bar{i}} = \prod_{j \neq i} n_j$ are relative prime.

That means there exists r_i and s_i such that $r_i * n_i + s_i * n_{\bar{i}} = 1$.

The numbers r_i and s_i can be found using the GCD algorithm.

Rewrite the above equation as $s_i * n_{\bar{i}} = 1 \bmod n_i$.

Since $n_{\bar{i}}$ contains all n_j, $j \neq i$, as factors, it is evenly divisible by all but n_i.

Chinese Remainder Theorem

If $n_1, n_2, \ldots, n_k$ are prime numbers then,

for any $1 \leq i \leq k$, n_i and $n_{\bar{i}} = \prod_{j \neq i} n_j$ are relative prime.

That means there exists r_i and s_i such that $r_i * n_i + s_i * n_{\bar{i}} = 1$.

The numbers r_i and s_i can be found using the GCD algorithm.

Rewrite the above equation as $s_i * n_{\bar{i}} = 1 \bmod n_i$.

Since $n_{\bar{i}}$ contains all n_j, $j \neq i$, as factors, it is evenly divisible by all but n_i.

Then $s_i * n_{\bar{i}} = 0 \bmod n_j, j \neq i$ and we can find x given a system of equations

$$\begin{aligned} x \bmod n_1 &= a_1 \\ x \bmod n_2 &= a_2 \\ &\ldots \\ x \bmod n_k &= a_k \end{aligned}$$

Chinese Remainder Theorem

If $n_1, n_2, \ldots, n_k$ are prime numbers then,

for any $1 \leq i \leq k$, n_i and $n_{\bar{i}} = \prod_{j \neq i} n_j$ are relative prime.

That means there exists r_i and s_i such that $r_i * n_i + s_i * n_{\bar{i}} = 1$.

The numbers r_i and s_i can be found using the GCD algorithm.

Rewrite the above equation as $s_i * n_{\bar{i}} = 1 \bmod n_i$.

Since $n_{\bar{i}}$ contains all n_j, $j \neq i$, as factors, it is evenly divisible by all but n_i.

Then $s_i * n_{\bar{i}} = 0 \bmod n_j, j \neq i$ and we can find x given a system of equations

$$\begin{aligned} x \bmod n_1 &= a_1 \\ x \bmod n_2 &= a_2 \\ &\ldots \\ x \bmod n_k &= a_k \end{aligned}$$

as follows:

$$x = \sum_{i=1}^{k} a_i * s_i * n_{\bar{i}} \bmod n_1 * n_2 * \ldots * n_k$$

Since

$$\begin{aligned} &x \bmod n_1 = a_1 * 1 \bmod n_1 + a_2 * 0 + a_3 * 0 + \ldots + a_k * 0 = a_1 \\ &x \bmod n_2 = a_1 * 0 + a_2 * 1 \bmod n_2 + a_3 * 0 + \ldots + a_k * 0 = a_2 \\ &\ldots \\ &x \bmod n_k = a_1 * 0 + a_2 * 0 + a_3 * 0 + \ldots + a_k * 1 \bmod n_k = a_k \end{aligned}$$