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

$$a \nmid b.$$

Obviously, any integer $n$ has divisors $\pm 1$ and $\pm n$, called the trivial divisors of $n$. If $a$ is a divisor of $n$, so is $-a$. Positive divisors of $n$ other than the trivial divisors are called nontrivial divisors.

Note that 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 follows:


**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 \( k \in \mathbb{P} \). Then, either \( p \le q \) or \( q \le p \). Assume \( p \le q \). We have

\[ p^2 \le pqk = n. \text{ Thus } p \le \sqrt{n}. \]

\[ \square \]

**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 \( \sqrt{143} < 12 \). For \( i = 2, 3, 5, 7, 11 \), check whether \( i \) divides 143. We find \( 11 \mid 143 \). So 143 is a composite number.

Is 157 a prime?
Since \( \sqrt{157} < 13 \) and for each \( i = 2, 3, 5, 7, 11 \), \( i \) is not a factor of 157, we see that 157 has no prime factor less or equal to \( \sqrt{157} \). So 157 is not a composite, i.e., 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 \( b \mid c \), then \( a \mid c \).

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

**Proof.** (a) Let \( b = q_1a \) and \( a = q_2b \) for some integers \( q_1 \) and \( q_2 \). Then

\[ b = q_1q_2b. \]
Dividing both sides by $b$, we have $q_1q_2 = 1$. It follows that $q_1 = q_2 = \pm 1$. Thus $b = \pm a$.

(b) Let $b = q_1a$ and $c = q_2b$ for some integers $q_1$ and $q_2$. Then $c = q_1q_2a$, that is, $a | c$.

(c) Let $b = q_1a$ and $c = q_2b$ for $q_1, q_2 \in \mathbb{Z}$. Then for $x, y \in \mathbb{Z}$,

$$bx + cy = (q_1x + q_2y)a,$$

that is, $a | (bx + cy)$. $\square$

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

**Proof.** Suppose there are finitely many primes, say,

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

Then the integer

$$a = p_1p_2 \cdots p_k + 1$$

is not divisible by any of the primes $p_1, p_2, \ldots, p_k$ because the remainders of $a$ dividing by $p_1, p_2, \ldots, p_k$ respectively are always 1. This means that $a$ has no prime factors. By definition of primes, the integer $a$ must be a prime, and this prime is larger than all primes $p_1, p_2, \ldots, p_k$, a contradiction. $\square$

**Theorem 1.4 (Division Algorithm).** For any integers $a$ and $b$, where $a > 0$, there are unique integers $q$ and $r$ such that

$$b = qa + r, \quad 0 \leq r < a.$$
Proof. Consider the set \( S = \{ b - ta \geq 0 \mid t \in \mathbb{Z} \} \). Obviously, \( S \) is nonempty and is bounded below. Then \( S \) has the unique minimum integer \( r \), i.e., there is an unique integer \( q \) such that \( b - qa = r \). We claim that \( r < a \). Suppose \( r \geq a \), then \( b - (q+1)a = r - a \geq 0 \) shows that \( r - a \) is an element of \( S \). This is contrary to that \( r \) is the minimum element of \( S \). \qed

Example 1.2. For integers \( a = 21 \) and \( b = -358 \), we have
\[-368 = -18 \cdot 21 + 10, \quad q = -18, \quad r = 10.\]

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 \( c \mid a \) and \( c \mid b \). Clearly, there are finitely many common divisors for \( a \) and \( b \); the very greatest one is called the greatest common divisor of \( a \) and \( b \), and is denoted by \( \gcd(a, b) \). For convenience, we assume \( \gcd(0, 0) = 0 \). Two integers \( a \) and \( b \) are called coprime (or relatively prime) if \( \gcd(a, b) = 1 \).

Theorem 2.1. Let \( d \) be the greatest common divisor of integers \( a \) and \( b \), i.e., \( d = \gcd(a, b) \). Then there exist integers \( x \) and \( y \) such that
\[ d = ax + by. \]

Proof. It is obviously true when \( a = b = 0 \). Assume that \( a \) and \( b \) are not simultaneously zero. We consider the set
\[ S = \{ au + bv \mid u, v \in \mathbb{Z} \} \]
and the set \( S_+ = S \cap \mathbb{P} \).

