Solving Congruences

Theorem 1 (Modular Inverses)**.** *Let n be a positive integer, and a an integer. Then the congruence $ax \equiv 1 \mod n$ has a solution x if and only if $\mathsf{gcd}(a, n) = 1$. In this case, the solution x is unique mod n.*

Proof. First suppose $\mathsf{gcd}(a, n) = 1$. By Bezout's Identity, we have $au + nv = 1$ for some integers u and v. In particular, $n|(au - 1)$, so that $au \equiv 1 \mod n$ as needed. Conversely, suppose $ax \equiv 1 \mod n$ has a solution u. By definition we have that n divides $au - 1$, so that $1 = au + nv$ for some integer v. Now let $d = \mathsf{gcd}(a, n)$, with $a = da'$ and $n = dn'$. Then $1 = d(a'u + n'v)$, so that $d = 1$ as claimed.

Finally, suppose we have two solutions of this equation, u_1 and u_2. Note that $au_1 \equiv au_2 \mod n$, so that n divides $au_1 - au_2 = a(u_1 - u_2)$. Since $\mathsf{gcd}(a, n) = 1$ we have $n|(u_1 - u_2)$ by Euclid's Lemma, so that $u_1 \equiv u_2 \mod n$ as claimed. □

Corollary 2. *Let $p > 1$ be a prime. If $ab \equiv 0 \mod p$, then either $a \equiv 0 \mod p$ or $b \equiv 0 \mod p$.*

Corollary 3. *Let p be a prime. If $a \in [1, p)$, then there is a unique $b \in [1, p)$ such that $ab \equiv 1 \mod p$. Moreover, a and b are distinct unless $a = 1$ or $a = p - 1$.*

Proof. The existence and uniqueness of b follows from the previous result. Now suppose $a = b$; that is, $a^2 \equiv 1 \mod p$. Then $(a - 1)(a + 1) \equiv 0 \mod p$. Since p is prime, we must have either $a - 1 \equiv 0 \mod p$ or $a + 1 \equiv 0 \mod p$; in the first case, $a = 1$, and in the second case, $a = p - 1$. □

Corollary 4 (Wilson's Theorem)**.** *Let $n > 2$ be an integer. Then n is prime if and only if $(p - 1)! \equiv -1 \mod p$.*

Proof. Suppose $n = p$ is prime, and consider the residues

$$1, 2, 3, \ldots, p - 2, p - 1.$$

All such residues *except* 1 and $p - 1$ come in inverse pairs. So after rearranging, we have

$$(p - 1)! = 1 \cdot (p - 1) \cdot (t_1 \cdot u_1) \cdot \cdots \cdot (t_k \cdot u_k),$$

where $t_i \cdot u_i \equiv 1 \mod p$. Thus $(p - 1)! \equiv p - 1 \equiv -1 \mod p$ as claimed.

Conversely, suppose n is not prime; then we have $1 < a < n$ and $1 < b < n$ such that $n = ab$. But now a and b both appear among the factors of $(n - 1)!$, so that $(n - 1)! \equiv 0 \mod n$. □

Theorem 5 (Simultaneous Linear Congruences)**.** *Let a and b be relatively prime positive integers. Then for any integers u and v, the system of congruences*

$$\begin{cases} x \equiv u \mod a \\ x \equiv v \mod b \end{cases}$$

has a unique solution mod n.

Proof. First we show existence. Since $\mathsf{gcd}(a, b) = 1$, by Bezout's Identity there exist integers h and k such that $1 = ah + bk$. Multiplying by $v - u$, we have

$$v - u = ah(v - u) + bk(v - u),$$

and rearranging, we let

$$t = u + ah(v - u) = v - bk(v - u).$$

Clearly $t \equiv u \mod a$ and $t \equiv v \mod b$.

Next we show uniqueness. To this end, suppose t and s are both solutions of this system. In particular, we have $t \equiv u \mod a$ and $t \equiv u \mod b$. Say $q_1 a = u - t = q_2 b$. Now a divides $q_2 b$, and since a and b are relatively prime, by Euclid's Lemma we have $a | q_2$. Thus $u - t = q_2' ab$, so that $t \equiv u \mod ab$ as needed. $\square$