math22

Congruences

In this note we will discuss the congruence relation on the set of integers, in particular we will develop an arithmetic of remainders similar (but not identical) to the usual arithmetic on the set of integers. First we state and prove the division algorithm, and then we give the definitions.

Theorem. (Division Algorithm) If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers $q, r \in \mathbb{Z}$ such that

$$a = q \cdot b + r$$

with $0 \leq r < b$. The integer q is called the **quotient** when a is divided by b, and the integer r is called the (**least nonnegative**) **remainder** when a is divided by b.

Proof. If b divides a, that is, $a = q \cdot b$ for some integer q, then $r = 0$ and we are done. Suppose then that b does not divide a, and let

$$S = \{a - tb \,|\, t \in \mathbb{Z},\ a - tb > 0\}.$$

Note that if $a > 0$ and $t = 0$, then

$$a = a - 0 \cdot b \in S,$$

so that $S \neq \emptyset$.

Also, note that if $a \leq 0$ and $t = a - 1$, then

$$a - tb = a - (a-1)b = a(1-b) + b > 0$$

since $b \geq 1$, and again $a - tb \in S$, so that $S \neq \emptyset$.

Therefore, for any $a \in \mathbb{Z}$, S is a nonempty set of positive integers, and by the well-ordering principle, S has a smallest element, call it r. Since $r \in S$, then

$$0 < r = a - qb$$

for some $q \in \mathbb{Z}$.

Note that if $r = b$, then $a = (q+1)b$ and b divides a, which is a contradiction. Also note that if $r > b$, then $r = b + c$ for some $c \in \mathbb{N}^+$, and then

$$a - qb = r = b + c$$

implies that $c = a - (q+1)b \in S$, and $c = r - b < r$, which contradicts the fact that r is the smallest element of S.

This shows that there exist integers q and r such that

$$a = q \cdot b + r$$

with $0 \leq r < b$.

Now we show that these integers are unique. Suppose that

$$a = q_1 b + r_1 \qquad \text{and} \qquad a = q_2 b + r_2$$

where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 < b$, then

$$q_1 b + r_1 = q_2 b + r_2 \tag{$*$}$$

and therefore

$$(q_1 - q_2)b = r_2 - r_1,$$

so that

$$|q_1 - q_2|b = |r_1 - r_2| < b. \tag{$**$}$$

If $q_1 \neq q_2$, then $|q_1 - q_2| \geq 1$, and $(**)$ implies that $b < b$, which is a contradiction. Therefore, $q_1 = q_2$, and then from $(*)$ we have $r_1 = r_2$.

□

Definition. Let $m \in \mathbb{Z}^+$, $m > 1$, for $a, b \in \mathbb{Z}$ we say that a is **congruent** to b **modulo** m, and we write $a \equiv b \pmod{m}$, or $a \equiv_m b$ if and only if $a - b$ is a multiple of m, that is, if and only if

$$a = b + k \cdot m$$

for some $k \in \mathbb{Z}$.

The first theorem shows that the relation $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

Theorem 1. If $m \in \mathbb{Z}^+$, $m > 1$, then

(a) $a \equiv a \pmod{m}$ for each $a \in \mathbb{Z}$. (reflexivity)

(b) $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$ for all a, $b \in \mathbb{Z}$. (symmetry)

(c) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$ for all a, b, $c \in \mathbb{Z}$. (transitivity)

Proof.

(a) If $a \in \mathbb{Z}$, then $a - a = 0 = 0 \cdot m$, so that $a \equiv a \pmod{m}$.

(b) If a, $b \in \mathbb{Z}$ and $a \equiv b \pmod{m}$, then $a - b = k \cdot m$ for some $k \in \mathbb{Z}$, and so $b - a = (-k) \cdot m$, so that $b \equiv a \pmod{m}$ also.

(c) If a, b, $c \in \mathbb{Z}$, with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a - b = k \cdot m$ and $b - c = \ell \cdot m$, for some k, $\ell \in \mathbb{Z}$, so that $a - c = a - b + b - c = (k + \ell) \cdot m$, and $a \equiv c \pmod{m}$.

□

The next result says that two integers a and b are congruent modulo m if and only if a and b leave the same remainder when the division algorithm is employed to divide them by m.

Theorem 2. If $m \in \mathbb{Z}^+$, $m > 1$, and a, $b \in \mathbb{Z}$, then $a \equiv b \pmod{m}$ if and only if a and b leave the same least nonnegative remainder when divided by m.

