Chinese Remainder Theorem

Chinese Remainder Theorem (first stated by the Chinese mathematician Sunzi):

Let $n_1, \ldots, n_k$ be natural numbers such that any pair of these numbers are relatively prime (i.e $\forall i \in [k] \, \forall j \in [k] \setminus \{i\} \, (\gcd(n_i, n_j) = 1)$. Let $N = \prod_{j=1}^{k} n_j$.
For any integers $a_1, \ldots, a_k$ there is a unique integer $x \in \{0, 1, \ldots, N-1\}$ such that $\forall j \in [k] \, (x \equiv a_j \bmod n_j)$

Example: If $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, $a_1 = 2$, $a_2 = 3$, and $a_3 = 4$, the Chinese Remainder Theorem says that there is a unique $x \in \{0, 1, \ldots, 104\}$ such that $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, and $x \equiv 4 \bmod 7$.

Here $x = 53$ as $53 \equiv 2 \bmod 3$, $53 \equiv 3 \bmod 5$, and $53 \equiv 4 \bmod 7$.

Proof of the Chinese Remainder Theorem

$n_1, \ldots, n_k \in \mathbb{N}$ and $\forall i \in [k] \forall j \in [k] \setminus \{i\} (\gcd(n_i, n_j) = 1)$.

$N = \prod_{j=1}^{k} n_j$. Goal: Given $a_1, \ldots, a_k \in \mathbb{Z}$, show that there is a unique $x \in \{0, 1, \ldots, N-1\}$ such that $\forall j \in [k] (x \equiv a_j \bmod n_j)$.

Fact: $\forall j \in [k] \left(\gcd\left(n_j, \frac{N}{n_j}\right) = 1\right)$.

For each j, let $c_j = \left(\frac{N}{n_j}\right)^{-1}$ in $\mathbb{Z}_{n_j}$ and take $e_j = c_j \left(\frac{N}{n_j}\right)$.

Claim: $e_j \equiv 1 \bmod n_j$ and $\forall j' \in [k] \setminus \{j\} (e_j \equiv 0 \bmod n_{j'})$.

Proof: In $\mathbb{Z}_{n_j}$, $e_j = c_j\left(\frac{N}{n_j}\right) = \left(\frac{N}{n_j}\right)^{-1}\left(\frac{N}{n_j}\right) = 1$ so $e_j \equiv 1 \bmod n_j$.

$\forall j' \in [k] \setminus \{j\}$, $n_{j'} \mid \frac{N}{n_j}$ and $\frac{N}{n_j} \mid e_j$ so $n_{j'} \mid e_j$ and thus $e_j \equiv 0 \bmod n_{j'}$.

Taking $x = \left(\sum_{j=1}^{k} a_j e_j\right) \bmod N$, $\forall j \in [k] (x \equiv a_j \bmod n_j)$.

To show that x is unique, assume $x, x' \in \{0, 1, \ldots, N-1\}$ and $\forall j \in [k] (x' \equiv x \equiv a_j \bmod n_j)$

Then $\forall j \in [k] (n_j \mid (x' - x))$. Fact: Since any pair of $n_1, \ldots, n_k$ are relatively prime, for any integer m, $(\forall j \in [n] (n_j \mid m) \leftrightarrow N \mid m)$ (i.e. $N = \operatorname{lcm}(n_1, \ldots, n_k)$).

Thus, $N \mid (x' - x)$ so $x' = x$.

Finding x

$x = \left(\sum_{j=1}^{k} a_j e_j\right) \bmod N$ where $e_j = c_j\left(\frac{N}{n_j}\right)$ and $c_j = \left(\frac{N}{n_j}\right)^{-1}$ in $\mathbb{Z}_{n_j}$.

Example: If $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, $a_1 = 2$, $a_2 = 3$, and $a_3 = 4$ then
$c_1 = 35^{-1}$ in $\mathbb{Z}_3$. $35 \equiv 2 \bmod 3$ and $2^{-1} = 2$ in $\mathbb{Z}_3$ so $c_1 = 2$.
$e_1 = 2 \cdot 35 = 70$. Note that $e_1 \equiv 1 \bmod 3$, $e_1 \equiv 0 \bmod 5$, and $e_1 \equiv 0 \bmod 7$.
$c_2 = 21^{-1}$ in $\mathbb{Z}_5$. $21 \equiv 1 \bmod 5$ and $1^{-1} = 1$ in $\mathbb{Z}_5$ so $c_2 = 1$.
$e_2 = 1 \cdot 21 = 21$. Note that $e_2 \equiv 0 \bmod 3$, $e_2 \equiv 1 \bmod 5$, and $e_2 \equiv 0 \bmod 7$.
$c_3 = 15^{-1}$ in $\mathbb{Z}_7$. $15 \equiv 1 \bmod 7$ and $1^{-1} = 1$ in $\mathbb{Z}_7$ so $c_3 = 1$.
$e_3 = 1 \cdot 15 = 15$. Note that $e_3 \equiv 0 \bmod 3$, $e_3 \equiv 0 \bmod 5$, and $e_3 \equiv 1 \bmod 7$.
Putting everything together,

$$x = (2 \cdot 70 + 3 \cdot 21 + 4 \cdot 15) \bmod 105 = 263 \bmod 105 = 53$$

Key idea: For each j, find a multiple of $\frac{N}{n_j}$ which is congruent to a_j modulo n_j and then add these multiples together modulo N.