1 Divisibility

Given two integers a, b with $a \neq 0$. We say that a **divides** b, written

$$a \mid b,$$

if there exists an integer q such that

$$b = qa.$$

When this is true, we say that a is a **factor** (or **divisor**) of b, and b is a **multiple** of a. If a is not a factor of b, we write

$$a \nmid b.$$

Any integer n has divisors ± 1 and $\pm n$, called the **trivial divisors** of n. If a is a divisor of n, so is $-a$. A positive divisor of n other than the trivial divisors is called a **nontrivial divisor** of n. Every integer is a divisor of 0.

A positive integer p ($\neq 1$) is called a **prime** if it has no nontrivial divisors, i.e., its positive divisors are only the trivial divisors 1 and p.

A positive integer is called **composite** if it is not a prime. The first few primes are listed as

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

Proposition 1.1. *Every composite number n has a prime factor $p \leq \sqrt{n}$.*

Proof. Since n is composite, there are primes p and q such that $n = pqk$, where $k \in \mathbb{P}$. Note that for primes p and

q, one is less than or equal to the other, say $p \le q$. Then $p^2 \le pqk = n$. Thus $p \le \sqrt{n}$. $\square$

Example 1.1. 6 has the prime factor $2 \le \sqrt{6}$;

9 has the prime factor $3 = \sqrt{9}$;

35 has the prime factor $5 \le \sqrt{35}$.

Is 143 a prime?

We find $\sqrt{143} < \sqrt{144} = 12$. For $i = 2, 3, 5, 7, 11$, check whether i divides 143. We find out $i \nmid 143$ for $i = 2, 3, 5, 7$, and $11 \mid 143$. So 143 is a composite number.

Is 157 a prime?

Since $\sqrt{157} < \sqrt{169} = 13$. For $i = 2, 3, 5, 7, 11$, we find out $i \nmid 157$. We see that 157 has no prime factor less or equal to $\sqrt{157}$. So 157 is not a composite; 157 is a prime.

Proposition 1.2. *Let a, b, c be nonzero integers.*

(a) *If $a \mid b$ and $b \mid a$, then $a = \pm b$.*

(b) *If $a \mid b$ and $b|c$, then $a \mid c$.*

(c) *If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.*

Proof. (a) Write $b = q_1 a$, $a = q_2 b$ for some $q_1, q_2 \in \mathbb{Z}$. Then

$$b = q_1 q_2 b.$$

Dividing both sides by b, we have $q_1 q_2 = 1$. This forces that $q_1 = q_2 = \pm 1$. Thus $b = \pm a$.

(b) Write $b = q_1 a$, $c = q_2 b$ for some integers $q_1, q_2 \in \mathbb{Z}$. Then $c = q_1 q_2 a$. This means that $a \mid c$.

(c) Write $b = q_1 a$, $c = q_2 a$ for some $q_1, q_2 \in \mathbb{Z}$. Then, for any $x, y \in \mathbb{Z}$,

$$bx + cy = q_1 ax + q_2 ay = (q_1 x + q_2 y)a.$$

This means that $a \mid (bx + cy)$. $\square$

Theorem 1.3. *There are infinitely many prime numbers.*

Proof. Suppose there are finitely many primes, say, they are listed as follows

$$p_1, p_2, \ldots, p_k.$$

Then the integer

$$a = p_1 p_2 \cdots p_k + 1$$

is not divisible by any of the primes $p_1, p_2, \ldots, p_k$ because the remainders of a divided by any p_i is always 1, $1 \le i \le k$. This means that a has no prime factors. By definition of primes, the integer a is a prime, and this prime is larger than all primes $p_1, p_2, \ldots, p_k$. So it is larger than itself, a contradiction. $\square$

Theorem 1.4 (Division Algorithm). *For any $a, b \in \mathbb{Z}$ with $a > 0$, there exist unique integers q, r such that*

$$b = qa + r, \qquad 0 \le r < a.$$

Proof. Define the set $S = \{b - ta \ge 0 : t \in \mathbb{Z}\}$. Then S is nonempty and bounded below. By the Well-Ordering Principle, S has the unique minimum integer r. Then there is a unique integer q such that $b - qa = r$. Thus

$$b = qa + r.$$

Clearly, $r \geq 0$. We claim that $r < a$. Suppose $r \geq a$, then

$$b - (q+1)a = r - a \geq 0.$$

This means that $r - a$ is an element of S, but smaller than r. This is contrary to that r is the minimum element in S. $\square$

Example 1.2. For integers $a = 24$ and $b = 379$, we have

$$379 = 15 \cdot 24 + 19, \qquad q = 15,\ r = 19.$$

For integers $a = 24$ and $b = -379$, we have

$$-379 = -14 \cdot 24 + 5, \qquad q = -14,\ r = 5.$$

2 Greatest Common Divisor

For integers a and b, not simultaneously 0, a **common divisor** of a and b is an integer c such that $c|a$ and $c|b$.

Definition 2.1. Let $a, b \in \mathbb{Z}$, not simultaneously 0. A positive integer d is called the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, if

(a) $d \mid a$, $d \mid b$, and

(b) If $c \mid a$ and $c \mid b$, then $c \mid d$.

Two integers a and b are called **coprime** (or **relatively prime**) if $\gcd(a, b) = 1$.

Theorem 2.2. *For any integers $a, b \in \mathbb{Z}$, if*

$$b = qa + r$$

for some integers $q, r \in \mathbb{Z}$, then

$$\gcd(a, b) = \gcd(a, r).$$

Proof. Write $d_1 = \gcd(a, b)$, $d_2 = \gcd(a, r)$.