For \( u = a, v = b \), we have \( au + bv = a^2 + b^2 > 0 \). Obviously, \( S \) is nonempty and bounded below. Let \( s \) be the smallest integer in \( S_+ \). Write

\[
s = au_0 + bv_0
\]

for some \( u_0, v_0 \in \mathbb{Z} \). We claim that \( d = s \).

Clearly, \( d \) divides every integer in \( S \) because \( d|a \) and \( d|b \). In particular, \( d|s \). We then have \( d \leq s \). To show \( s \leq d \), we claim that \( s \) divides every integer in \( S \). In fact, for any \( au + bv \in S \) with \( u, v \in \mathbb{Z} \), let

\[
au + bv = qs + r, \quad 0 \leq r < s.
\]

Then \( r = a(u - qv_0) + b(v - qu_0) \in S \). If \( r \) was positive, then \( r \in S_+ \) and \( s \) could not be the smallest integer in \( S_+ \). So \( r = 0 \). Thus \( s|(au + bv) \). In particular, taking \((u, v) = (0, 1)\) and \((u, v) = (1, 0)\), we see that \( s|a \) and \( s|b \). So \( s \) is a positive common divisor of \( a \) and \( b \). By definition of \( \text{gcd} \), \( s \leq d \). \( \square \)

**Theorem 2.2.** Let \( a, b, d \in \mathbb{P} \). Then \( d = \text{gcd}(a, b) \) if and only if

1. \( d|a, \ d|b \);
2. If \( c|a, \ c|b \), then \( c|d \).

**Proof.** “\( \Rightarrow \):” By definition, \( \text{gcd} \) is a common divisor of \( a \) and \( b \), so we have (1). By Theorem 2.1, there exist integers \( x, y \) such that

\[
d = ax + by.
\]
If \( c \mid a, \ c \mid b \), then \( c \mid (ax + by) \), i.e., \( c \mid d \).

\[ \iff \]

(1) indicates that \( d \) is a common divisor of \( a \) and \( b \). Let \( c \) be positive common divisor \( c \) of \( a \) and \( b \). We have \( c \mid d \) by (2). Thus \( c \leq d \). So \( d \) is the greatest among all common divisors of \( a \) and \( b \). \( \square \)

**Theorem 2.3.** For integers \( a, b, q, \) and \( r \), if

\[ b = qa + r, \]

then

\[ \gcd(a, b) = \gcd(a, r). \]

**Proof.** Let \( d_1 = \gcd(a, b) \), \( d_2 = \gcd(a, r) \). Since \( r = b - qa \), we have \( d_1 \mid r \). This means that \( d_1 \) is a common divisor of \( a \) and \( r \). Thus \( d_1 \leq d_2 \). Since \( b = qa + r \), we have \( d_2 \mid b \). This means that \( d_2 \) is a common divisor of \( a \) and \( b \). Hence, \( d_2 \leq d_1 \). Therefore \( d_1 = d_2 \). \( \square \)

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

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

\[
egin{align*}
3627 &= 12 \cdot 297 + 63, & \gcd(297, 3627) &= \gcd(63, 297) \\
297 &= 4 \cdot 63 + 45, & &= \gcd(45, 63) \\
63 &= 1 \cdot 45 + 18, & &= \gcd(18, 45) \\
45 &= 2 \cdot 18 + 9, & &= \gcd(9, 18) \\
18 &= 2 \cdot 9; & &= 9.
\end{align*}
\]
The procedure to calculate \( \gcd(297, 3627) \) applies to any pair of positive integers. Let \( a \) be a positive integer and \( b \) a nonnegative integer. Repeating the Division Algorithm will produce finite sequences of nonnegative integers \( q_i \) and \( r_i \) such that

\[
\begin{align*}
b &= q_0a + r_0, & 0 \leq r_0 < a, \\
a &= q_1r_0 + r_1, & 0 \leq r_1 < r_0, \\
r_0 &= q_2r_1 + r_2, & 0 \leq r_2 < r_1, \\
r_1 &= q_3r_2 + r_3, & 0 \leq r_3 < r_2, \\
&\vdots \\
r_{k-2} &= q_kr_{k-1} + r_k, & 0 \leq r_k < r_{k-1}, \\
r_{k-1} &= q_{k+1}r_k + r_{k+1}, & r_{k+1} = 0.
\end{align*}
\]

