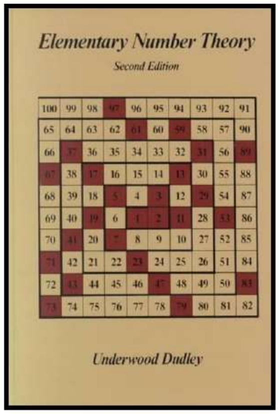
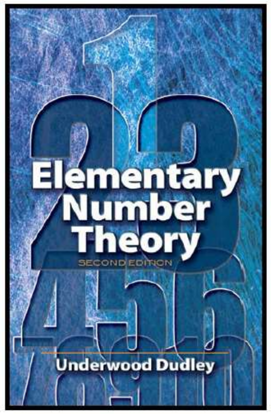
Elementary Number Theory

Section 5. Linear Congruences—Proofs of Theorems





Lemma 5.1

Lemma 5.1. If $(a, m) \nmid b$ then $ax \equiv b \pmod{m}$ has no solutions.

Proof. The contrapositive of the claim is: "If $ax \equiv b \pmod{m}$ has a solution then $(a, m) \mid b$. Let r be a solution." Then $ar \equiv b \pmod{m}$ so that (by the definition of "congruence") $m \mid (ar - b)$ or (by the definition of "divides") $ar - b = km$ for some $k \in \mathbb{Z}$.

Since $(a, m) \mid ar$ (because $(a, m) \mid a$) and $(a, m) \mid km$ (because $(a, m) \mid m$) then Lemma 1.2 $(a, m) \mid (ar - km)$. That is, $(a, m) \mid b$. So the contrapositive holds, and hence the original claim holds. □

Lemma 5.2

Lemma 5.2. If $(a, m) = 1$ then $ax \equiv b \pmod{m}$ has exactly one solution.

Proof. Since $(a, m) = 1$ by hypothesis, then by Theorem 1.4 there are integers r and s such that $ar + ms = 1 = (a, m)$. Therefore $n(ar + ms) = b(1)$ or $a(rb) + m(sb) = b$. So $arb - b = -msb$ and $arb - b$ is a multiple of m, or $a(rb) \equiv b \pmod{m}$. Then the least residue of rb modulo m is a solution of $ax \equiv b \pmod{m}$, as claimed.

Next, we need to show that is only one solution. ASSUME that both r and s are solutions to $ax \equiv b \pmod{m}$. Then $ar \equiv b \pmod{m}$ and $as \equiv b \pmod{m}$ and hence $ar \equiv as \pmod{m}$. So by Theorem 4.4 we can cancel the common factor a to get $r \equiv s \pmod{m}$. Then, by the definition of congruence, $m \mid (r - s)$. But r and s are least residues modulo m (by the definition of "solution"), so $0 \le r < m$ and $0 \le s < m$. Thus $-m < r - s < m$, along with the fact that $m \mid (r - s)$, implies that $r - s = 0$ or $r = s$. Therefore, the solution is unique, as claimed. □

Lemma 5.3

Lemma 5.3. Let $d = (a, m)$. If $d \mid b$ then $ax \equiv b \pmod{m}$ has exactly d solutions.

Proof. The linear congruence $ax \equiv b \pmod{m}$ is equivalent to the equation $ax = b + km$ for some $k \in \mathbb{Z}$. So if we cancel the common factor $d = (a, m)$ (which divides a and m by definition, and divides b by hypothesis) then we get $(a/d)x = (b/d) + k(m/d)$ or $(a/d)x = (b/d) \pmod{m/d}$. Now a/d and m/d are relatively prime, $(a/b, m/d) = 1$, since we have divided out $d = (a, m)$. So by Lemma 5.2, $(a/d)x = (b/d) \pmod{m/d}$ has exactly one solution, say $x = r$ where $0 \le r < m/d$. Notice that $x = r$ is also a solution to $ax \equiv b \pmod{m}$. Let $x = s$ be any other solution of $ax \equiv b \pmod{m}$. Then $ar \equiv as \equiv b \pmod{m}$, and so by Theorem 4.5 $r \equiv s \pmod{m/d}$. That is, $s - r = k(m/d)$ or $x = r + k(m/d)$ for some $k \in \mathbb{Z}$. ...

Lemma 5.3 (continued 1)

Lemma 5.3. Let $d = (a, m)$. If $d \mid b$ then $ax \equiv b \pmod{m}$ has exactly d solutions.