Since $d_1 \mid a$ and $d_1 \mid b$, then $d_1 \mid r$ because $r = b - qa$. So d_1 is a common divisor of a and r. Thus, by definition of $\gcd(a, r)$, d_1 divides d_2. Similarly, since $d_2 \mid a$ and $d_2 \mid r$, then $d_2 \mid b$ because $b = qa + r$. So d_2 is a common divisor of a and b. By definition of $\gcd(a, b)$, d_2 divides d_1. Hence, by Proposition 1.2 (a), $d_1 = \pm d_2$. Thus $d_1 = d_2$. $\square$

The above proposition gives rise to a simple constructive method to calculate gcd by repeating the Division Algorithm.

Example 2.1. Find $\gcd(297, 3627)$.

$$\begin{array}{lcll}
3627 & = & 12 \cdot 297 + 63, \quad \gcd(297, 3627) & = \gcd(63, 297) \\
297 & = & 4 \cdot 63 + 45, & = \gcd(45, 63) \\
63 & = & 1 \cdot 45 + 18, & = \gcd(18, 45) \\
45 & = & 2 \cdot 18 + 9, & = \gcd(9, 18) \\
18 & = & 2 \cdot 9; & = 9.
\end{array}$$

The procedure to calculate $\gcd(297, 3627)$ applies to any pair of positive integers.

Let $a, b \in \mathbb{N}$ be nonnegative integers. Write $d = \gcd(a, b)$. Repeating the Division Algorithm, we find nonnegative integers $q_i, r_i \in \mathbb{N}$ such that

$$\begin{array}{lcll} b & = & q_0 a + r_0, & 0 \le r_0 < a, \\ a & = & q_1 r_0 + r_1, & 0 \le r_1 < r_0, \\ r_0 & = & q_2 r_1 + r_2, & 0 \le r_2 < r_1, \\ r_1 & = & q_3 r_2 + r_3, & 0 \le r_3 < r_2, \\ & \vdots & & \\ r_{k-2} & = & q_k r_{k-1} + r_k, & 0 \le r_k < r_{k-1}, \\ r_{k-1} & = & q_{k+1} r_k + r_{k+1}, & r_{k+1} = 0. \end{array}$$

The nonnegative sequence $\{r_i\}$ is strictly decreasing. It must end to 0 at some step, say, $r_{k+1} = 0$ for the very first time. Then $r_i \neq 0$, $0 \le i \le k$. Reverse the sequence $\{r_i\}_{i=0}^k$ and make substitutions as follows:

$$\begin{array}{lcl} d & = & r_k, \\ r_k & = & r_{k-2} - q_k r_{k-1}, \\ r_{k-1} & = & r_{k-3} - q_{k-1} r_{k-2}, \\ & \vdots & \\ r_1 & = & a - q_1 r_0, \\ r_0 & = & b - q_0 a. \end{array}$$

We see that $\gcd(a, b)$ can be expressed as an integral linear combination of a and b. This procedure is known as the **Euclidean Algorithm**.

We summarize the above argument into the following theorem.

Theorem 2.3. *For any integers $a, b \in \mathbb{Z}$, there exist in-*

tegers $x, y \in \mathbb{Z}$ *such that*

$$\gcd(a, b) = ax + by.$$

Example 2.2. Express $\gcd(297, 3627)$ as an integral linear combination of 297 and 3627.

Dy the Division Algorithm, we have $\gcd(297, 3627) = 9$. By the Euclidean Algorithm,

$$\begin{aligned}
9 &= 45 - 2 \cdot 18 \\
&= 45 - 2(63 - 45) \\
&= 3 \cdot 45 - 2 \cdot 63 \\
&= 3(297 - 4 \cdot 63) - 2 \cdot 63 \\
&= 3 \cdot 297 - 14 \cdot 63 \\
&= 3 \cdot 297 - 14(3627 - 12 \cdot 297) \\
&= 171 \cdot 297 - 14 \cdot 3627.
\end{aligned}$$

Example 2.3. Find $\gcd(119, 45)$ and express it as an integral linear combination of 45 and 119.

Applying the Division Algorithm,

$$\begin{aligned}
119 &= 2 \cdot 45 + 29 \\
45 &= 29 + 16 \\
29 &= 16 + 13 \\
16 &= 13 + 3 \\
13 &= 4 \cdot 3 + 1
\end{aligned}$$

So $\gcd(119, 45) = 1$. Applying the Euclidean Algorithm,

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 = 13 - 4(16 - 13) \\ &= 5 \cdot 13 - 4 \cdot 16 = 5(29 - 16) - 4 \cdot 16 \\ &= 5 \cdot 29 - 9 \cdot 16 = 5 \cdot 29 - 9(45 - 29) \\ &= 14 \cdot 29 - 9 \cdot 45 = 14(119 - 2 \cdot 45) - 9 \cdot 45 \\ &= 14 \cdot 119 - 37 \cdot 45 \end{aligned}$$

Example 2.4. Find $\gcd(119, -45)$ and express it as linear combination of 119 and -45.

We have $\gcd(119, -45) = \gcd(119, 45) = 1$. Since

$$1 = 14 \cdot 119 - 37 \cdot 45,$$

we have $\gcd(119, -45) = 14 \cdot 119 + 37 \cdot (-45)$.

Remark. For any $a, b \in \mathbb{Z}$, $\gcd(a, -b) = \gcd(a, b)$. Expressing $\gcd(a, -b)$ in terms of a and $-b$ is the same as that of expressing $\gcd(a, b)$ in terms of a and b.

Proposition 2.4. *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. By the Euclidean Algorithm, there are integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Then

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Since $a \mid ac$ and $a \mid bc$, thus $c \mid (acx + bcy)$ by Proposition 1.2 (c). Therefore $a \mid c$. $\square$

Theorem 2.5 (Unique Factorization). *Every integer $a \geq 2$ can be uniquely factorized into the form*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

where $p_1, p_2, \ldots, p_m$ are distinct primes, $e_1, e_2, \ldots, e_m$ are positive integers, and $p_1 < p_2 < \cdots < p_s$.

