

The Chinese Remainder Theorem

Theorem 5: Suppose that m_1, m_2, \dots, m_r are positive integers such that

$$\gcd(m_i, m_j) = 1, \quad \text{for all } i < j.$$

Put

$$m = m_1 m_2 \cdots m_r,$$

$$m'_i = \frac{m}{m_i}, \quad 1 \leq i \leq r,$$

and choose integers m_i^* such that

$$m'_i m_i^* \equiv 1 \pmod{m_i}, \quad 1 \leq i \leq r.$$

Then for integers x, a_1, \dots, a_r , the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots \quad \quad \quad \vdots$$

$$x \equiv a_r \pmod{m_r}$$

hold if and only if

$$x \equiv a_1 m_1^* m'_1 + \dots + a_r m_r^* m'_r \pmod{m}.$$

Note: This method is explained in Master Sun Tzu's *Arithmetical Manual* (written between 273 - 473 A.D.) It is one of the earliest preserved Chinese textbooks on Arithmetic.