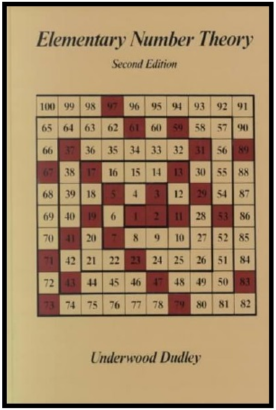
Elementary Number Theory

Section 4. Congruences—Proofs of Theorems



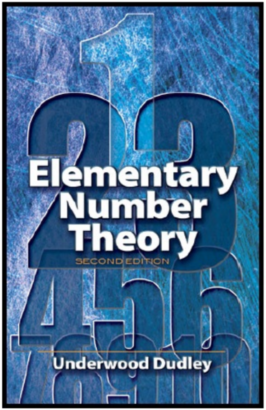


Table of contents

Theorem 4.1

Theorem 4.1. We have $a \equiv b \pmod{m}$ if and only if there is integer k such that $a = b + km$.

Proof. Suppose that $a \equiv b \pmod{m}$. Then by definition, $m \mid (a - b)$. By the definition of divisibility, there is some integer k with $km = a - b$, or $a = b + km$ as claimed.

Theorem 4.1

Theorem 4.1. We have $a \equiv b \pmod{m}$ if and only if there is integer k such that $a = b + km$.

Proof. Suppose that $a \equiv b \pmod{m}$. Then by definition, $m \mid (a - b)$. By the definition of divisibility, there is some integer k with $km = a - b$, or $a = b + km$ as claimed.

Conversely, suppose $a = b + km$ (this is Exercise 4.3 in the book). Then $km = a - b$ and by the definition of divisibility, $m \mid (a - b)$. By the definition of equivalent modulo m, this implies $a \equiv b \pmod{m}$, as claimed. □

Theorem 4.1

Theorem 4.1. We have $a \equiv b \pmod{m}$ if and only if there is integer k such that $a = b + km$.

Proof. Suppose that $a \equiv b \pmod{m}$. Then by definition, $m \mid (a - b)$. By the definition of divisibility, there is some integer k with $km = a - b$, or $a = b + km$ as claimed.

Conversely, suppose $a = b + km$ (this is Exercise 4.3 in the book). Then $km = a - b$ and by the definition of divisibility, $m \mid (a - b)$. By the definition of equivalent modulo m, this implies $a \equiv b \pmod{m}$, as claimed. □

Theorem 4.2

Theorem 4.2. Every integer is congruent modulo m to exactly one of $0, 1, 2, \ldots, m-1$. This number is called the *least residue* of the integer modulo m.

Proof. Let a be an integer. Then by Theorem 1.2 (The Division Algorithm), we have $a = qm + r$ where $0 \leq r < m$ for unique integers q and r. Since $a = qm + r$ then by the definition of equivalent modulo m we have $a \equiv r \pmod{m}$. Since r is uniquely determined by a and m, the claim follows. □

Theorem 4.2

Theorem 4.2. Every integer is congruent modulo m to exactly one of $0, 1, 2, \ldots, m-1$. This number is called the *least residue* of the integer modulo m.

Proof. Let a be an integer. Then by Theorem 1.2 (The Division Algorithm), we have $a = qm + r$ where $0 \leq r < m$ for unique integers q and r. Since $a = qm + r$ then by the definition of equivalent modulo m we have $a \equiv r \pmod{m}$. Since r is uniquely determined by a and m, the claim follows. □

Theorem 4.3.

Theorem 4.3. We have $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m.

Solution. Suppose a and b leave the same remainder, say r, when divided by m. Then $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1 and q_2. Then $a - b = (q_1 m + r) - (q_2 m + r) = m(q_1 - q_2)$, and by the definition of divisibility we have $m \mid (a - b)$. So by the definition of equivalent modulo m, we have $a \equiv b \pmod{m}$.

Theorem 4.3.

Theorem 4.3. We have $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m.

Solution. Suppose a and b leave the same remainder, say r, when divided by m. Then $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1 and q_2. Then $a - b = (q_1 m + r) - (q_2 m + r) = m(q_1 - q_2)$, and by the definition of divisibility we have $m \mid (a - b)$. So by the definition of equivalent modulo m, we have $a \equiv b \pmod{m}$.

Conversely, suppose $a \equiv b \pmod{m}$. Then $a \equiv b \equiv r \pmod{m}$, where r is the least residue given by Theorem 4.2. Then, as in the proof of Theorem 4.3, by Theorem 1.2 (The Division Algorithm) we have $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1 and q_2. Since $0 \leq r < m - 1$, then we have that r is the remainder both when a is divided by m and when b is divided by m, as claimed. $\square$

Theorem 4.3.