Proof. (Not required) We first show that a has a factorization into primes. If a has only the trivial divisors, then a itself is a prime, and it obviously has unique factorization. If a has some nontrivial divisors, then

$$a = bc$$

for some positive integers $b, c \in \mathbb{P}$ other than 1 and a. So $b < a$, $c < a$. By induction, the positive integers b and c have factorizations into primes. Consequently, a has a factorization into primes.

Next we show that the factorization of a is unique in the sense of the theorem.

Let $a = q_1^{f_1} q_2^{f_2} \cdots a_n^{f_n}$ be any factorization, where $q_1, q_2, \ldots, q_n$ are distinct primes, $f_1, f_2, \ldots, f_n$ are positive integers, and $q_1 < q_2 < \cdots < q_n$. We claim that $m = n$, $p_i = q_i$, $e_i = f_i$ for all $1 \leq i \leq m$.

Suppose $p_1 < q_1$. Then p_1 is distinct from the primes $q_1, q_2, \ldots, q_n$. It is clear that $\gcd(p_1, q_i) = 1$, and so

$$\gcd(p_1, q_i^{f_i}) = 1 \quad \text{for all} \quad 1 \leq i \leq n.$$

Note that $p_1 \mid q_1^{f_1} q_2^{f_2} \cdots a_n^{f_n}$. Since $\gcd(p_1, q_1^{f_1}) = 1$, by Proposition 2.4, we have $p_1 \mid q_2^{f_2} \cdots a_n^{f_n}$. Since $\gcd(p_1, q_2^{f_2}) = 1$, again by Proposition 2.4, we have $p_1 \mid q_3^{f_2} \cdots a_n^{f_n}$. Repeating the argument, eventually we have $p_1 \mid q_n^{f_n}$, which is contrary to $\gcd(p_1, q_n^{f_n}) = 1$. We thus conclude $p_1 \geq q_1$. Similarly, $q_1 \geq p_1$. Therefore $p_1 = q_1$. Next we claim $e_1 = f_1$.

Suppose $e_1 < f_1$. Then

$$p_2^{e_2} \cdots p_m^{e_m} = p_1^{f_1 - e_1} q_2^{f_2} \cdots q_n^{f_n}.$$

This implies that $p_1 | p_2^{e_2} \cdots p_m^{e_m}$. If $m = 1$, then $p_2^{e_2} \cdots p_m^{e_m} = 1$. So $p_1 \mid 1$. This is impossible because p_1 is a prime. If $m \geq 2$, since $\gcd(p_1, p_i) = 1$, we have $\gcd(p_1, p_i^{e_i}) = 1$ for all $2 \leq i \leq m$. Applying Proposition 2.4 repeatedly, we have $p_1 | p_m^{e_m}$, which is contrary to $\gcd(p_1, p_m^{e_m}) = 1$. We thus conclude $e_1 \geq f_1$. Similarly, $f_1 \geq e_1$. Therefore $e_1 = f_1$.

Now we have obtained $p_2^{e_2} \cdots p_m^{e_m} = q_2^{f_2} \cdots q_n^{f_n}$. If $m < n$, then by induction we have $p_1 = q_1, \ldots, p_m = q_m$ and $e_1 = f_1, \ldots, e_m = f_m$. Thus $1 = q_{m+1}^{f_{m+1}} \cdots q_n^{f_n}$. This is impossible because $q_{m+1}, \ldots, q_n$ are primes. So $m \geq n$. Similarly, $n \geq m$. Hence we have $m = n$. By induction, we have $e_2 = f_2, \ldots, e_m = f_m$.

Our proof is finished. $\square$

Example 2.5. Factorize the numbers 180 and 882, and find $\gcd(180, 882)$.

Solution. 180/2=90, 90/2=45, 45/3=15, 15/3=5, 5/5=1. Then $360 = 2^2 \cdot 3^2 \cdot 5$. Similarly, 882/2=441, 441/3=147, 147/3=49, 49/7=7, 7/7=1. We have $882 = 2 \cdot 3^2 \cdot 7^2$. Thus $\gcd(180, 882) = 2 \cdot 3^2 = 18$.

3 Least Common Multiple

For two integers a and b, a positive integer m is called a **common multiple** of a and b if $a \mid m$ and $b \mid m$.

Definition 3.1. Let $a, b \in \mathbb{Z}$. The **least common multiple** of a and b, denoted by $\operatorname{lcm}(a, b)$, is a positive integer m such that

(a) $a \mid m$, $b \mid m$, and

(b) If $a \mid c$ and $b \mid c$, then $m \mid c$.

Proposition 3.2. *For any nonnegative integers $a, b \in \mathbb{N}$,*

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

Proof. Let $a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$, where $p_1 < p_2 < \cdots < p_n$, e_i and f_i are nonnegative integers, $1 \le i \le n$. Then by the Unique Factorization Theorem,

$$\begin{aligned} \gcd(a, b) &= p_1^{g_1} p_2^{g_2} \cdots p_n^{g_n}, \\ \operatorname{lcm}(a, b) &= p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n}, \end{aligned}$$

where $g_i = \min(e_i, f_i)$, $h_i = \max(e_i, f_i)$, $1 \le i \le n$. Note that for any real numbers $x, y \in \mathbb{R}$,

$$\min(x, y) + \max(x, y) = x + y.$$

Thus

$$g_i + h_i = e_i + f_i, \quad 1 \le i \le n.$$

Therefore

$$\begin{aligned} ab &= p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_n^{e_n+f_n} \\ &= p_1^{g_1+h_1} p_2^{g_2+h_2} \cdots p_n^{g_n+h_n} \\ &= \gcd(a,b) \cdot \operatorname{lcm}(a,b). \end{aligned}$$

$\square$

4 Solving $ax + by = c$

Example 4.1. Find an integer solution for the equation

$$25x + 65y = 10.$$

Solution. Applying the Division Algorithm,

$$\begin{aligned} 65 &= 2 \cdot 25 + 15, \\ 25 &= 15 + 10, \\ 15 &= 10 + 5. \end{aligned}$$

Then $\gcd(25, 65) = 5$. Applying the Euclidean Algorithm,

$$\begin{aligned} 5 &= 15 - 10 \\ &= 15 - (25 - 15) \\ &= -25 + 2 \cdot 15 \\ &= -25 + 2 \cdot (65 - 2 \cdot 25) \\ &= -5 \cdot 25 + 2 \cdot 65. \end{aligned}$$

By inspection, $(x, y) = (-5, 2)$ is a solution for the equation

$$25x + 65y = 5.$$

Since $\frac{10}{5} = 2$, then $(x, y) = 2(-5, 2) = (-10, 4)$ is a solution for $25x + 65y = 10$.