Proof. Suppose that a and b leave the same least nonnegative remainders when divided by m, then from the division algorithm we can write (uniquely)

$$a = k \cdot m + r \qquad \text{and} \qquad b = \ell \cdot m + r$$

where k, ℓ, $r \in \mathbb{Z}$ and $0 \leq r < m$, so that

$$a - b = k \cdot m + r - (\ell \cdot m + r) = (k - \ell) \cdot m$$

and thus, $a \equiv b \pmod{m}$.

Conversely, suppose that $a \equiv b \pmod{m}$. From the division algorithm we can write (uniquely)

$$a = k \cdot m + r$$

where k, $r \in \mathbb{Z}$ and $0 \leq r < m$.

Since $a \equiv b \pmod{m}$, then $a - b = \ell \cdot m$ for some $\ell \in \mathbb{Z}$, so that

$$b = a - \ell \cdot m = k \cdot m - \ell \cdot m + r = (k - \ell) \cdot m + r$$

where $0 \leq r < m$, and therefore a and b leave the same least nonnegative remainder when divided by m.

□

From the division algorithm, when an integer a is divided by the positive integer $m > 1$, we have

$$a = k \cdot m + r$$

where $0 \leq r < m$.

Thus, the only possible least nonnegative remainders are

$$0,\ 1,\ 2,\ \ldots,\ m - 1$$

and the congruence relation $\equiv_m$ partitions the set of integers $\mathbb{Z}$ into the union of m pairwise disjoints sets, called **congruence classes**

$$\mathbb{Z} = [\,0\,] \cup [\,1\,] \cup [\,2\,] \cup \cdots \cup [\,m - 1\,],$$

where

$$\begin{aligned}
[\,0\,] &= \{\, 0 + m \cdot x \,|\, x \in \mathbb{Z} \,\} \\
[\,1\,] &= \{\, 1 + m \cdot x \,|\, x \in \mathbb{Z} \,\} \\
[\,2\,] &= \{\, 2 + m \cdot x \,|\, x \in \mathbb{Z} \,\} \\
&\vdots \\
[\,m - 1\,] &= \{\, m - 1 + m \cdot x \,|\, x \in \mathbb{Z} \,\}
\end{aligned}$$

Note that for $0 \leq r \leq m-1$, the congruence class containing r, denoted by $[\,r\,]$, consists of precisely those integers x such that $x \equiv r \pmod{m}$; and each integer $x \in \mathbb{Z}$, is in exactly one of the congruence classes $[\,0\,], [\,1\,], [\,2\,], \ldots, [\,m-1\,]$.

Example 1. If $m = 2$, then there are two congruence classes modulo 2, namely

$$[\,0\,] = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

and

$$[\,1\,] = \{\ldots, -3, -1, 1, 3, \ldots\}$$

that is, the **even** integers, and the **odd** integers.

Since $\mathbb{Z} = [\,0\,] \cup [\,1\,]$ and $[\,0\,] \cap [\,1\,] = \emptyset$, we have another proof of the fact that every integer is either even or odd, and no integer is both even and odd.

□

Example 2. If $m = 3$, then there are three congruence classes modulo 3, namely

$$[\,0\,] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[\,1\,] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[\,2\,] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

since there are only three possible least nonnegative remainders when an integer is divided by 3.

Thus, every integer m has exactly one of the forms

$$m = 3k, \qquad \text{or} \qquad m = 3k+1, \qquad \text{or} \qquad m = 3k+2$$

for some integer k.

Note that this implies that exactly one of the following is true

$$m^2 = 9k^2, \qquad \text{or} \qquad m^2 = 9k^2 + 6k + 1, \qquad \text{or} \qquad m^2 = 9k^2 + 12k + 3 + 1$$

for some integer k, that is, the square of an integer m can only be congruent to 0 or 1 modulo 3.

□

If $m > 1$ is a positive integer, we use $\mathbb{Z}_m$ to denote the set

$$\mathbb{Z}_m = \{\,[\,0\,], [\,1\,], [\,2\,], \ldots, [\,m-1\,]\,\}$$

of distinct congruence classes modulo m. If there is no danger of ambiguity, we often write

$$\mathbb{Z}_m = \{\,0, 1, 2, \ldots, m-1\,\}.$$

Addition and multiplication of congruence classes can be defined as follows, for $a, b \in \mathbb{Z}$,

$$[\,a\,] + [\,b\,] = [\,a+b\,] \qquad \text{and} \qquad [\,a\,] \cdot [\,b\,] = [\,a \cdot b\,],$$

and we leave it as an exercise to show that these operations are well-defined. In fact, these definitions of addition and multiplication give the set $\mathbb{Z}_m$ the structure of a commutative ring with identity.