Theorem 4.3. We have $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m.

Solution. Suppose a and b leave the same remainder, say r, when divided by m. Then $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1 and q_2. Then $a - b = (q_1 m + r) - (q_2 m + r) = m(q_1 - q_2)$, and by the definition of divisibility we have $m \mid (a - b)$. So by the definition of equivalent modulo m, we have $a \equiv b \pmod{m}$.

Conversely, suppose $a \equiv b \pmod{m}$. Then $a \equiv b \equiv r \pmod{m}$, where r is the least residue given by Theorem 4.2. Then, as in the proof of Theorem 4.3, by Theorem 1.2 (The Division Algorithm) we have $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1 and q_2. Since $0 \leq r < m - 1$, then we have that r is the remainder both when a is divided by m and when b is divided by m, as claimed. $\square$

Lemma 4.1

Lemma 4.1. For integers a, b, c, and d we have

(a) $a \equiv a \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. (a) (This is Exercise 4.6.) Notice that $m \mid 0$, or $m \mid (a - a)$, so by the definition of equivalent modulo m, $a \equiv a \pmod{m}$, as claimed.

Lemma 4.1

Lemma 4.1. For integers a, b, c, and d we have

(a) $a \equiv a \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. (a) (This is Exercise 4.6.) Notice that $m \mid 0$, or $m \mid (a - a)$, so by the definition of equivalent modulo m, $a \equiv a \pmod{m}$, as claimed.

(b) (This is Exercise 4.7.) $a \equiv b \pmod{m}$ then by the definition of equivalent modulo m, we have $m \mid (a - b)$. By the definition of divisibility, $a - b = km$ for some integer k. Hence $b - a = (-k)m$ for integer $-k$ and so by the definition of equivalent modulo m, $b \equiv a \pmod{m}$, as claimed.

Lemma 4.1

Lemma 4.1. For integers a, b, c, and d we have

(a) $a \equiv a \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. (a) (This is Exercise 4.6.) Notice that $m \mid 0$, or $m \mid (a - a)$, so by the definition of equivalent modulo m, $a \equiv a \pmod{m}$, as claimed.

(b) (This is Exercise 4.7.) $a \equiv b \pmod{m}$ then by the definition of equivalent modulo m, we have $m \mid (a - b)$. By the definition of divisibility, $a - b = km$ for some integer k. Hence $b - a = (-k)m$ for integer $-k$ and so by the definition of equivalent modulo m, $b \equiv a \pmod{m}$, as claimed.

Lemma 4.1 (continued 1)

Lemma 4.1. For integers a, b, c, and d we have

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. (c) (This is Exercise 4.8.) Since $a \equiv b \pmod{m}$ then by the definition of equivalent modulo m, we have $m \mid (a - b)$. Since $b \equiv c \pmod{m}$ then by the definition of equivalent modulo m, we have $m \mid (b - c)$. By the definition of divisibility, $a - b = k_1 m$ and $b - c = k_2 m$ for some integers k_1 and k_2. Hence $a - c = (a - b) + (b - c) = k_1 m + k_2 m$ $= (k_1 + k_2)m$ and by the definition of divisibility $m \mid (a - c)$. Then by the definition of equivalent modulo m, $a \equiv c \pmod{m}$, as claimed.

Lemma 4.1 (continued 2)

Lemma 4.1. For integers a, b, c, and d we have

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. (d) (This is Exercise 4.9.) As in part (c), $a - b = k_1 m$ and $c - d = k_2 m$ for some integers k_1 and k_2. Hence, $(a + c) - (b + d) = (a - b) + (c - d) = k_1, + k_2 m = (k_1 + k_2)m$. Then by the definition of equivalent modulo m, $a + c \equiv b + d \pmod{m}$, as claimed.

(e) Since $a \equiv b \pmod{m}$ then $b - a = km$ for some integer k by Theorem 4.1. Similarly, $c \equiv d \pmod{m}$ implies $d - c = jm$ for some integer j. So $ac - bd = ac - (a + km)(c + jm) = ac - ac - ajm - ckm - kjm^2 = m(-aj - ck - kjm)$, and by the definition of equivalent modulo m, $ac \equiv bd \pmod{m}$, as claimed. □

Lemma 4.1 (continued 2)

Lemma 4.1. For integers a, b, c, and d we have

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. (d) (This is Exercise 4.9.) As in part (c), $a - b = k_1 m$ and $c - d = k_2 m$ for some integers k_1 and k_2. Hence, $(a + c) - (b + d) = (a - b) + (c - d) = k_1, +k_2 m = (k_1 + k_2)m$. Then by the definition of equivalent modulo m, $a + c \equiv b + d \pmod{m}$, as claimed.