Example 4.2. Find an integer solution for the equation

$$25x + 65y = 18.$$

Solution. Since $\gcd(25, 65) = 5$, if the equation has a solution, then $5 \mid (25x + 65y)$. So $5 \mid 18$ by Proposition 1.2 (c). This is a contradiction. Hence the equation has no solution.

Theorem 4.1. *The linear Diophantine equation*

$$ax + by = c,$$

has a solution if and only if $\gcd(a, b) \mid c$.

Theorem 4.2. *Let S be the set of solutions of the equation*

$$ax + by = c. \tag{1}$$

Let S_0 be the set of solutions of the homogeneous equation

$$ax + by = 0. \tag{2}$$

If $(x, y) = (u_0, v_0)$ is a solution of (2), then S is given by

$$S = \{(u_0 + s, v_0 + t) : (s, t) \in S_0\}.$$

In other words, all solutions of (1) are given by

$$\begin{cases} x = u_0 + s \\ y = v_0 + t \end{cases}, \quad (s, t) \in S_0. \tag{3}$$

Proof. Since $(x, y) = (u_0, v_0)$ is a solution of (1), then $au_0 + bv_0 = c$. For any solution $(x, y) = (s, t)$ of (2), we have $as + bt = 0$. Thus

$$a(u_0 + s) + b(v_0 + t) = (au_0 + bv_0) + (as + bt) = c.$$

This means that $(x, y) = (u_0 + s, v_0 + t)$ is a solution of (1).

Conversely, for any solution $(x, y) = (u, v)$ of (1), we have $au + bv = c$. Let $(s_0, t_0) = (u - u_0, v - v_0)$. Then

$$\begin{aligned} as_0 + bt_0 &= a(u - u_0) + b(v - v_0) \\ &= (au + bv) - (au_0 + bv_0) \\ &= c - c = 0. \end{aligned}$$

This means that (s_0, t_0) is a solution of (2). Note that

$$(u, v) = (u_0 + s_0, v_0 + t_0).$$

This shows that the solution $(x, y) = (u, v)$ is a solution of the form in (3). Our proof is finished. □

Theorem 4.3. *Let $d = \gcd(a, b)$. The solution set S_0 of*

$$ax + by = 0$$

is given by

$$S_0 = \left\{ k\left(\frac{b}{d}, -\frac{a}{d}\right) : k \in \mathbb{Z} \right\}.$$

In other words,

$$\begin{cases} x = (b/d)k \\ y = -(a/d)k \end{cases}, \quad k \in \mathbb{Z}.$$

Proof. The equation $ax + by = 0$ can be written as

$$ax = -by.$$

Write $m = ax = -by$. Then $a \mid m$ and $b \mid m$, i.e., m is a multiple of a and b. Thus $m = k \cdot \operatorname{lcm}(a, b)$ for some $k \in \mathbb{Z}$. Therefore $ax = k \cdot \operatorname{lcm}(a, b)$ implies

$$x = \frac{k \cdot \operatorname{lcm}(a, b)}{a} = \frac{kab}{da} = \frac{kb}{d}.$$

Similarly, $-by = k \cdot \operatorname{lcm}(a, b)$ implies

$$y = \frac{k \cdot \operatorname{lcm}(a, b)}{-b} = \frac{kab}{-db} = -\frac{ka}{d}.$$

□

Theorem 4.4. *Let $d = \gcd(a, b)$ and $d \mid c$. Let (u_0, v_0) be a particular solution of the equation*

$$ax + by = c.$$

The all solutions of the above equation are given by

$$\begin{cases} x = u_0 + bk/d \\ y = v_0 - ak/d \end{cases}, \quad k \in \mathbb{Z}.$$

Proof. It follows from Theorem 4.2 and Theorem 4.3. □

Example 4.3. Find all integer solutions for the equation

$$25x + 65y = 10.$$

Solution. Find $\gcd(25, 65) = 5$ and have got a special solution $(x, y) = (-10, 4)$ in a previous example. Now consider the equation $25x + 65y = 0$. Divide both sides by 5 to have,

$$5x + 13y = 0.$$

Since $\gcd(5, 13) = 1$, all solutions for the above equation are given by $(x, y) = k(-13, 5)$, $k \in \mathbb{Z}$. Thus all solutions of $25x + 65y = 10$ are given by

$$\begin{cases} x &= -10 - 13k \\ y &= \quad\quad 4 + 5k \end{cases}, \quad k \in \mathbb{Z}.$$

Example 4.4.

$$168x + 668y = 888.$$

Solution. Find $\gcd(168, 668) = 4$ by the Division Algorithm

$$\begin{aligned} 668 &= 3 \cdot 168 + 164 \\ 168 &= 164 + 4 \\ 164 &= 41 \cdot 4 \end{aligned}$$

By the Euclidean Algorithm,

$$\begin{aligned} 4 &= 168 - 164 \\ &= 168 - (668 - 3 \cdot 168) \\ &= 4 \cdot 168 + (-1) \cdot 668. \end{aligned}$$

