Mathematical Reasoning

Chapter 6. Number Theory

6.4. Congruence; Divisibility Tests—Proofs of Theorems

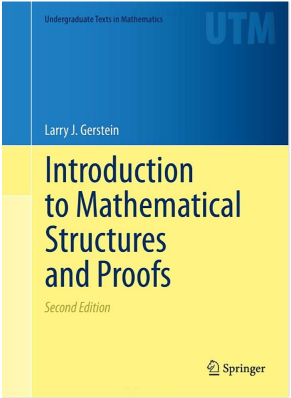

Table of contents

1. Theorem 6.41
2. Theorem 6.42
3. Theorem 6.45
4. Corollary 6.46. Test for Divisibility by 9
5. Theorem 6.48. Test for Divisibility by 11

Theorem 6.41

Theorem 6.41. Fix $m > 0$. Then congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Proof. First, let $a \in \mathbb{Z}$. Then $a = a + m(0)$ and so by Note 6.4.A we have $a \equiv a \pmod{m}$. That is, congruence modulo m is reflexive.

Theorem 6.41

Theorem 6.41. Fix $m > 0$. Then congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Proof. First, let $a \in \mathbb{Z}$. Then $a = a + m(0)$ and so by Note 6.4.A we have $a \equiv a \pmod{m}$. That is, congruence modulo m is reflexive.

Second, suppose $a \equiv b \pmod{m}$. Then by Note 6.4.A, $a = b + mk$ for some $k \in \mathbb{Z}$. Hence, $b = a + m(-k)$ for $-k \in \mathbb{Z}$ so that, by Note 6.4.A, $b \equiv a \pmod{m}$. That is, congruence modulo m is symmetric.

Theorem 6.41

Theorem 6.41. Fix $m > 0$. Then congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Proof. First, let $a \in \mathbb{Z}$. Then $a = a + m(0)$ and so by Note 6.4.A we have $a \equiv a \pmod{m}$. That is, congruence modulo m is reflexive.

Second, suppose $a \equiv b \pmod{m}$. Then by Note 6.4.A, $a = b + mk$ for some $k \in \mathbb{Z}$. Hence, $b = a + m(-k)$ for $-k \in \mathbb{Z}$ so that, by Note 6.4.A, $b \equiv a \pmod{m}$. That is, congruence modulo m is symmetric.

Finally, suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by Note 6.4.A, $a = b + mk_1$ and $b = c + mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then $a = (c + mk_2) + mk_1 = c + m(k_1 + k_2)$, so be Note 6.4.A we have $a \equiv c \pmod{m}$. That is, congruence modulo m is transitive.

Therefore, since congruence modulo m is symmetric, reflexive, and transitive, then by Definition 2.55 it is an equivalence relation. □

Theorem 6.41

Theorem 6.41. Fix $m > 0$. Then congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Proof. First, let $a \in \mathbb{Z}$. Then $a = a + m(0)$ and so by Note 6.4.A we have $a \equiv a \pmod{m}$. That is, congruence modulo m is reflexive.

Second, suppose $a \equiv b \pmod{m}$. Then by Note 6.4.A, $a = b + mk$ for some $k \in \mathbb{Z}$. Hence, $b = a + m(-k)$ for $-k \in \mathbb{Z}$ so that, by Note 6.4.A, $b \equiv a \pmod{m}$. That is, congruence modulo m is symmetric.

Finally, suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by Note 6.4.A, $a = b + mk_1$ and $b = c + mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then $a = (c + mk_2) + mk_1 = c + m(k_1 + k_2)$, so be Note 6.4.A we have $a \equiv c \pmod{m}$. That is, congruence modulo m is transitive.

Therefore, since congruence modulo m is symmetric, reflexive, and transitive, then by Definition 2.55 it is an equivalence relation. □

Theorem 6.42

Theorem 6.42. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

Proof. By Note 6.4.A, $a = b + mk_1$ and $c = d + mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then $a + c = (b + mk_1) + (d + mk_2) = (b + d) + m(k_1 + k_2)$. Therefore $a + c =\equiv b + d \pmod{m}$, as claimed.