The next results show that congruence behaves the same way as equality with respect to addition and multiplication, and the first theorem shows when congruence of two integers modulo $m > 1$ implies that the integers are, in fact, equal.

Theorem 3. If $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ with $0 \leq a, b < m$, and $a \equiv b \pmod{m}$, then $a = b$.

Proof. Since $a \equiv b \pmod{m}$ there exists an integer k such that $a - b = k \cdot m$, and since $0 \leq a, b \leq m - 1$, then we have

$$0 \leq a \leq m - 1 \qquad \text{and} \qquad -(m-1) \leq -b \leq 0,$$

and adding these two inequalities we get

$$-(m-1) \leq a - b \leq m - 1.$$

But if $a - b$ is a multiple of m and $-(m-1) \leq a - b \leq m - 1$, then we must have $a - b = 0$, since there is only one multiple of m between $-(m-1)$ and $m - 1$, namely, $0 \cdot m$. Therefore, $a = b$.

□

Theorem 4. If $m > 1$ is a positive integer and $a, b, c, d, \in \mathbb{Z}$ with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

(i) $a + c \equiv b + d \pmod{m}$

(ii) $a \cdot c \equiv b \cdot d \pmod{m}$

Proof. Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ there exist integers k and ℓ such that

$$a - b = k \cdot m \qquad \text{and} \qquad c - d = \ell \cdot m,$$

and therefore $a + c - (b + d) = a - b + c - d = k \cdot m + \ell \cdot m = (k + \ell) \cdot m$, so that $a + c \equiv b + d \pmod{m}$.

Also, $a \cdot c - b \cdot d = a \cdot c - b \cdot c + b \cdot c - b \cdot d = (a - b)d + b(c - d) = (k \cdot d + b \cdot \ell)m$, so that $a \cdot c \equiv b \cdot d \pmod{m}$.

□

Example 3. Find the least nonnegative remainder when 5^{110} is divided by 6.

Solution. First we note that $5 \equiv -1 \pmod{6}$, and using the previous theorem, we have

$$\begin{aligned} 5^2 &\equiv (-1)^2 \pmod{6} \\ 5^3 &\equiv (-1)^3 \pmod{6} \\ 5^4 &\equiv (-1)^4 \pmod{6} \\ &\vdots \\ 5^{110} &\equiv (-1)^{110} \pmod{6} \end{aligned}$$

and therefore $5^{110} \equiv 1 \pmod{6}$, and there exists an integer k such that $5^{110} = 6k + 1$.

□

Congruences may behave the same way as equality with respect to addition and multiplication, but not with respect to division. For example, the cancellation law, which held for the integers, is no longer true for congruences.

Example 4. Note that

$$5 \cdot 10 \equiv 2 \cdot 10 \,(\mathrm{mod}\, 15),$$

since

$$50 - 20 = 30 = 2 \cdot 15.$$

However, we cannot cancel the 10 in this congruence, since $5 - 2 = 3$ is not a multiple of 15, that is,

$$5 \not\equiv 2 \,(\mathrm{mod}\, 15).$$

□

We need to discuss the greatest common divisor of two integers before trying to ascertain when the cancellation law is valid for congruences.

Greatest Common Divisor

We introduced the notion of "divisibility" for two integers a and b when we discussed the division algorithm, now we give a formal definition and note some properties of the division operation.

Definition. If $a, b \in \mathbb{Z}$, then we say that b **divides** a and we write $b \mid a$, if and only if $b \neq 0$ and there exists an integer q such that $a = q \cdot b$. In this case, we also say that b is a **divisor** of a, or that a is a **multiple** of b. If b does not divide a, then we write $b \nmid a$.

We have the following properties for the division operation.

Theorem 5. If $a, b, c \in \mathbb{Z}$, then

(a) $1 \mid a$ and $a \mid 0$

(b) if $a \mid b$ and $b \mid a$ then $a = \pm b$

(c) if $a \mid b$ and $b \mid c$ then $a \mid c$

(d) if $a \mid b$ then $a \mid b \cdot x$ for all $x \in \mathbb{Z}$

(e) if $x = y + z$ and a divides any two of the integers x, y, or z, then a divides the remaining integer

(f) if $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for all $x, y \in \mathbb{Z}$.