Dividing $\frac{888}{4} = 222$, we obtain a special solution

$$(x, y) = 222(4, -1) = (888, -222)$$

Solve $168x + 668y = 0$. Dividing both sides by 4,

$$42x + 167y = 0 \quad \text{i.e.} \quad 42x = -167y.$$

The general solutions for $168x + 668y = 0$ are given by

$$(x, y) = k(167, -42), \quad k \in \mathbb{Z}.$$

The general solutions for $168x + 668y = 888$ are given by

$$(x, y) = (888, -222) + k(167, -42), \quad k \in \mathbb{Z}.$$

$$\text{i.e.} \left\{ \begin{array}{rcrr} x &=& 888 & +167k \\ y &=& -222 & -42k \end{array} \right., \quad k \in \mathbb{Z}.$$

5 Modulo Integers

Let n be a fixed positive integer. Two integers a and b are said to be **congruent** modulo n, written

$$a \equiv b \pmod{n}$$

and read "a **equals** b **modulo** n," if $n \mid (b-a)$.

For all $k, l \in \mathbb{Z}$, $a \equiv b \pmod{n}$ is equivalent to

$$a + kn \equiv b + ln \pmod{n}.$$

In fact, the difference

$$(b + ln) - (a + kn) = (b - a) + (l - k)n$$

is a multiple of n if and only if $b - a$ is a multiple of n.

Example 5.1.

$$3 \equiv 5 \pmod{2}, \quad 368 \equiv 168 \pmod{8},$$

$$-8 \equiv 10 \pmod{9}, \quad 3 \not\equiv 5 \pmod{3},$$

$$368 \not\equiv 268 \pmod{8}, \quad -8 \not\equiv 18 \pmod{9}.$$

Proposition 5.1. *Let n be a fixed positive integer. If*

$$a_1 \equiv b_1 \pmod{n}, \quad a_2 \equiv b_2 \pmod{n},$$

then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n},$$
$$a_1 - a_2 \equiv b_1 - b_2 \pmod{n},$$

$$a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

If $a \equiv b \pmod{n}$, $d \mid n$, *then*

$$a \equiv b \pmod{d}.$$

Proof. Since $a_1 \equiv b_1 \pmod{n}$, $a_2 \equiv b_2 \pmod{n}$, there are integers k_1, k_2 such that

$$b_1 - a_1 = k_1 n, \quad b_2 - a_2 = k_2 n.$$

Then

$$(b_1 + b_2) - (a_1 + a_2) = (k_1 + k_2)n;$$
$$(b_2 - b_1) - (a_1 - a_2) = (k_1 - k_2)n;$$

$$\begin{aligned} b_1 b_2 - a_1 a_2 &= b_1 b_2 - b_1 a_2 + b_1 a_2 - a_1 a_2 \\ &= b_1(b_2 - a_2) + (b_1 - a_1)a_2 \\ &= bk'n + kna' \\ &= (b_1 k_2 + a_2 k_1)n. \end{aligned}$$

Thus

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n};$$
$$a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

If $d \mid n$, then $n = dl$ for some $l \in \mathbb{Z}$. Thus

$$b - a = kn = (kl)d.$$

Therefore, $a \equiv b \pmod{d}$. $\square$

Example 5.2.

$$6 \equiv 14 \pmod 8 \implies 2 \cdot 6 \equiv 2 \cdot 14 \pmod 8;$$

$$6 \equiv 14 \pmod 8 \iff \frac{6}{2} \equiv \frac{14}{2} \left(\mathrm{mod}\ \frac{8}{2}\right);$$

However,

$$2 \cdot 3 \equiv 2 \cdot 7 \pmod 8 \not\Longrightarrow 3 \equiv 7 \pmod 8.$$

In fact,

$$3 \not\equiv 7 \pmod 8.$$

Theorem 5.2. *Let $c \mid a$, $c \mid b$, and $c \mid n$. Then*

$$a \equiv b \pmod n \quad \iff \quad \frac{a}{c} \equiv \frac{b}{c} \left(\mathrm{mod}\ \frac{n}{c}\right).$$

Proof. Write $a = ca_1$, $b = cb_1$, $n = cn_1$. Then

$$\begin{aligned} a \equiv b \pmod n &\iff b - a = kn \quad \text{for an integer } k \\ &\iff c(b_1 - a_1) = kcn_1 \\ &\iff b/c - a/c = b_1 - a_1 = kn_1 \\ &\iff a/c \equiv b/c \pmod{n/c}. \end{aligned}$$

□

Theorem 5.3.

$$a \equiv b \pmod m, \quad a \equiv b \pmod n,$$
$$\iff$$
$$a \equiv b \pmod{\mathrm{lcm}(m, n)}.$$

In particular,

$$\gcd(m, n) = 1 \quad \iff \quad a \equiv b \pmod{mn}.$$

Proof. Write $l = \mathrm{lcm}(m, n)$. If $a \equiv b \pmod m$, $a \equiv b \pmod n$, then $m \mid (b - a)$ and $n \mid (b - a)$. Thus $l \mid (b - a)$, i.e., $a \equiv b \pmod l$.

Conversely, if $a \equiv b \pmod l$, then $l \mid (b - a)$. Since $m \mid l$, $n \mid l$, we have $m \mid (b - a)$, $n \mid (b - a)$. Thus $a \equiv b \pmod m$, $a \equiv b \pmod n$.

In particular, if $\gcd(m, n) = 1$, then $l = mn$. □

Definition 5.4. An integer a is called **invertible** modulo n if there exists an integer b such that

$$ab \equiv 1 \pmod n.$$

If so, b is called the **inverse** of a modulo n.

Proposition 5.5. *An integer a is invertible modulo n if and only if* $\gcd(a, n) = 1$

Proof. "$\Rightarrow$": If a is invertible modulo n, say its inverse is b, then exists an integer k such that $ab = 1 + kn$, i.e.,

$$1 = ab - kn.$$

Thus $\gcd(a, n)$ divides 1. Hence $\gcd(a, n) = 1$.

