Chinese Remainder Theorem (CRT)

Theorem 1. If $n_1, n_2, \ldots, n_k$ are pairwise co-prime integers and if $a_1, a_2, \ldots, a_k$ are any integers such that $0 \leqslant a_i < n_i$ for every $i = 1, 2, \ldots, k$, then the system of congruence equations

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{1}$$

has a unqiue solution $0 \leqslant x < N$, where $N = \prod_{i=1}^{k} n_k$, such that $x \bmod n_i = a_i$ for every $i = 1, 2, \ldots, k$.

Proof. Suppose that x and y are both solutions to (1). Then

$$\forall i = 1, 2, \ldots, k : x \bmod n_i = y \bmod n_i = a_i \implies n_i | x - y \ .$$

Since all n_i are pairwise co-prime, their product N also divides $x - y$, and hence $x \equiv y \pmod{N}$. Considering that x and y are nonnegative and less than N, the statement $N | x - y$ is true only if $x = y$. Hence, the solution to the system (1) is unique. $\square$

Theorem 2. A mappping $\varphi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ defined by

$$\varphi : a \bmod N \mapsto (a \bmod n_1, \ldots a \bmod n_k)$$

is a ring-isomorphism.

Proof. First, we show that φ is bijective. Define an inverse mapping $\varphi^{-1} = \psi$ as

$$\psi : \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$$

by

$$\psi : (a \bmod n_1, \ldots, a \bmod n_k) \mapsto a \bmod N \ .$$

Then for all $(a \bmod n_1, \ldots, a \bmod n_k) \in \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ and for all $b \bmod N \in \mathbb{Z}/N\mathbb{Z}$:

$$\begin{aligned} &(\varphi \circ \psi)(a \bmod n_1, \ldots, a \bmod n_k) = \varphi(a \bmod N) = (a \bmod n_1, \ldots, a \bmod n_k) \ , \\ &(\psi \circ \varphi)(b) = \psi(b \bmod n_1, \ldots, b \bmod n_k) = b \bmod N \ . \end{aligned}$$

Hence, $\varphi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ is a bijection.

Next, we show that φ is an isomorphism (i.e., preserves operations). For all $a \bmod N, b \bmod N \in \mathbb{Z}/N\mathbb{Z}$ it must hold that

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b) \ , \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \ . \end{aligned}$$

Observe that

$$\begin{aligned}
\varphi(a \bmod N + b \bmod N) &= \varphi(a + b \bmod N) = (a + b \bmod n_1, \dots, a + b \bmod n_k) \\
&= (a \bmod n_1, \dots, a \bmod n_k) + (b \bmod n_1, \dots, b \bmod n_k) \\
&= \varphi(a \bmod N) + \varphi(b \bmod N) \ , \\
\varphi(a \bmod N \cdot b \bmod N) &= \varphi(ab \bmod N) = (ab \bmod n_1, \dots, ab \bmod n_k) \\
&= (a \bmod n_1, \dots a \bmod n_k) \cdot (b \bmod n_1, \dots, b \bmod n_k) \\
&= \varphi(a \bmod N) \cdot \varphi(b \bmod N) \ .
\end{aligned}$$

Hence, $\varphi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ is a ring-isomorphism, and therefore

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \ .$$

□

Corollary 1. $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. In other words, computing in $\mathbb{Z}_{pq}$ is the same as computing in $\mathbb{Z}_p \times \mathbb{Z}_q$.

Theorem 3. Let n_1, n_2 be co-prime integers and let a_1, a_2 be any integers such that $a_1 < n_1$ and $0 \leqslant a_2 < n_2$. Then the solution to the system of congruence equations

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

is

$$x \equiv a_1 m_2 n_2 + a_2 m_1 n_1 \ ,$$

where m_1 and m_2 are the coefficients of the Bézout identity $m_1 n_1 + m_2 n_2 = 1 = \gcd(n_1, n_2)$.

Proof. Indeed, considering that by the Bézout identity $m_2 n_2 = 1 - m_1 n_1$,

$$\begin{aligned}
x &= a_1 m_2 n_2 + a_2 m_1 n_1 = a_1(1 - m_1 n_1) + a_2 m_1 n_1 \\
&= a_1 + (a_2 - a_1) m_1 n_1 \implies x \equiv a_1 \pmod{n_1} \ .
\end{aligned}$$

Similarly, by the Bézout identity, $m_1 n_1 = 1 - m_2 n_2$, and hence

$$\begin{aligned}
x &= a_1 m_2 n_2 + a_2 m_1 n_1 = a_1 m_2 n_2 + a_2(1 - m_2 n_2) \\
&= a_2 + (a_1 - a_2) m_2 n_2 \implies x \equiv a_2 \pmod{n_2} \ .
\end{aligned}$$

□

Theorem 4. Let $n_1, n_2, \dots, n_k$ be pairwise co-prime integers and let $a_1, a_2, \dots, a_k$ be any integers such that $0 \leqslant a_i < n_i$ for all $i = 1, 2, \dots, k$, and let $N = n_1 \cdot n_2 \cdot n_k$. Then the solution of the system of congruence equations

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

is

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{N} \ ,$$

where $N_i = \frac{N}{n_i}$ and M_i is the Bézout coefficient satisfying $M_i N_i + m_i n_i = 1 = \gcd(N_i, n_i)$.

Proof. As N_j is a multiple of n_i for $i \neq j$, it holds that

$$\begin{aligned} x = \sum_{i=1}^{k} a_i M_i N_i = & \underbrace{a_1 M_1 N_1}_{\equiv 0 \pmod{n_i}} + \ldots + a_i M_i N_i + \ldots + \underbrace{a_k M_k N_k}_{\equiv 0 \pmod{n}_i} \\ \equiv & \ a_i M_i N_i \pmod{n_i} \ . \end{aligned}$$

Since $gcd(N_i, n_i) = 1$, the Bézout identity $M_i N_i + m_i n_i = 1$ applies, and hence $M_i N_i = 1 - m_i n_i$. And so

$$x \equiv a_i M_i N_i \pmod{n_i} \equiv a_i(1 - m_i n_i) \pmod{n_i} \equiv a_i \pmod{n_i} \ .$$

$\square$