Also, $ac = (b + mk_1)(b + mk_2) = bd + m(k_1 d + k_2 b + mk_1 k_2)$, so $ac \equiv bd \pmod{m}$, as claimed. □

Theorem 6.42

Theorem 6.42. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

Proof. By Note 6.4.A, $a = b + mk_1$ and $c = d + mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then $a + c = (b + mk_1) + (d + mk_2) = (b + d) + m(k_1 + k_2)$. Therefore $a + c = \equiv b + d \pmod{m}$, as claimed.

Also, $ac = (b + mk_1)(b + mk_2) = bd + m(k_1 d + k_2 b + mk_1 k_2)$, so $ac \equiv bd \pmod{m}$, as claimed. □

Theorem 6.45

Theorem 6.45. Every nonnegative integer is congruent modulo 9 to the sum of its decimal digits. Symbolically, if $0 \leq a_i \leq 9$ for $0 \leq i \leq t$, then

$$\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod 9.$$

Proof. Since $10 \equiv 1 \pmod 9$, then by Corollary 6.43 (the multiplicative part) $10^i \equiv 1 \pmod 9$ for all $i \geq 0$ and $a_i \cdot 10^i \equiv a_i \pmod 9$, and by Corollary 6.42 (the additive part) $\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod 9$, as claimed. □

Theorem 6.45

Theorem 6.45. Every nonnegative integer is congruent modulo 9 to the sum of its decimal digits. Symbolically, if $0 \le a_i \le 9$ for $0 \le i \le t$, then

$$\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod 9.$$

Proof. Since $10 \equiv 1 \pmod 9$, then by Corollary 6.43 (the multiplicative part) $10^i \equiv 1 \pmod 9$ for all $i \ge 0$ and $a_i \cdot 10^i \equiv a_i \pmod 9$, and by Corollary 6.42 (the additive part) $\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod 9$, as claimed. □

Corollary 6.46. Test for Divisibility by 9

Corollary 6.46. Test for Divisibility by 9).
An integer is a multiple of 9 if and only if the sum of its decimal digits is a multiple of 9.

Proof. First notice that we can assume without loss of generality that the given integer is nonnegative.

Corollary 6.46. Test for Divisibility by 9

Corollary 6.46. Test for Divisibility by 9).
An integer is a multiple of 9 if and only if the sum of its decimal digits is a multiple of 9.

Proof. First notice that we can assume without loss of generality that the given integer is nonnegative.

Suppose that $a \equiv b \pmod{m}$ and $m \mid a$. Then by Note 6.4.A $a = b + mk_1$ for some $k_1 \in \mathbb{Z}$, and $a = mk_2$ for some $k_2 \in \mathbb{Z}$. Therefore $b = a - mk_1 = mk_2 - mk_1 = m(k_2 - k_1)$ and hence $m \mid b$. Since congruence modulo m is symmetric by Theorem 6.41, then we have

$$\text{If } a \equiv b \pmod{m}, \text{ then } m \mid a \Leftrightarrow m \mid b.$$

Corollary 6.46. Test for Divisibility by 9

Corollary 6.46. Test for Divisibility by 9).
An integer is a multiple of 9 if and only if the sum of its decimal digits is a multiple of 9.

Proof. First notice that we can assume without loss of generality that the given integer is nonnegative.

Suppose that $a \equiv b \pmod{m}$ and $m \mid a$. Then by Note 6.4.A $a = b + mk_1$ for some $k_1 \in \mathbb{Z}$, and $a = mk_2$ for some $k_2 \in \mathbb{Z}$. Therefore $b = a - mk_1 = mk_2 - mk_1 = m(k_2 - k_1)$ and hence $m \mid b$. Since congruence modulo m is symmetric by Theorem 6.41, then we have

$$\text{If } a \equiv b \pmod{m}, \text{ then } m \mid a \Leftrightarrow m \mid b.$$

Applying this with $m = 9$ to $\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod{9}$, which holds by Theorem 6.45, we have that 9 divides $n = \sum_{i=1}^{t} a_i \cdot 10^i$ if and only if 9 divides $\sum_{i=0}^{t} a_i = a_0 + a_1 + \cdots a_t$, as claimed. □

Corollary 6.46. Test for Divisibility by 9

Corollary 6.46. Test for Divisibility by 9).
An integer is a multiple of 9 if and only if the sum of its decimal digits is a multiple of 9.

Proof. First notice that we can assume without loss of generality that the given integer is nonnegative.