"$\Leftarrow$": By the Euclidean Algorithm, there exist integers u, v such that $1 = au + nv$. Then $au \equiv 1 \pmod n$. □

Example 5.3. The invertible integers modulo 12 are the following numbers

$$1, 5, 7, 11.$$

Numbers $0, 2, 3, 4, 6, 8, 9, 10$ are not invertible modulo 12.

Theorem 5.6. *Let* $\gcd(c, n) = 1$. *Then*

$$a \equiv b \pmod{n} \iff ca \equiv cb \pmod{n}$$

Proof. By the Euclidean Algorithm, there are integers u, v such that

$$1 = cu + nv.$$

Then $1 \equiv cu \pmod{n}$; i.e., a and u are inverses of each other modulo n

"$\Rightarrow$": $c \equiv c \pmod{n}$ and $a \equiv b \pmod{n}$ imply

$$ca \equiv cb \pmod{n}.$$

This true without $\gcd(c, n) = 1$.

"$\Leftarrow$": $ca \equiv cb \pmod{n}$ and $u \equiv u \pmod{n}$ imply that

$$uca \equiv ucb \pmod{n}.$$

Replace $uc = 1 - vn$; we have $a - avn \equiv b - bvn \pmod{n}$. This means $a \equiv b \pmod{n}$. □

Example 5.4. Find the inverse modulo 15 for each of the numbers 2, 4, 7, 8, 11, 13.

Solution. Since $2 \cdot 8 \equiv 1 \pmod{15}$, $4 \cdot 4 \equiv 1 \pmod{15}$. Then 2 and 8 are inverses of each other; 4 is the inverse of itself.

Write $15 = 2 \cdot 7 + 1$. Then $15 - 2 \cdot 7 = 1$. Thus $-2 \cdot 7 \equiv 1 \pmod{15}$. The inverse of 7 is -2. Since $-2 \equiv 13 \pmod{15}$, the inverse of 7 is also 13. In fact,

$$7 \cdot 13 \equiv 1 \pmod{15}.$$

Similarly, $15 = 11 + 4$, $11 = 2 \cdot 4 + 3$, $4 = 3 + 1$, then

$$\begin{aligned} 1 &= 4 - 3 = 4 - (11 - 2 \cdot 4) \\ &= 3 \cdot 4 - 11 = 3 \cdot (15 - 11) - 11 \\ &= 15 - 4 \cdot 11. \end{aligned}$$

Thus the inverse of 11 is -4. Since $-4 \equiv 11 \pmod{15}$, the inverse of 11 is also itself, i.e., $11 \cdot 11 \equiv 1 \pmod{15}$.

6 Solving $ax \equiv b \pmod{n}$

Theorem 6.1. *The congruence equation*

$$ax \equiv b \pmod{n}$$

has a solution if and only if $\gcd(a, n)$ *divides* b.

Proof. Let $d = \gcd(a, n)$. The congruence equation has a solution if and only if there exist integers x and k such that $b = ax + kn$. This is equivalent to $d \mid b$. $\square$

Remark. For all $k, l \in \mathbb{Z}$, we have

$$ax \equiv b \pmod{n} \iff (a + kn)x \equiv b + ln \pmod{n}.$$

In fact, the difference

$$(b + ln) - (a + kn)x = (b - ax) + (l - kx)n$$

is a multiple of n if and only if $b - ax$ is a multiple of n.

Theorem 6.2. *Let* $\gcd(a, n) = 1$. *Then there exists an integer* u *such that* $au \equiv 1 \pmod{n}$*; the solutions for the equation* $ax \equiv b \pmod{n}$ *are given by*

$$x \equiv ub \pmod{n}.$$

Proof. Since $\gcd(a, n) = 1$, there exist $u, v \in \mathbb{Z}$ such that $1 = au + nv$. So $1 \equiv au \pmod{n}$, i.e., $au \equiv 1 \pmod{n}$. Since u is invertible modulo n, we have

$$ax \equiv b \pmod{n} \Longleftrightarrow uax \equiv ub \pmod{n}.$$

Since $au = 1 - nv$, then $uax = (1 - nv)x = x - vxn$. Thus

$$ax \equiv b \pmod{n} \Longleftrightarrow x - vxn \equiv ub \pmod{n}.$$

Therefore

$$ax \equiv b \pmod{n} \Longleftrightarrow x \equiv ub \pmod{n}.$$

$\square$

Example 6.1. Find all integers x for

$$9x \equiv 27 \pmod{15}.$$

Solution. Find $\gcd(9, 15) = 3$. Dividing both sides by 3,

$$3x \equiv 9 \pmod{5} \quad \Longleftrightarrow \quad 3x \equiv 4 \pmod{5}.$$

Since $\gcd(3, 5) = 1$, the integer 3 is invertible and its inverse is 2. Multiplying 2 to both sides,

$$6x \equiv 8 \pmod{5}.$$

Since $6 \equiv 1 \pmod{5}$, $8 \equiv 3 \pmod{5}$, then

$$x \equiv 3 \pmod{5}.$$

In other words,

$$x = 3 + 5k, \quad k \in \mathbb{Z}.$$

Example 6.2. Solve the equation $668x \equiv 888 \pmod{168}$.

Solution. Find $\gcd(668, 168) = 4$, then

$$167x \equiv 222 \pmod{42}.$$

By the Division Algorithm,

$$167 = 3 \cdot 42 + 41; \quad 42 = 41 + 1.$$

By the Euclidean Algorithm,

$$1 = 42 - 41 = 42 - (167 - 3 \cdot 42) = 4 \cdot 42 - 167.$$

Then $-167 \equiv 1 \pmod{42}$; the inverse of 167 is -1. Multiplying -1 to both sides, we have $x \equiv -222 \pmod{42}$. Thus

$$x \equiv -12 \pmod{42} \quad \text{or} \quad x \equiv 30 \pmod{42}; \quad \text{i.e.}$$

$$x = 30 + 42k, \quad k \in \mathbb{Z}.$$

Algorithm for solving $ax \equiv b \pmod{n}$.