Notice that the sequence \( \{r_i\} \) is strictly decreasing; it ends eventually to 0 at some step, say, \( r_{k+1} = 0 \) for the first time. Then \( r_i \neq 0 \) for all \( 0 \leq i \leq k \). Reverse the sequence \( \{r_i\}_{i=0}^k \) and make substitutions as follows:

\[
\begin{align*}
\gcd(a, b) &= r_k, \\
r_k &= r_{k-2} - q_kr_{k-1}, \\
r_{k-1} &= r_{k-3} - q_{k-1}r_{k-2}, \\
&\vdots \\
r_1 &= a - q_1r_0, \\
r_0 &= b - q_0a.
\end{align*}
\]

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**.
Example 2.2. The greatest common divisor of 297 and 3627, written as an integral linear combination of 297 and 3627, can be obtained as follows:

\[
\text{gcd}(297, 3627) = 45 - 2 \cdot 18 \\
= 45 - 2(63 - 45) \\
= 3 \cdot 45 - 2 \cdot 63 \\
= 3(297 - 4 \cdot 63) - 2 \cdot 63 \\
= 3 \cdot 297 - 14 \cdot 63 \\
= 3 \cdot 297 - 14(3627 - 12 \cdot 297) \\
= 171 \cdot 297 - 14 \cdot 3627.
\]

Proposition 2.4. Let \(a, b, c \in \mathbb{Z}\). If \(a \mid bc, \ \text{gcd}(a, b) = 1\), then \(a \mid c\).

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

\[
c = 1 \cdot c = (ax + by)c = acx + bc y.
\]

Since \(a \mid ac\) and \(a \mid bc\), thus \(a \mid c\). \(\square\)

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. If \(a\) has only the trivial divisors, then \(a\) itself is a prime, and it obviously has unique factorization. If \(a\) has some non-trivial divisors, then

\[
a = bc
\]
for some positive integers $b$ and $c$ other than 1 and $a$. Obviously, $b < a$ and $c < a$. By induction, the positive integers $b$ and $c$ have factorizations into primes. Consequently, $a$ has a factorization into primes.

Let $a = q_1^{f_1} q_2^{f_2} \cdots a_n^{f_n}$ be another 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 $p_1 \mid q_3^{f_3} \cdots a_n^{f_n}$. Repeating the argument, we finally obtain that $p_1 \mid q_n^{f_n}$, which is contrary to $\gcd(p_1, q_n^{f_n}) = 1$. We thus conclude that $p_1 \geq q_1$. Similarly, $p_1 \leq q_1$. Hence $p_1 = q_1$. Next we claim that $e_1 = f_1$.

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 $p_1 \mid p_2^{e_2} \cdots p_m^{e_m}$. If $m = 1$, it would imply that $p_1$ divides 1, which is impossible because $p_1$ is a prime. If $m \geq 2$, note that $\gcd(p_1, p_i) = 1$ and so $\gcd(p_1, p_i^{e_i}) = 1$ for all $2 \leq i \leq m$; by the same token of applying Proposition 2.4 repeatedly, we have $p_1 \mid p_m^{e_m}$, which is contrary to $\gcd(p_1, p_m^{e_m}) =$
1. This means that we must have \( e_1 \geq f_1 \). Similarly, \( e_1 \leq f_1 \). Hence \( e_1 = f_1 \).

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, \( m \leq n \). Hence we have \( m = n \). By induction on \( m = n \), we obtain that \( e_2 = f_2, \ldots, e_m = f_m \).

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 \( b \mid m \). The smallest integer among the common multiples of \( a \) and \( b \) is called the least common multiple of \( a \) and \( b \), and is denoted by \( \text{lcm}(a, b) \).

**Proposition 3.1.** For any nonnegative integers \( a \) and \( b \),

\[
ab = \gcd(a, b) \text{lcm}(a, b).
\]

**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, \( 1 \leq i \leq n \). Then by the Unique Factorization Theorem,

\[
\gcd(a, b) = p_1^{g_1} p_2^{g_2} \cdots p_n^{g_n},
\]

\[
\text{lcm}(a, b) = p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n},
\]

10
where \( g_i = \min(e_i, f_i) \) and \( h_i = \max(e_i, f_i) \) for all \( 1 \leq i \leq n \). It is clear that

\[
ab = p_1^{g_1+h_1} p_2^{g_2+h_2} \cdots p_n^{g_n+h_n},
\]

and \( g_i + h_i = e_i + f_i \) for all \( 1 \leq i \leq n \). \( \square \)

**Proposition 3.2.** An integer \( m \) is the least common multiple of integers \( a \) and \( b \) if and only if

(a) \( a \mid m, b \mid m \);

(b) if \( a \mid n, b \mid n \), then \( m \mid n \).

