The Chinese Remainder Theorem

**Theorem 6:** Suppose that \( m_1, m_2, \ldots, m_r \) are positive integers such that
\[
\gcd(m_i, m_j) = 1, \quad \text{for all } i < j.
\]
Put
\[
m = m_1 m_2 \cdots m_r,
\]
\[
m'_i = \frac{m}{m_i}, \quad 1 \leq i \leq r,
\]
\[
e_i = m'_i m_i^*, \quad 1 \leq i \leq r,
\]
where \( m_i^* \) is chosen such that
\[
m'_i m_i^* \equiv 1 \pmod{m_i}, \quad 1 \leq i \leq r.
\]
If \( x, a_1, \ldots, a_r \in \mathbb{Z} \), then the simultaneous congruences
\[
\begin{align*}
x & \equiv a_1 \pmod{m_1} \\
x & \equiv a_2 \pmod{m_2} \\
\vdots & \vdots \\
x & \equiv a_r \pmod{m_r}
\end{align*}
\]
hold if and only if
\[
x \equiv a_1 e_1 + \ldots + a_r e_r \pmod{m}.
\]
**Note:** By construction we have
\[
e_i \equiv \delta_{ij} \pmod{m_j}, \quad \text{for all } i, j.
\]
Example: We have a certain number of things. If we count them by 3’s, we have 2 left over. If we count them by 5’s, we have 3 left over. If we count them by 7’s, we have 2 left over. How many things do we have?

Solution: If $x$ denotes the number of things in question, then

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}.$$

We apply CRT with $m_1 = 3, m_2 = 5, m_3 = 7$. Since these are distinct primes, the gcd-condition is clearly satisfied. Moreover, $m = 3 \cdot 5 \cdot 7 = 105$ and

$$m'_1 = \frac{3 \cdot 5 \cdot 7}{3} = 35, \quad m'_2 = \frac{3 \cdot 5 \cdot 7}{5} = 21, \quad m'_3 = \frac{3 \cdot 5 \cdot 7}{7} = 15.$$ 

To find the $m_i^*$’s, we solve

$$m'_1 m_1^* \equiv 2 m_1^* \equiv 1 \pmod{3} \Rightarrow m_1^* \equiv 2 \pmod{3}$$
$$m'_2 m_2^* \equiv m_2^* \equiv 1 \pmod{5} \Rightarrow m_2^* \equiv 1 \pmod{5}$$
$$m'_3 m_3^* \equiv m_3^* \equiv 1 \pmod{7} \Rightarrow m_3^* \equiv 1 \pmod{7}$$

Thus: $e_1 = m'_1 m_1^* = 35 \cdot 2 = 70, e_2 = 21 \cdot 1 = 21, e_3 = 15$ and so by applying the formula we obtain

$$x \equiv a_1 e_1 + a_2 e_2 + a_3 e_3 \pmod{m}$$
$$\equiv 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 \pmod{105}$$
$$\equiv 35 + 63 + 30 \equiv 128 \equiv 23 \pmod{105}.$$ 

Thus, $x \equiv 23 \pmod{105}$, and so the smallest number of things we can have is 23.

---

1 See Master Sun Tzu’s Arithmetical Manual, written 273–473 A.D.
Remark: The Chinese Remainder Theorem is an easy consequence of the following form of Euclid’s Lemma.

Euclid’s Lemma: If \( m = m_1 \cdots m_r \), and if
\[
\gcd(m_i, m_j) = 1, \quad \text{for all } i \neq j,
\]
then for any \( c \in \mathbb{Z} \) we have that
\[
m_1 \mid c, \; m_2 \mid c, \; \ldots, \; m_r \mid c \quad \iff \quad m \mid c.
\]

Theorem 6* (CRT): If \( m = m_1 \cdots m_r \), where the \( m_i \)'s satisfy (1), then the map
\[
\varphi(x \mod m) = (x \mod m_1, \ldots, x \mod m_r)
\]
defines an isomorphism of rings
\[
\varphi : \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}.
\]

In particular, we obtain an isomorphism of groups:
\[
(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^\times.
\]

Remark: Note that Theorem 6 gives us a formula for computing the inverse map \( \varphi^{-1} \) of \( \varphi \).

Corollary: If \( m_1, \ldots, m_r \) satisfy (1), then
\[
\phi(m_1 \cdots m_r) = \phi(m_1) \cdots \phi(m_r).
\]
Thus \( \phi(m) = m \prod_{p|m} \left( 1 - \frac{1}{p} \right) \).