Step 1. Find $d = \gcd(a, n)$ by the Division Algorithm.

Step 2. If $d = 1$, apply the Euclidean Algorithm to find $u, v \in \mathbb{Z}$ such that $1 = au + nv$.

Step 3. Do the multiplication $uax \equiv ub \pmod{n}$. All solutions $x \equiv ub \pmod{n}$ are obtained. Stop.

Step 4. If $d > 1$, check whether $d \mid b$. If $d \nmid b$, there is no solution. Stop. If $d \mid b$, do the division

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\operatorname{mod} \frac{n}{d}\right).$$

Rewrite a/d as a, b/d as b, and n/d as n. Go to Step 1.

Proof. Since $1 = au + nv$, we have $au \equiv 1 \pmod{n}$. This means that a and u are inverses of each other modulo n. So

$$ax \equiv b \pmod{n} \iff uax \equiv ub \pmod{n}.$$

Since $ua = 1 - vn$, then $uax = (1 - vn)x = x - vxn$. Thus

$$uax \equiv ub \pmod{n} \iff x \equiv ub \pmod{n}.$$

$\square$

Example 6.3. Solve the equation $245x \equiv 49 \pmod{56}$.

Solution. Applying the Division Algorithm,

$$\begin{aligned} 245 &= 4 \cdot 56 + 21 \\ 56 &= 2 \cdot 21 + 14 \\ 21 &= 14 + 7 \end{aligned}$$

Applying the Euclidean Algorithm,

$$\begin{aligned} 7 &= 21 - 14 = 21 - (56 - 2 \cdot 21) \\ &= 3 \cdot 21 - 56 = 3 \cdot (245 - 4 \cdot 56) - 56 \\ &= 3 \cdot 245 - 13 \cdot 56 \end{aligned}$$

Dividing both sides by 7, we have

$$1 = 3 \cdot 35 - 13 \cdot 8.$$

Thus $3 \cdot 35 \equiv 1 \pmod{8}$. Dividing the original equation by 7, we have $35x \equiv 7 \pmod{8}$. Multiplying 3 to both sides, we obtain solutions

$$x \equiv 21 \equiv 5 \pmod{8}$$

7 Chinese Remainder Theorem

Example 7.1. Solve the system

$$\begin{cases} x \equiv 0 \pmod{n_1} \\ x \equiv 0 \pmod{n_2} \end{cases}$$

Solution. By definition of solution, x is a common multiple of n_1 and n_2. So x is a multiple of $\operatorname{lcm}(n_1, n_2)$. Thus the system is equivalent to

$$x \equiv 0 \pmod{\operatorname{lcm}(n_1, n_2)}.$$

Theorem 7.1. *Let S be the solution set of the system*

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \end{cases} \tag{4}$$

Let S_0 be the solution set of the homogeneous system

$$\begin{cases} a_1 x \equiv 0 \pmod{n_1} \\ a_2 x \equiv 0 \pmod{n_2} \end{cases} \tag{5}$$

If $x = x_0$ is a solution of (4), then all solutions of (4) are given by

$$x = x_0 + s, \quad s \in S_0. \tag{6}$$

Proof. We first show that $x = x_0 + s$, where $s \in S_0$, are indeed solutions of (4). In fact, since x_0 is a solution for (4) and s is a solution for (5), we have

$$\begin{cases} a_1 x_0 \equiv b_1 \pmod{n_1} \\ a_2 x_0 \equiv b_2 \pmod{n_2} \end{cases}, \quad \begin{cases} a_1 s \equiv 0 \pmod{n_1} \\ a_2 s \equiv 0 \pmod{n_2} \end{cases};$$

i.e., n_1 divides $(b_1 - a_1x_0)$ and a_1s; n_2 divides $(b_2 - a_2x_0)$ and a_2s. Then n_1 divides $[(b_1 - a_1x_0) - a_1s]$, and n_2 divides $[(b_2 - a_2x_0) - a_2s]$; i.e., n_1 divides $[b_1 - a_1(x_0 + s)]$, and n_2 divides $[b_2 - a_2(x_0 + s)]$. This means that $x = x_0 + s$ is a solution of (4).

Conversely, let $x = t$ be any solution of (4). We will see that $s_0 = t - x_0$ is a solution of (5). Hence the solution $t = x_0 + s_0$ is of the form in (6). $\square$

Algorithm for solving the system

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases} \tag{7}$$

Step 1. Reduced the system to the form

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases} \tag{8}$$

Step 2. Set $x = c_1 + ym_1 = c_2 + zm_2$, where $y, z \in \mathbb{Z}$. Find a solution $(y, z) = (y_0, z_0)$ for the equation

$$m_1y - m_2z = c_2 - c_1.$$

Consequently, $x_0 = c_1 + m_1y_0 = c_2 + m_2z_0$.