**Proof.** By the Unique Factorization Theorem. \( \square \)

**Example 3.1.** Find all integer solutions for the linear equation \( 25x + 65y = 10 \).

**Solution:** Applying the Division Algorithm,

\[
\begin{align*}
65 &= 2 \cdot 25 + 15, \\
25 &= 15 + 10, \\
15 &= 10 + 5.
\end{align*}
\]

Applying the Euclidean Algorithm,

\[
\begin{align*}
gcd(25, 65) &= 15 - 10 \\
&= 15 - (25 - 15) \\
&= -25 + 2 \cdot 15 \\
&= -25 + 2 \cdot (65 - 2 \cdot 25) \\
&= -5 \cdot 25 + 2 \cdot 65.
\end{align*}
\]
Thus the integer solutions are given by
\[
\begin{align*}
x &= 2(-5) + 13k = -10 + 13k \\
y &= 2 \cdot 2 - 5k = 4 - 5k,
\end{align*}
k \in \mathbb{Z}.
\]

**Exercise 1.** Let \( S_c \) be the solution set of the linear Diophantine equation
\[ ax + by = c, \]
i.e., \( S_c = \{(x, y) \in \mathbb{Z}^2 | ax + by = c\} \). Show that, if \( S_c \neq \emptyset \), then there is a bijection \( f : S_0 \longrightarrow S_c \), where \( S_0 = \{(x, y) \in \mathbb{Z}^2 | ax + by = 0\} \).

Let \((x, y) = (u, v)\) be a particular solution for \( ax + by = c \). Then \( f \) can be given by
\[ f(x, y) = (u + x, v + y), \quad (x, y) \in S_0. \]
The function \( f \) has the inverse \( f^{-1} : S_c \longrightarrow S_0 \), given by
\[ f^{-1}(x, y) = (x - u, y - v), \quad (x, y) \in S_c. \]

**Theorem 3.3.** Let \( a, b \in \mathbb{Z} \), not simultaneously zero, \( d = \gcd(a, b) \). Then the linear Diophantine equation
\[ ax + by = c \]
has an integer solution if and only if \( d | c \). Moreover, if \((x, y) = (u, v)\) is a particular solution, then all solutions are given by
\[
\begin{align*}
x &= u + \frac{bk}{\gcd(a, b)} \\
y &= v - \frac{ak}{\gcd(a, b)},
\end{align*}
k \in \mathbb{Z}.
Proof. It is clear that \((x, y) = (u, v) + \frac{1}{d}(kb, -ka)\) are integer solutions. We only need to show that all integer solutions for the equation

\[ ax + by = 0. \]

Write the equation as

\[ ax = -by. \]

We have \(b \mid ax\) and \(a \mid by\). This means that \(ax\) and \(by\) are both common multiples of \(a\) and \(b\). Thus \(\text{lcm}(a, b)\) is a common divisor of \(ax\) and \(by\). Let \(ax = k\text{lcm}(a, b)\) for some \(k \in \mathbb{Z}\). Then

\[
\begin{align*}
\begin{cases}
ax &= k\text{lcm}(a, b) \\
by &= -k\text{lcm}(a, b)
\end{cases} \quad k \in \mathbb{Z}.
\end{align*}
\]

Thus

\[
\begin{align*}
\begin{cases}
x &= \frac{k\text{lcm}(a, b)}{a} = \frac{bk}{\gcd(a, b)} \\
y &= -\frac{k\text{lcm}(a, b)}{b} = -\frac{ak}{\gcd(a, b)}.
\end{cases}
\end{align*}
\]

\[\square\]
Example 3.2.

\[ 168x + 668y = 888. \]

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

\[
\begin{align*}
668 &= 3 \cdot 168 + 164 \\
168 &= 164 + 4 \\
164 &= 41 \cdot 4
\end{align*}
\]

By the Euclidean Algorithm,

\[
4 = 168 - 164 \\
= 168 - (668 - 3 \cdot 168) \\
= 4 \cdot 168 + (-1) \cdot 668.
\]

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

\[
(x_0, y_0) = 222(4, -1) = (888, -222)
\]

Solve \( 168x + 668y = 0 \). Dividing both sides by \( \gcd(168, 668) \),

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

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

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

i.e.

\[
\begin{align*}
x &= 888 + 167k \\
y &= -222 - 42k
\end{align*}
\]
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 \( n \mid (b - a) \).

