Chinese remainder theorem

Theorem (Chinese remainder theorem)

Suppose that $\gcd(m, n) = 1$*. Then for any* $a, b \in Z$ *there is a unique* x *mod* mn *such that* $x \equiv a \mod m$ *and* $x \equiv b \mod n$*.*

In fact, if $m_i \in Z$ *for* $i = 1, \ldots, n$ *and* $\gcd(m_i, m_j) = 1$ *for* $i \neq j$ *then for any* $a_i \in Z$ *for* $i = 1, \ldots, n$ *there is a unique* x *mod* $m_1 m_2 \ldots m_n$ *such that* $x \equiv a_i \mod m_i$ *for all* i*.*

Fermat's little theorem

Theorem (Fermat's little theorem)

Suppose that p is prime and p does not divide a. Then

$$a^{p-1} \equiv 1 \mod p.$$

- Define the Euler ϕ-function on the set of positive integers by

$$\phi(n) = \text{ the number of } k, 0 < k < n \text{ such that } \gcd(k, n) = 1.$$

Theorem (Euler's theorem)

Suppose $n > 0$ and $\gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n.$$

Calculation of the ϕ-function

Lemma

For p a prime, $\phi(p^n) = p^{n-1}(p-1)$.

Lemma

Suppose that $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

Theorem

If $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ then

$$\phi(n) = p_1^{m_1-1} p_2^{m_2-1} \cdots p_k^{m_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).$$

Corollary

If p and q are distinct primes then $\phi(pq) = (p-1)(q-1)$.