Proof. We will prove part (b), and leave the rest as an exercise.

Suppose that $a \mid b$ and $b \mid a$, from the definition of the division operation it follows that $a \neq 0$ and $b \neq 0$, and that there exist integers k and ℓ such that

$$a = k \cdot b \qquad \text{and} \qquad b = \ell \cdot a,$$

so that

$$a = k \cdot b = k \cdot \ell \cdot a,$$

and from the cancellation law, since $a \neq 0$, we have $k \cdot \ell = 1$. Since k and ℓ are nonzero integers, then $|k| \geq 1$ and $|\ell| \geq 1$, so we must have either $k = \ell = 1$ or $k = \ell = -1$, that is, either $a = b$ or $a = -b$.

□

Since we are only really interested in *positive* divisors, we make the following definition:

Definition. If $a, b \in \mathbb{Z}$, a positive integer c is said to be a **common divisor** of a and b if and only if $c \,|\, a$ and $c \,|\, b$.

Example 5. The common divisors of 42 and 70 are 1, 2, 7, 14, and $d = 14$ is the *greatest* of the common divisors of 42 and 70.

Definition. If $a, b \in \mathbb{Z}$, where at least one of the integers a and b is nonzero, then a positive integer d is called a **greatest common divisor** of a and b if and only if

(i) $d \,|\, a$ and $d \,|\, b$,

(ii) for any common divisor c of a and b, we have $c \,|\, d$.

Any greatest common divisor of a and b is denoted by $\gcd(a, b)$, and we have the following theorem.

Theorem 6. For any $a, b \in \mathbb{Z}^+$, there exists a unique $d \in \mathbb{Z}^+$ such that d is the greatest common divisor of a and b, that is, $d = \gcd(a, b)$.

Moreover, $d = \gcd(a, b)$ is the smallest positive integer that can be written as a linear combination of a and b, that is, the smallest positive integer d such that

$$d = ax + by$$

for some $x, y \in \mathbb{Z}$.

Proof. Given $a, b \in \mathbb{Z}^+$, let

$$S = \{as + bt \,|\, s, t \in \mathbb{Z},\ as + bt > 0\},$$

then S is a nonempty set of positive integers (a and b are in S), and by the well-ordering principle, S has a smallest element, say d. We claim that d is a greatest common divisor of a and b.

Since $d \in S$, then $d = ax + by$ for some $x, y \in \mathbb{Z}$, and if c is a common divisor of a and b, then $c \,|\, d$ also.

If $d \nmid a$, then from the division algorithm, there exist integers q and r such that

$$a = q \cdot d + r$$

with $0 < r < d$, so that

$$r = a - q \cdot d = a - q(ax + by) = (1 - qx)a + (-qy)b,$$

and $r \in S$ and $0 < r < d$, which contradicts the choice of d as the least element of S.

Thus, $d \,|\, a$, and a similar argument shows that $d \,|\, b$.

Therefore, any $a, b \in \mathbb{Z}^+$ have a greatest common divisor.

To prove uniqueness, suppose that d_1 and d_2 are positive integers that satisfy the definition of the greatest common divisor, then $d_1 \,|\, d_2$ and $d_2 \,|\, d_1$, and since d_1 and d_2 are positive, Theorem 5 implies that $d_1 = d_2$.

□

Note: We have shown that any two positive integers a and b have a unique greatest common divisor, which we denote by $\gcd(a, b)$. We define it for other integers as follows:

(i) if $a \in \mathbb{Z}$, with $a \neq 0$, then we define
$$\gcd(a, 0) = |a|,$$

(ii) if $a, b \in \mathbb{Z}^+$, then we define
$$\gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(a, b),$$

(iii) $\gcd(0, 0)$ is **not** defined.

Definition. If $a, b \in \mathbb{Z}$, then we say that the integers a and b are **relatively prime** or **coprime** if and only if $\gcd(a, b) = 1$, that is, if and only if
$$ax + by = 1$$
for some $x, y \in \mathbb{Z}$.

Theorem 7. If $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$, then
$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1,$$
that is, $\dfrac{a}{d}$ and $\dfrac{b}{d}$ are relatively prime.

Proof. There exist $x, y \in \mathbb{Z}$ such that $d = ax + by$, and therefore
$$\frac{a}{d} \cdot x + \frac{b}{d} \cdot y = 1,$$
and this is the smallest postive integer which is a linear combination of a/d and b/d.