Proof (continued). That is, $s - r = k(m/d)$ or $x = r + k(m/d)$ for some $k \in \mathbb{Z}$. For $k \in \{0, 1, \ldots, d-1\}$, we have numbers which are least residues modulo m since (recall that $0 \le r \ < m/d$):

$$0 \le r + k(m/d) < (m/d) + (d-1)(m/d) = d(m/d) = m.$$

Also, for each such $r + k(m/d)$ we have

$$\begin{aligned}(a/d)(r + k(m/d)) &= (a/d)r + k(a/d)(m/d)\\ &\equiv (a/d)r \pmod{m/d} \text{ since } k(a/d) \text{ is an integer}\\ &\equiv b/d \pmod{m/d} \text{ since } ar \equiv b \pmod{m}\\ &\quad \text{implies that } ar/d \equiv b/d \pmod{m/d}.\end{aligned}$$

Lemma 5.3 (continued 2)

Lemma 5.3. Let $d = (a, m)$. If $d \mid b$ then $ax \equiv b \pmod{m}$ has exactly d solutions.

Proof (continued). Therefore $x = r + k(m/d)$ we have $(a/d)(r + k(m/d) = (a/d)x \equiv (b/d) (\text{mod } m/d)$. This then implies that $ax \equiv b \pmod{m}$. Now s is an arbitrary solution of $ax \equiv b \pmod{m}$, so every solution $ax \equiv b \pmod{m}$ is of the form $r + k(m/d)$ where $k \in \{0, 1, \ldots, d-1\}$. These solutions are different and hence $ax \equiv b \pmod{m}$ has exactly d solutions, as claimed. □

Theorem 5.2

Theorem 5.2. The Chinese Remainder Theorem.
The system of congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, k$, where $(m_i, m_j) = 1$ if $i \ne j$, has a unique solution modulo $m_1 m_2 \cdots m_k$.

Proof. We prove by induction. With $k = 1$, $x = a_1 \pmod{m_1}$ has a unique solution and the base case is established.

With $k = 2$, we have $x \equiv a_1$ (mod m_1, which implies $x = a_1 + k_1 m_1$ for some $k_1 \in \mathbb{Z}$. In this case we also need $x = a_1 + k_1 \equiv a_2 \pmod{m_2}$, or $k_1 m_1 \equiv a_2 - 1_a \pmod{m_2}$. Since $(m_1, m_2) = 1$ then by Lemma 5.2 (treating k_1 as the unknown) there is a solution k_1 modulo m_2, say $k_1 = t$ where $0 \le t < m_2$, and so k_1 is of the form $k_1 = t + k_2 m_2$. Therefore $x = a_1 + (t + k_2 m_2)m_1 \equiv a_1 + t m_1 \pmod{m_1 m_2}$ satisfies both congruences and the claim holds for $k = 2$ (we address uniqueness below).

Theorem 5.2 (continued 1)

Theorem 5.2. The Chinese Remainder Theorem.
The system of congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, k$, where $(m_i, m_j) = 1$ if $i \ne j$, has a unique solution modulo $m_1 m_2 \cdots m_k$.

Proof (continued). Now suppose the claim holds for $k = r - 1$. Then the system $x = a_i \pmod{m_i}$ for $i = 1, 2, \ldots, r-1$ has a solution $x = s$. Now we consider the system:

$$x = a_i \pmod{m_i} \text{ for } i = 1, 2, \ldots, r-1, \text{ and } x \equiv a_r \pmod{m_r}.$$

But this is just 2 congruences, and show has a solution based on the case $k = 2$ and the fact that the greatest common divisor $(m_1 m_2 \cdots m_{r-1}, m_r) = 1$. So by induction, the system of congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, k$, where $(m_i, m_j) = 1$ for $i \ne j$, has a solution.

Theorem 5.2 (continued 2)

Theorem 5.2. The Chinese Remainder Theorem.
The system of congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, k$, where $(m_i, m_j) = 1$ if $i \neq j$, has a unique solution modulo $m_1 m_2 \cdots m_k$.

Proof (continued). For uniqueness, suppose r and s are both solutions of the system. Then $r \equiv s \equiv a_1 \pmod{m_i}$ for $i = 1, 2, \ldots, k$. So $r - s \equiv 0 \pmod{m_i}$ and hence $m_i \mid (r - s)$ for $i = 1, 2, \ldots, k$; that is $r - s$ is a common multiple of $m_1, m_2, \ldots, m_k$. Applying the Fundamental Theorem of Arithmetic (Theorem 2.2) to each m_i, observing that the m_i are relatively prime, and using Lemma 2.6 we have that $(m_1 m_2 \cdots m_k) \mid (r - s)$. But r and s are least residues modulo $m_1 m_2 \cdots m_k$ (by the definition of "solution"), so $-m_1 m_2 \cdots m_k < r - s < m_1 m_2 \cdots m_k$ and therefore $r - s = 0$ (see Note 5.A), or $r = s$. So solutions are unique, and the claim holds. □