Elementary Number Theory: The Theory of Congruences

Arjun Vardhan

†

Created: 8th April 2022
Last updated: 5th July 2022

1 Basic Properties of Congruence

- Let $n \in \mathbb{N}$. $a, b \in \mathbb{Z}$ are said to be congruent modulo n, denoted $a \equiv b \mod n$, if $n \mid (a-b)$.
- **Let $a, b \in \mathbb{Z}$. $a \equiv b \mod n$ if and only if a and b leave the same non-negative remainder on division by n.** *Proof:* Let $a = b + kn$ for some $k \in \mathbb{Z}$. By the division algorithm, $b = qn + r$, where $0 \leq r < n$. Thus $a = (k+q)n + r$. Conversely, suppose $a = q_1 n + r$ and $b = q_2 n + r$, where $0 \leq r < n$. Then $a - b = (q_1 - q_2)n$ and thus $n \mid (a-b) \implies a \equiv b \mod n$. ■
- **Let $n > 1$ be fixed and $a, b, c, d \in \mathbb{Z}$. Then:**
  1. $a \equiv a \mod n$. *Proof:* $n \mid 0 = a - a$. ■
  2. **If $a \equiv b \mod n$, then $b \equiv a \mod n$.** *Proof:* $n \mid a - b \implies a - b = kn \implies b - a = -kn \implies b \equiv a \mod n$. ■
  3. **If $a \equiv b \mod n$, and $b \equiv c \mod n$, then $a \equiv c \mod n$.** *Proof:* $a = b + k_1 n$ and $b = c + k_2 n \implies a = c + (k_1 + k_2)n \implies n \mid a - c \implies a \equiv c \mod n$. ■
  4. **If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.** *Proof:* $a = b + k_1 n$ and $c = d + k_2 n \implies a + c = b + d + (k_1 + k_2)n \implies n \mid (a+c) - (b+d) \implies a + c \equiv b + d \mod n$. Also, $ac = (b + k_1 n)(d + k_2 n) = bd + bk_2 n + dk_1 n + k_1 k_2 n^2$. Therefore, $n \mid ac - bd \implies ac \equiv bd \mod n$. ■
  5. **If $a \equiv b \mod n$, then $a + c \equiv b + c \mod n$ and $ac \equiv bc \mod n$.** *Proof:* $a = b + kn \implies a + c = b + c + kn \implies n \mid (a+c) - (b+c) \implies a + c \equiv b + c \mod n$. Additionally, $ac = bc + kcn \implies n \mid ac - bc \implies ac \equiv bc \mod n$. ■
  6. **If $a \equiv b \mod n$, then $a^k \equiv b^k \mod n$ for any positive integer k.** *Proof:* $a^k - b^k = (a-b)(a^{n-1} + a^{n-2}b + ...)$. Since $n \mid a - b$, $n \mid a^k - b^k \implies a^k \equiv b^k \mod n$. ■
- **If $ca \equiv cb \mod n$, then $a \equiv b \mod \frac{n}{d}$, where $d = \gcd(c, n)$.** *Proof:* $ca - cb = kn$. Since $\gcd(c, n) = d$, there exist relatively prime integers r, s such that $c = dr$ and $n = ds$. Then, $r(a-b) = ks$. As $s \mid r(a-b)$ and $\gcd(r, s) = 1$, by euclid's lemma $s \mid a - b$. So $a \equiv b \mod \frac{n}{d}$, as $s = \frac{n}{d}$. ■
- **Corollary: If $ca \equiv cb \mod n$ and $\gcd(c, n) = 1$, then $a \equiv b \mod n$.**
- **Corollary: If $ca \equiv cb \mod p$, where p is prime and $p \nmid c$, then $a \equiv b \mod n$.** *Proof:* p being prime and $p \nmid c$ implies $\gcd(p, c) = 1$. ■

2 Binary and Decimal Representations of Integers

-

3 Linear Congruences and the Chinese Remainder Theorem

- An equation of the form $ax \equiv b \mod n$ is called a linear congruence. A solution to this would an integer x_0 such that $ax_0 \equiv b \mod n$.