(e) Since $a \equiv b \pmod{m}$ then $b - a = km$ for some integer k by Theorem 4.1. Similarly, $c \equiv d \pmod{m}$ implies $d - c = jm$ for some integer j. So $ac - bd = ac - (a + km)(c + jm) = ac - ac - ajm - ckm - kjm^2 = m(-aj - ck - kjm)$, and by the definition of equivalent modulo m, $ac \equiv bd \pmod{m}$, as claimed. □

Theorem 4.4.

Theorem 4.4. If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$. That is, we can cancel a factor on both sides of a congruence if the factor is relatively prime to the modulus.

Proof. Since $ac \equiv bc \pmod{m}$ then by the definition of congruence modulo m, $m \mid (ac - bc)$ or $m \mid c(a - b)$. Since $(m, c) = 1$ then by Theorem 1.5 we have $m \mid (a - b)$. So by the definition of congruence modulo m, $a \equiv b \pmod{m}$, as claimed. □

Theorem 4.4.

Theorem 4.4. If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$. That is, we can cancel a factor on both sides of a congruence if the factor is relatively prime to the modulus.

Proof. Since $ac \equiv bc \pmod{m}$ then by the definition of congruence modulo m, $m \mid (ac - bc)$ or $m \mid c(a - b)$. Since $(m, c) = 1$ then by Theorem 1.5 we have $m \mid (a - b)$. So by the definition of congruence modulo m, $a \equiv b \pmod{m}$, as claimed. □

Theorem 4.5.

Theorem 4.5. If $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

Proof. Since $ac \equiv bc \pmod{m}$ then by the definition of congruence modulo m, $m \mid (ac - bc)$ or $m \mid c(a - b)$. By the definition of divisibility, $c(a - b) = km$ for some integer k. Since $d = (c, m)$ then c/d and m/d are integers. So $c(a - b)/d = km/d$ of $(c/d)(a - b) = k(m/d)$; that is, $(m/d) \mid (c/d)(a - b)$. By Theorem 1.1 we have $(m/d, c/d) = 1$, and so by Corollary 1.1 we have $(m/d) \mid (a - b)$. By the definition of congruence modulo m/d we have $a \equiv b \pmod{m/d}$, as claimed. □

Theorem 4.5.

Theorem 4.5. If $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

Proof. Since $ac \equiv bc \pmod{m}$ then by the definition of congruence modulo m, $m \mid (ac - bc)$ or $m \mid c(a - b)$. By the definition of divisibility, $c(a - b) = km$ for some integer k. Since $d = (c, m)$ then c/d and m/d are integers. So $c(a - b)/d = km/d$ of $(c/d)(a - b) = k(m/d)$; that is, $(m/d) \mid (c/d)(a - b)$. By Theorem 1.1 we have $(m/d, c/d) = 1$, and so by Corollary 1.1 we have $(m/d) \mid (a - b)$. By the definition of congruence modulo m/d we have $a \equiv b \pmod{m/d}$, as claimed. □

Theorem 4.6.

Theorem 4.6. Every integer is congruent modulo 9 to the sum of its digits.

Proof. Let n be an integer with decimal representation $\pm d_k d_{k-1} d_{k-2} \cdots d_1 d_0$. That is,

$$n = \pm(d_k 10^k + d_{k-2} 10^{k-1} + d_{k-2} 10^{k-2} + \cdots d_1 10^1 + d_0 10^0).$$

Now $10 \equiv 1 \pmod 9$ and, more generally, for any $i \in \mathbb{N}$ we have $10^i \equiv 1 \pmod 9$. So

$$n \equiv \pm(d_k + d_{k-1} + d_{k-2} + \cdots + d_1 + d_0) \pmod 9,$$

as claimed. $\square$

Theorem 4.6.

Theorem 4.6. Every integer is congruent modulo 9 to the sum of its digits.

Proof. Let n be an integer with decimal representation $\pm d_k d_{k-1} d_{k-2} \cdots d_1 d_0$. That is,

$$n = \pm(d_k 10^k + d_{k-2} 10^{k-1} + d_{k-2} 10^{k-2} + \cdots d_1 10^1 + d_0 10^0).$$

Now $10 \equiv 1 \pmod 9$ and, more generally, for any $i \in \mathbb{N}$ we have $10^i \equiv 1 \pmod 9$. So

$$n \equiv \pm(d_k + d_{k-1} + d_{k-2} + \cdots + d_1 + d_0) \pmod 9,$$

as claimed. □