□

Example 6. Since $\gcd(3, 5) = 1$, then we can find integers x and y such that $3x + 5y = 1$. For example, take $x = 2$ and $y = -1$, then
$$3(2) + 5(-1) = 1.$$
However, for any $k \in \mathbb{Z}$, we have
$$1 = 3(2 - 5k) + 5(-1 + 3k),$$
so the solution for x and y is not unique.

Now we can determine when the cancellation law hold for congruences.

Theorem 8. Let $m \in \mathbb{Z}^+$ and a, b, $c \in \mathbb{Z}$, with $d = \gcd(c, m)$, if $a \cdot c \equiv b \cdot c \pmod{m}$, then $a \equiv b \pmod{\frac{m}{d}}$.

Proof. If $a \cdot c \equiv b \cdot c \pmod{m}$ then there exists an integer k such that $a \cdot c - b \cdot c = k \cdot m$, that is, $c(a-b) = k \cdot m$, and therefore
$$\frac{c}{d}(a - b) = k \cdot \frac{m}{d}.$$
Since $\gcd\left(\frac{c}{d}, \frac{m}{d}\right) = 1$, then $\frac{m}{d} \mid a - b$, that is, $a \equiv b \pmod{\frac{m}{d}}$.

□

Corollary 9. Let $m \in \mathbb{Z}^+$ and a, b, $c \in \mathbb{Z}$, with $\gcd(m, c) = 1$, that is, m and c are relatively prime.

If $a \cdot c \equiv b \cdot c \pmod{m}$, then $a \equiv b \pmod{m}$, that is, the cancellation law holds.

Euclidean Algorithm

The proof of the existence of the greatest common divisor in Theorem 6 was nonconstructive, that is, it did not tell us how to find the greatest common divisor. Now we give an algorithm to find the gcd of two positive integers a and b.

First we note that if a and b are positive integers and $b \mid a$, then we have $\gcd(a, b) = b$.

Let a and b be positive integers and suppose that $b \nmid a$, we know from the division algorithm that there exist unique integers q_1 and r_1, such that

$$a = b \cdot q_1 + r_1 \tag{1}$$

with $0 < r_1 < b$. From (1), the integers a and b have the same common divisors as the integers b and r_1, and therefore $\gcd(a, b) = \gcd(b, r_1)$.

Continuing, we find unique integers q_2 and r_2, such that

$$b = r_1 \cdot q_2 + r_2 \tag{2}$$

with $0 < r_2 < r_1$ if $r_1 \nmid b$,

$$\vdots$$

and continuing in this manner, we find unique integers q_k and r_k, such that

$$r_{k-2} = r_{k-1} \cdot q_k + r_k \tag{k}$$

with $0 < r_k < r_{k-1}$ if $r_{k-1} \nmid r_{k-2}$.

This process must terminate, since the remainders are all nonnegative and are strictly decreasing.

If r_n is the last nonzero remainder, then the last two equations are

$$\begin{aligned} r_{n-2} &= r_{n-1} \cdot q_n + r_n \\ r_{n-1} &= r_n \cdot q_{n+1}. \end{aligned}$$

It is clear that

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n,$$

since at any stage the integers r_{k-2} and r_{k-1} have the same common divisors as the integers r_{k-1} and r_k, and hence the same greatest common divisor.

This is the **Euclidean algorithm** for computing the greatest common divisor of two positive integers a and b, and the fact that we can write

$$\gcd(a, b) = s \cdot a + t \cdot b$$

for some integers s and t (Theorem 6) is sometimes called the **extended Euclidean algorithm**.

This can be done most easily by working from the bottom up in the equations in the Euclidean algorithm. We will give an example in the next section when we find the modular inverse.

Linear Congruences

Given a positive integer $m > 1$, a **linear congruence** is a congruence of the form

$$ax \equiv b \,(\mathrm{mod}\, m) \qquad (*)$$

where a and b are integers. A **solution** to the linear congruence is an integer x_0 such that $ax_0 \equiv b \,(\mathrm{mod}\, m)$, that is, an integer that satisfies the congruence $(*)$.

For example, we have $3 \cdot 4 \equiv 2, (\mathrm{mod}\, 10)$, so that 4 is a solution to the congruence $3x \equiv 2 \,(\mathrm{mod}\, 10)$. However, the congruence $2x \equiv 1 \,(\mathrm{mod}\, 4)$ has no solution, since there does not exist an integer x such that $2x - 1$ is divisible by 4.