**Note.** For all \( k, l \in \mathbb{Z} \),

\[
a \equiv b \pmod{n} \iff a + kn \equiv b + ln \pmod{n}.
\]

Let \( \overline{a} \) denote set of solutions of the equation

\[
x \equiv a \pmod{n}; \quad \text{i.e.,}
\]

\[
\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}.
\]

We call \( \overline{a} \) the **residue class** of \( a \) modulo \( n \). There are \( n \) residue classes of modulo \( n \), i.e., \( \overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n - 1} \).

**Example 4.1.**

\[
3 \equiv 5 \pmod{2}, \quad 368 \equiv 168 \pmod{8}, \quad -8 \equiv 10 \pmod{9},
\]

\[
3 \not\equiv 5 \pmod{3}, \quad 368 \not\equiv 268 \pmod{8}, \quad -8 \not\equiv 18 \pmod{9}.
\]

**Proposition 4.1.** 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

\[
\begin{align*}
(b_1 + b_2) - (a_1 + a_2) &= (k_1 + k_2)n; \\
(b_2 - b_1) - (a_1 - a_2) &= (k_1 - k_2)n;
\end{align*}
\]

\[
\begin{align*}
b_1 b_2 - a_1 a_2 &= b_1 b_2 - b_1 a_2 + b_1 a_2 - a_1 a_2 \\
&= b_1 (b_2 - a_2) + (b_1 - a_1) a_2 \\
&= bk' n + k n a' \\
&= (b_1 k_2 + a_2 k_1) n.
\end{align*}
\]

Thus

\[
\begin{align*}
a_1 \pm a_2 &\equiv b_1 \pm b_2 \pmod{n}; \\
a_1 a_2 &\equiv b_1 b_2 \pmod{n}.
\end{align*}
\]

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 4.2.

\[ 6 \equiv 14 \pmod{8} \implies 2 \cdot 6 \equiv 2 \cdot 14 \pmod{8}; \]
\[ 6 \equiv 14 \pmod{8} \iff \frac{6}{2} \equiv \frac{14}{2} \left( \pmod{\frac{8}{2}} \right); \]

However,
\[ 2 \cdot 3 \equiv 2 \cdot 7 \pmod{8} \nRightarrow 3 \equiv 7 \pmod{8}. \]

In fact,
\[ 3 \not\equiv 7 \pmod{8}. \]

Theorem 4.2. Let \( c \mid a \), \( c \mid b \), and \( c \mid n \). Then
\[ a \equiv b \pmod{n} \iff \frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{n}{c}}. \]

Proof. Write \( a = ca_1 \), \( b = cb_1 \), \( n = cn_1 \). Then
\[ a \equiv b \pmod{n} \iff b - a = kn \text{ for an integer } k \]
\[ \iff c(b_1 - a_1) = kcn_1 \]
\[ \iff b/c - a/c = b_1 - a_1 = kn_1 \]
\[ \iff a/c \equiv b/c \pmod{n/c}. \]

\[ \square \]

Theorem 4.3.
\[ a \equiv b \pmod{m}, \quad a \equiv b \pmod{n}, \]
\[ \iff \quad a \equiv b \pmod{\text{lcm}(m, n)}. \]

In particular,
\[ \gcd(m, n) = 1 \iff a \equiv b \pmod{mn}. \]
Proof. Write \( l = \text{lcm}(m, n) \). 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 \( l = mn \).

\[ \square \]

**Definition 4.4.** 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 4.5.** 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 \( au \equiv 1 \pmod{n} \).

\[ \square \]

**Example 4.3.** 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 4.6.** 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 \( 1 \equiv cu \pmod{n} \).