- Two solutions of $ax \equiv b \mod n$, say x_1 and x_2, are treated as equal if $x_1 \equiv x_2 \mod n$. Thus we want to find all possible incongruent integers satisfying a linear congruence.

- The linear congruence $ax \equiv b \mod n$ is equivalent to the diophantine equation $ax - ny = b$ (they have the same solutions).

- **The linear congruence $ax \equiv b \mod n$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. In such a case, it has d mutually incongruent solutions.** *Proof:* This congruence is equivalent to the diophantine equation $ax - ny = b$, which has a solution if and only if $d \mid b$. Moreover, if x_0, y_0 is a specific solution, then every other solution is of the form $x_0 + \frac{n}{d}t$, $y_0 + \frac{n}{d}t$. Suppose x_0 is a solution and consider $x_0 + \frac{n}{d}t$ when $t = 0, 1, 2..., d-1$. We need to show that all of these are incongruent modulo n and that any integer satisfying the congruence is congruent to one of them. Suppose $x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \mod n$, where $0 \leq t_1 < t_2 \leq d-1$. Then $\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \mod n$ and since $\gcd(\frac{n}{d}, n) = \frac{n}{d}$, we have $t_1 \equiv t_2 \mod d$. Thus $d \mid t_2 - t_1$, but this is impossible as $t_2 - t_1 < d$. Now let $x_0 + \frac{n}{d}t$ be an arbitrary solution to the congruence. By the division algorithm, $t = qd + r$, where $0 \leq r \leq d - 1$. So $x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}qd + \frac{n}{d}r = x_0 + qn + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r \mod n$. ■

- **Corollary: If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \mod n$ has a unique solution.**

- Consider a system of linear congruences: $a_1x \equiv b_1 \mod m_1$, $a_2x \equiv b_2 \mod m_2$,..., $a_rx \equiv b_r \mod m_r$, where the moduli m_i are pairwise relatively prime. The system will obviously have no solution unless each congruence is individually solvable, so $d_k \mid b_k$ for each k, where $d_k = \gcd(a_k, m_k)$. The factor d_k can be cancelled from the kth congruence to produce a new, simpler system of congruences with the same solutions: $a_1'x \equiv b_1' \mod n_1$, $a_2'x \equiv b_2' \mod n_2$,...,$a_r'x \equiv b_r' \mod n_r$, where $n_k = \frac{m_k}{d_k}$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Also, $\gcd(a_k', n_k) = 1$ for all k.

- **Chinese Remainder Theorem: Let $n_1, n_2, .., n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences $x \equiv a_1 \mod n_1$, $x \equiv a_2 \mod n_2$,.., $x \equiv a_r \mod n_r$ has a unique solution modulo the integer $n_1n_2...n_r$.** *Proof:* Let $n = n_1n_2...n_r$. For each $k = 1, 2, ..., r$, let $N_k = \frac{n}{n_k} = n_1...n_{k-1}n_{k+1}...n_r$. As n_i are relatively prime pairwise, $\gcd(N_k, n_k) = 1$. Thus it is possible to solve $N_kx \equiv 1 \mod n_k$; let the unique solution be x_k. Let $\overline{x} = a_1N_1x_1 + a_2N_2x_2 + ... + a_rN_rx_r$. As $n_k \mid N_i$ for $i \neq k$, $N_i \equiv 0 \mod n_k$ and so $a_iN_ix_i \equiv 0 \mod n_k$. Thus $\overline{x} \equiv a_kN_kx_k \mod n_k$. But as $N_kx_k \equiv 1 \mod n_k$, we have $\overline{x} \equiv a_k \mod n_k$. Thus $\overline{x}$ is a simulatenous solution to the system of congruences. Now suppose x' is any other solution to the system. Then $\overline{x} \equiv a_k \equiv x' \mod n_k$ for $k = 1, 2, ..., r$. So $n_k \mid \overline{x} - x'$ for each k. Because $\gcd(n_i, n_j) = 1$, $n_1n_2...n_r \mid \overline{x} - x'$, thus $x' \equiv \overline{x} \mod n$. ■

- **The system of linear congruences $ax + by \equiv r \mod n$, $cx + dy \equiv s \mod n$ has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.** *Proof:*