The next theorem gives a necessary and sufficient condition for the linear congruence $(*)$ to have a solution.

Recall that if a and b integers which are not both 0, then the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the smallest positive integer which divides both a and b.

Theorem 10. If $m > 1$ is a positive integer and a, $b \in \mathbb{Z}$, then the linear congruence

$$ax \equiv b \,(\mathrm{mod}\, m)$$

has a solution if and only if $d \,|\, b$, where $d = \gcd(a, m)$. Moreover, if $d \,|\, b$, then the congruence has d incongruent solutions.

Proof. Let $d = \gcd(a, m)$, and suppose that $d \,|\, b$, then there exists an integer k such that $b = kd$. From the Euclidean algorithm, there exist integers x and y such that $d = ax + my$, and therefore,

$$b = k(ax + my) = a(kx) + m(ky)$$

and letting $x_0 = kx$, we have $ax_0 \equiv b \,(\mathrm{mod}\, m)$ and x_0 is a solution to the congruence.

Conversely, if x_0 is a solution to the congruence, then $ax_0 \equiv b \,(\mathrm{mod}\, m)$, so that $b = ax_0 + km$ for some integer k, and therefore if $d = \gcd(a, m)$, then $d \,|\, b$.

Finally, suppose that $d \,|\, b$ and that x_0 is an arbitrary solution to the congruence $ax \equiv b \,(\mathrm{mod}\, m)$, then

$$x_0 + \left(\frac{m}{d}\right) k$$

is also a solution for $k = 0, 1, 2, \ldots, d - 1$, since $ax_0 + \left(\frac{m}{d}\right) ak \equiv ax_0 + \left(\frac{a}{d}\right) km \equiv ax_0 \equiv b \,(\mathrm{mod}\, m)$.

If $x_1 = x_0 + \left(\frac{m}{d}\right) k_1$ and $x_2 = x_0 + \left(\frac{m}{d}\right) k_2$ are two solutions and $x_1 \equiv x_2 \,(\mathrm{mod}\, m)$, then

$$\left(\frac{m}{d}\right) k_1 \equiv \left(\frac{m}{d}\right) k_2 \,(\mathrm{mod}\, m),$$

and from Theorem 5, since $\dfrac{m}{d} \,|\, m$, then

$$k_1 \equiv k_2 \,(\mathrm{mod}\ d),$$

that is, x_1 and x_2 are congruent modulo m if and only if k_1 and k_2 are congruent modulo d, thus, x_1 and x_2 are incongruent modulo m if and only if they belong to distinct equivalence classes modulo d.

□

Note: The d incongruent (modulo m) solutions $x = x_0 + \left(\frac{m}{d}\right)k$, where $0 \leq k \leq d-1$, make up what is called the **general solution** of the linear congruence $ax \equiv b \pmod{m}$.

As a corollary to this theorem, we have a useful result.

Corollary 11. If $m > 1$ is a positive integer and a, $b \in \mathbb{Z}$, then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution if and only if $\gcd(a, m) = 1$, that is, if and only if a and m are relatively prime.

In particular, if $b = 1$, then we have

Corollary 12. If $m > 1$ is a positive integer and $a \in \mathbb{Z}$, then the linear congruence

$$ax \equiv 1 \pmod{m}$$

has a solution if and only if $\gcd(a, m) = 1$, that is, if and only if a and m are relatively prime. In this case, the unique solution is called the **inverse** of a modulo m and is denoted by a^{-1}.

If $m > 1$ is a positive integer and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, the Euclidean algorithm gives an elementary method to find the inverse of a modulo m, namely, we use the algorithm to find integers x and y such that

$$ax + my = 1,$$

and then $a^{-1} \equiv x \pmod{m}$.

Example 7. Find the inverse of 12 modulo 35.

Solution. Applying the Euclidean algorithm we have

$$\begin{aligned} 35 &= 2 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0 \end{aligned}$$

and the last nonzero remainder is 1, that is, $\gcd(35, 12) = 1$, so that 12 has an inverse modulo 35.

Working backwards, we write the greatest common divisor 1 as a linear combination of 35 and 12,

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 \\ &= 12 - 1 \cdot (35 - 2 \cdot 12) \\ &= 3 \cdot 12 + 1 \cdot 35 \end{aligned}$$

so that

$$12 \cdot 3 \equiv 1 \pmod{35},$$

and the inverse of 12 modulo 35 is 3.