Suppose that $a \equiv b \pmod{m}$ and $m \mid a$. Then by Note 6.4.A $a = b + mk_1$ for some $k_1 \in \mathbb{Z}$, and $a = mk_2$ for some $k_2 \in \mathbb{Z}$. Therefore $b = a - mk_1 = mk_2 - mk_1 = m(k_2 - k_1)$ and hence $m \mid b$. Since congruence modulo m is symmetric by Theorem 6.41, then we have

$$\text{If } a \equiv b \pmod{m}, \text{ then } m \mid a \Leftrightarrow m \mid b.$$

Applying this with $m = 9$ to $\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod{9}$, which holds by Theorem 6.45, we have that 9 divides $n = \sum_{i=1}^{t} a_i \cdot 10^i$ if and only if 9 divides $\sum_{i=0}^{t} a_i = a_0 + a_1 + \cdots a_t$, as claimed. □

Theorem 6.48. Test for Divisibility by 11

Theorem 6.48. (Test for Divisibility by 11).
An integer n with decimal representation $n = a_t a_{t-1} \dots a_0$ is divisible by 11 if and only if the number $a_t - a_{t-1} + a_{t-2} - \cdots \pm a_1 \mp a_0$ is divisible by 11.

Proof. Now $n = a_t a_{t-1} \dots a_0$ means $n = \sum_{i=0}^{t} a_i \cdot 10^i$. Since $10 \equiv -1 \pmod{11}$, then by Corollary 6.43 (the multiplicative part) $10^i \equiv (-1)^i \pmod{11}$ for all $i \geq 0$ and $a_i \cdot 10^i \equiv (-1)^i a_i \pmod{11}$, and by Corollary 6.42 (the additive part) $\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} (-1)^i a_i \pmod{11}$.

Theorem 6.48. Test for Divisibility by 11

Theorem 6.48. (Test for Divisibility by 11).
An integer n with decimal representation $n = a_t a_{t-1} \ldots a_0$ is divisible by 11 if and only if the number $a_t - a_{t-1} + a_{t-2} - \cdots \pm a_1 \mp a_0$ is divisible by 11.

Proof. Now $n = a_t a_{t-1} \ldots a_0$ means $n = \sum_{i=0}^{t} a_i \cdot 10^i$. Since $10 \equiv -1 \pmod{11}$, then by Corollary 6.43 (the multiplicative part) $10^i \equiv (-1)^i \pmod{11}$ for all $i \geq 0$ and $a_i \cdot 10^i \equiv (-1)^i a_i \pmod{11}$, and by Corollary 6.42 (the additive part) $\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} (-1)^i a_i \pmod{11}$. We saw in the proof of Corollary 6.47 that

$$\text{If } a \equiv b \pmod{m}, \text{ then } m \mid a \Leftrightarrow m \mid b,$$

so with $m = 11$ we have that 11 divides $n = \sum_{i=0}^{t} a_i \cdot 10^i$ if and only if 11 divides $\sum_{i=0}^{t} (-1)^i a_i = \pm(a_t - a_{t-1} + a_{t-2} = \cdots \pm a_0)$, as claimed. □

Theorem 6.48. Test for Divisibility by 11

Theorem 6.48. (Test for Divisibility by 11).
An integer n with decimal representation $n = a_t a_{t-1} \ldots a_0$ is divisible by 11 if and only if the number $a_t - a_{t-1} + a_{t-2} - \cdots \pm a_1 \mp a_0$ is divisible by 11.

Proof. Now $n = a_t a_{t-1} \ldots a_0$ means $n = \displaystyle\sum_{i=0}^{t} a_i \cdot 10^i$. Since $10 \equiv -1 \pmod{11}$, then by Corollary 6.43 (the multiplicative part) $10^i \equiv (-1)^i \pmod{11}$ for all $i \geq 0$ and $a_i \cdot 10^i \equiv (-1)^i a_i \pmod{11}$, and by Corollary 6.42 (the additive part) $\displaystyle\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} (-1)^i a_i \pmod{11}$. We saw in the proof of Corollary 6.47 that

$$\text{If } a \equiv b \pmod{m}, \text{ then } m \mid a \Leftrightarrow m \mid b,$$

so with $m = 11$ we have that 11 divides $n = \sum_{i=0}^{t} a_i \cdot 10^i$ if and only if 11 divides $\sum_{i=0}^{t} (-1)^i a_i = \pm(a_t - a_{t-1} + a_{t-2} = \cdots \pm a_0)$, as claimed. □