\[\Rightarrow: c \equiv c \pmod{n}, a \equiv b \pmod{n} \Rightarrow ca \equiv cb \pmod{n}.\]

\[\Leftarrow: ca \equiv cb \pmod{n} \text{ and } u \equiv u \pmod{n} \text{ imply that } uca \equiv ucb \pmod{n}.\] Applying \( 1 \equiv cu \pmod{n} \), we have \( a \equiv b \pmod{n} \). \hfill \Box

**Example 4.4.** Find the inverses of 2, 4, 7, 8, 11, 13 modulo 15 respectively.

**Solution.** \( 2 \cdot 8 \equiv 1 \pmod{15}, 4 \cdot 4 \equiv 1 \pmod{15} \).

Write \( 15 = 2 \cdot 7 + 1 \). Then \( 15 - 2 \cdot 7 = 1 \). Thus \( -2 \cdot 7 \equiv 1 \pmod{15} \). Since \( -2 \equiv 13 \pmod{15} \), then

\[7 \cdot 13 \equiv 1 \pmod{15}.\]

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

\[1 = 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 = 3 \cdot (15 - 11) - 11 = 15 - 4 \cdot 11.\]

Thus the inverse of 11 is \( -4 \equiv 11 \pmod{15} \), i.e., \( 11 \cdot 11 \equiv 1 \pmod{15} \).

**Theorem 4.7.** Let \( n \in \mathbb{P} \). 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 \( d \mid b \). \qed

**Exercise 2.** Let \( S_b \) be the set of solutions of the congruence equation \( ax \equiv b \pmod{n} \). If \( x = u \) is a particular solution of \( S_b \). Show that the function \( f : S_0 \to S_b \), defined by

\[
    f(x) = x + u,
\]

is a bijection.

**Note.** For all \( k, l \in \mathbb{Z} \),

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

**Example 4.5.** Find all integers \( x \) for

\[
    9x \equiv 27 \pmod{15}.
\]

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

\[
    3x \equiv 9 \pmod{5} \iff 3x \equiv 4 \pmod{5}.
\]

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

\[
    x \equiv 3 \pmod{5}.
\]

Thus

\[
    x = 3 + 5k, \quad k \in \mathbb{Z}.
\]
**Example 4.6.** Find all integers $x$ such that

$$668x \equiv 888 \pmod{168}.$$ 

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

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

By the Division Algorithm, $167 = 3 \cdot 42 + 41$; $42 = 41 + 1$. 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

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

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

**Exercise 3.** Let $S$ be the solution set of the system

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases} \quad (1)$$

Let $S_0$ be the solution set of the same system with $(b_1 = b_2 = 0$. If $S \neq \emptyset$ has a particular solution $x = u$, then the function

$f : S_0 \longrightarrow S$, defined by

$$f(x) = x + u, \quad x \in S_0$$

is a bijection.

**Example 4.7.** How to solve the system of modular equations

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases} \quad (2)$$

21
Solution. Apply the Division Algorithm to find 
\[ d_i = \gcd(a_i, n_i), \quad i = 1, 2. \]
Reduce the system (2) to the following by dividing both side by \( d_i \) respectively.
\[
\begin{cases}
  a_1'x \equiv b_1' \pmod{n_1'} \\
  a_2'x \equiv b_2' \pmod{n_2'}
\end{cases}
\]
where \( a_i' = a_i/d_i, \ b_i' = b_i/d_i, \ n_i' = n_i/d_i, \) and 
\[ \gcd(a_i', n_i') = 1, \quad i = 1, 2. \]
Apply the Euclidean Algorithm to find \( u_i, v_i \) such that 
\[ a_i'u_i + n_i'v_i = 1. \]
Then \( a_i'u_i \equiv 1 \pmod{n_i'} \), \( i = 1, 2. \) Thus (3) can be written as
\[
\begin{cases}
  x \equiv u_1b_1' \pmod{n_1'} \\
  x \equiv u_2b_2' \pmod{n_2'}
\end{cases}
\]
Set \( c_i = u_ib_i', \ m_i = n_i', \ i = 1, 2. \) We have
\[
\begin{cases}
  x \equiv c_1 \pmod{m_1} \\
  x \equiv c_2 \pmod{m_2}
\end{cases}
\]
Let \( x = c_1 + ym_1 = c_2 + zm_2 \) for \( y, z \in \mathbb{Z} \). Solve \((y, z)\) for 
\[ m_1y - m_2z = c_2 - c_1 \]
to get a special solution \((y, z) = (y_0, z_0)\). Hence 
\[ x_0 = c_1 + m_1y_0 = c_2 + m_2z_0. \]
Finally, set \( m = \text{lcm}(m_1, m_2) \); the system (2) becomes 
\[ x \equiv x_0 \pmod{m}. \]
Example 4.8. Find all integral solutions for
\[
\begin{align*}
12x & \equiv 96 \pmod{20} \\
20x & \equiv 70 \pmod{30}
\end{align*}
\]