Step 3. Set $m = \operatorname{lcm}(m_1, m_2)$. The system (7) becomes

$$x \equiv x_0 \pmod{m}.$$

Proof. It follows from Theorem 7.1. $\square$

Example 7.2. Solve the system

$$\begin{cases} 10x \equiv 6 \pmod{4} \\ 12x \equiv 30 \pmod{21} \end{cases}$$

Solution. Applying the Division Algorithm,

$$\gcd(10,4) = 2, \quad \gcd(12,21) = 3.$$

Dividing the 1st equation by 2 and the second equation by 3,

$$\begin{cases} 5x \equiv 3 \pmod{2} \\ 4x \equiv 10 \pmod{7} \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 \pmod{2} \\ 4x \equiv 3 \pmod{7} \end{cases}$$

The system is equivalent to

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 6 \pmod{7} \end{cases}$$

Set $x = 1 + 2y = 6 + 7z$, $y, z \in \mathbb{Z}$. Then

$$2y - 7z = 5.$$

Applying the Division Algorithm, $7 = 3 \cdot 2 + 1$. Applying the Euclidean Algorithm, $1 = -3 \cdot 2 + 7$. Then $5 = -15 \cdot 2 + 5 \cdot 7$. We obtain a solution $(y_0, z_0) = (-15, -5)$. Thus

$$x_0 = 1 + 2y_0 = 6 + 7z_0 = -29$$

is a special solution. The general solution for

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 0 \pmod{7} \end{cases}$$

is $x \equiv 0 \pmod{14}$. Hence the solution is given by

$$x \equiv -29 \equiv -1 \equiv 13 \pmod{14}$$

Example 7.3. Solve the system

$$\begin{cases} 12x \equiv 96 \pmod{20} \\ 20x \equiv 70 \pmod{30} \end{cases}$$

Solution. Applying the Division Algorithm to find,

$$\gcd(12, 20) = 4, \quad \gcd(20, 30) = 10.$$

Then

$$\begin{cases} 3x \equiv 24 \pmod 5 \\ 2x \equiv 7 \pmod 3 \end{cases}$$

Applying the Euclidean Algorithm,

$$\gcd(3, 5) = 1 = 2 \cdot 3 - 1 \cdot 5.$$

Then $2 \cdot 3 \equiv 1 \pmod 5$. Similarly,

$$\gcd(2, 3) = 1 = -1 \cdot 2 + 1 \cdot 3$$

and $-1 \cdot 2 = 1 \pmod 3$. (Equivalently, $2 \cdot 2 \equiv 1 \pmod 3$.) Then, 2 is the inverse of 3 modulo 5; -1 or 2 is the inverse of 2 modulo 3. Thus

$$\begin{cases} 2 \cdot 3x \equiv 2 \cdot 24 \pmod 5 \\ -1 \cdot 2x \equiv -1 \cdot 7 \pmod 3 \end{cases}$$

$$\begin{cases} x \equiv 48 \equiv 3 \pmod 5 \\ x \equiv -7 \equiv 2 \pmod 3 \end{cases}$$

Set $x = 3 + 5y = 2 + 3z$, where $y, z \in \mathbb{Z}$. That is,

$$5y - 3z = -1.$$

We find a special solution $(y_0, z_0) = (1, 2)$. So $x_0 = 3 + 5y_0 = 2 + 3z_0 = 8$. Thus the original system is equivalent to

$$x \equiv 8 \pmod{15}$$

and all solutions are given by

$$x = 8 + 15k, \quad k \in \mathbb{Z}.$$

Example 7.4. Find all integer solutions for the system

$$\begin{cases} x \equiv 486 \pmod{186} \\ x \equiv 386 \pmod{286} \end{cases}$$

Solution. The system can be reduced to

$$\begin{cases} x \equiv 114 \pmod{186} \\ x \equiv 100 \pmod{286} \end{cases}$$

Set $x = 114 + 186y = 100 + 286z$, i.e.,

$$186y - 286z = -14.$$

Applying the Division Algorithm,

$$\begin{aligned} 286 &= 186 + 100, \\ 186 &= 100 + 86, \\ 100 &= 86 + 14, \\ 86 &= 6 \cdot 14 + 2. \end{aligned}$$

Then $\gcd(186, 286) = 2$. Applying the Euclidean Algorithm,

$$\begin{aligned} 2 &= 86 - 6 \cdot 14 \\ &= 86 - 6(100 - 86) = 7 \cdot 86 - 6 \cdot 100 \\ &= 7(186 - 100) - 6 \cdot 100 = 7 \cdot 186 - 13 \cdot 100 \\ &= 7 \cdot 186 - 13(286 - 186) = 20 \cdot 186 - 13 \cdot 286. \end{aligned}$$

Note that $\frac{-14}{2} = -7$. So we get a special solution

$$(y_0, z_0) = -7(20, 13) = (-140, -91).$$

Thus $x_0 = 114 + 186y_0 = 100 + 286z_0 = -25926$. Note that $\operatorname{lcm}(186, 286) = 26598$. The general solutions are given by

$$x \equiv -25926 \equiv 672 \pmod{26598}.$$

Theorem 7.2 (Chinese Remainder Theorem). *Let $n_1, n_2, \ldots, n_k \in \mathbb{P}$. If $\gcd(n_i, n_j) = 1$ for all $i \neq j$, then the system of congruence equations*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

has a unique solution modulo $n_1 n_2 \cdots n_k$.

Thinking Problem. In the Chinese Remainder Theorem, if

$$\gcd(n_i, n_j) = 1,$$

is not satisfied, does the system have solutions? Assuming it has solutions, are the solutions unique modulo some integers?

8 Important Facts

1. $a \equiv b \pmod{n} \iff a + kn \equiv b + ln \pmod{n}$ for all $k, l \in \mathbb{Z}$.
2. If $c \mid a$, $c \mid b$, $c \mid n$, then
$$a \equiv b \pmod{n} \quad \iff \quad a/c \equiv b/c \pmod{n/c}.$$
3. An integer a is called **invertible** modulo n if there exists an integer b such that
$$ab \equiv 1 \pmod{n}.$$

If so, b is called the **inverse** of a modulo n.

4. An integer a is invertible modulo $n \iff \gcd(a, n) = 1$.
5. If $\gcd(c, n) = 1$, then
$$a \equiv b \pmod{n} \iff ca \equiv cb \pmod{n}.$$
6. Equation $ax \equiv b \pmod{n}$ has solution $\iff \gcd(a, n) \mid b$.
7. For all $k, l \in \mathbb{Z}$,
$$ax \equiv b \pmod{n} \iff (a + kn)x \equiv b + ln \pmod{n}.$$