Solution. Applying the Division Algorithm to find
\[
\gcd(12, 20) = 4, \quad \gcd(20, 30) = 10.
\]
Then
\[
\begin{align*}
3x & \equiv 24 \pmod{5} \\
2x & \equiv 7 \pmod{3}
\end{align*}
\]
Applying the Euclidean Algorithm to find
\[
\gcd(3, 5) = 1 = 2 \cdot 3 - 1 \cdot 5
\]
so that \(2 \cdot 3 \equiv 1 \pmod{5}\); and to find
\[
\gcd(2, 3) = 1 = -1 \cdot 2 + 1 \cdot 3
\]
so that \(-1 \cdot 2 = 1 \pmod{3}\). (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
\[
\begin{align*}
2 \cdot 3x & \equiv 2 \cdot 24 \pmod{5} \\
-1 \cdot 2x & \equiv -1 \cdot 7 \pmod{3}
\end{align*}
\]
\[
\begin{align*}
x & \equiv 48 \pmod{5} \\
x & \equiv -7 \pmod{3}
\end{align*}
\]
\[
\begin{align*}
x & \equiv 3 \pmod{5} \\
x & \equiv 2 \pmod{3}
\end{align*}
\]
Set $x = 3 + 5y = 2 + 3z$, where $y, z \in \mathbb{Z}$, i.e.,

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

We find a special solution $(y_0, z_0) = (1, 2)$; so $x_0 = 8$. 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 4.9.** 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,

$$\begin{align*}
286 &= 186 + 100, \\
186 &= 100 + 86, \\
100 &= 86 + 14, \\
86 &= 6 \cdot 14 + 2.
\end{align*}$$
Then \( \gcd(186, 286) = 2 \). Applying the Euclidean Algorithm,
\[
2 = 86 - 6 \cdot 14 \\
= 86 - 6(100 - 86) = 7 \cdot 86 - 6 \cdot 100 \\
= 7(186 - 100) - 6 \cdot 100 = 7 \cdot 186 - 13 \cdot 100 \\
= 7 \cdot 186 - 13(286 - 186) = 20 \cdot 186 - 13 \cdot 286.
\]

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 \( \text{lcm}(186, 286) = 26598 \). The general solutions for
\[
\begin{cases}
  x \equiv 0 \pmod{186} \\
  x \equiv 0 \pmod{286}
\end{cases}
\]
are given by \( x \equiv 0 \pmod{\text{lcm}(168, 268)} \), i.e., \( x \equiv 0 \pmod{26598} \). Hence
\[
x \equiv -25926 \equiv 672 \pmod{26598}; \quad \text{i.e.} \quad x = 672 + 26598k, \quad k \in \Z.
\]

**Theorem 4.8 (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
\[
\begin{align*}
x &\equiv b_1 \pmod{n_1} \\
x &\equiv b_2 \pmod{n_2} \\
&\vdots \\
x &\equiv b_k \pmod{n_k}.
\end{align*}
\]
has a unique solution modulo \( n_1n_2 \cdots n_k \).
Exercise 4. In the Chinese Remainder Theorem, if
\[ \gcd(n_i, n_j) = 1, \]
is not satisfied, does the system have solutions? If yes, are the solutions unique modulo some integers?
5 Important Facts

1. Let \( \overline{a} \) denote set of solutions of the equation

\[
x \equiv a \pmod{n}; \quad \text{i.e.,}
\]

\[
\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}.
\]

We call \( \overline{a} \) the **residue class** of \( a \) modulo \( n \). There are \( n \) residue classes of modulo \( n \), i.e., \( 0, 1, 2, \ldots, n-1 \).

2. If \( c \mid a, c \mid b, c \mid n \), then

\[
a \equiv b \pmod{n} \iff \frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{n}{c}}.
\]

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 \( k, l \in \mathbb{Z} \),

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