2. Fundamental theorem of arithmetic

2.1 Greatest common divisor and Euclidean algorithm

Theorem 2.1 Given integers a and b, not both 0. There exists a unique positive integer d such that

(i) $d \mid a$ and $d \mid b$;
(ii) If $\delta \mid a$ and $\delta \mid b$, then $\delta \mid d$.

Definition 2.1 The number d in Theorem 2.1 is called the *greatest common divisor* of a and b, written as $d = \gcd(a,b) = (a,b)$.

R The gcd of a and b is the largest positive integer that is a divisor of both a and b.

Definition 2.2 If $(a,b) = 1$, we say that a and b are *relatively prime*, or *coprime*.

The proof of Theorem 2.1 is based on the so-called *Euclidean Algorithm*.

Proof (Euclidean Algorithm). Without loss of generality, we assume that $a \geq b > 0$. We also put $r_{-1} = a$ and $r_0 = b$. Now, we iteratively write

$$r_{-1} = q_1 r_0 + r_1, \qquad 0 < r_1 < r_0; \tag{2.1a}$$
$$r_0 = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1; \tag{2.1b}$$
$$r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2; \tag{2.1c}$$
$$\cdots$$
$$r_{k-2} = q_k r_{k-1} + r_k, \qquad 0 < r_k < r_{k-1}; \tag{2.1d}$$
$$r_{k-1} = q_{k+1} r_k + 0. \tag{2.1e}$$

We claim that $d = r_k > 0$.

(i). By (2.1e), we have $r_k \mid r_{k-1}$. Then by (2.1d), $r_k \mid r_{k-2}$. Continuing this process, we have $r_k \mid r_0 = b$ and $r_k \mid r_{-1} = a$.

(ii). If $\delta \mid a = r_{-1}$ and $\delta \mid b = r_0$, we know from (2.1a) that $\delta \mid r_1$, and then by (2.1b), $\delta \mid r_2$. Continuing this process, we have $\delta \mid r_k = d$. ■

We may use the Euclidean algorithm to calculate the gcd.

Example 2.1 *Find* $(1071, 462)$:

$$\begin{aligned} 1071 &= 2 \times 462 + 147; \\ 462 &= 3 \times 147 + \mathbf{21}; \\ 147 &= 7 \times 21 + 0. \end{aligned}$$

Thus, $(1071, 462) = 21$.

Definition 2.3 The greatest common divisor of $n_1, \ldots, n_k$ is the largest positive integer that divides all of $n_1, \ldots, n_k$.

2.2 Modular systems

Definition 2.4 A *modular system* S is a subset of integers such that

(i) If $n \in S$, then $-n \in S$;
(ii) If $m, n \in S$, then $m + n \in S$.

R Modular systems are instances of additive groups under the "+" operation.

Example 2.2 The set of integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is a modular system. The set of multiples of 3, namely, $\{\ldots, -6, -3, 0, 3, 6, \ldots\}$, is also a modular system. Further, the set $\{0\}$ is also a modular system.

Theorem 2.2 Let S be a modular system such that $S \neq \emptyset$. Then

(i) $0 \in S$;
(ii) If $n \in S$ and x is an integer, then $xn \in S$.

Proof. (i). Let $m \in S$ since S is non-empty. Then by definition, $-m \in S$. Finally, $0 = m + (-m) \in S$.

(ii). Without loss of generality, we assume that x is a nonnegative integer. Otherwise, we write $xn = (-x)(-n)$. Note that the statement is true for $x = 0$ by Part (i). Assume that it is true for $x = 0, \ldots, k$ for some $k \geq 0$, i.e., $xn \in S$ for $x = 0, \ldots, k$. Then for $x = k + 1$, we have $(k+1)n = n + kn \in S$ since both n and kn are in S. The statement then follows by induction. ■

Theorem 2.3 Let a and b be integers. Then $S = \{ax + by : x, y \in \mathbb{Z}\}$ is a modular system.

Proof. (i). Given any $n \in S$, it is of the form $n = ax + by$ for some integers x and y. Now, $-n = -(ax + by) = a \cdot (-x) + b \cdot (-y) \in S$.

(ii). Given any $m, n \in S$, then they are of the form $m = ax_1 + by_1$ and $n = ax_2 + by_2$. Now, $m + n = a(x_1 + x_2) + b(y_1 + y_2) \in S$. ■

Theorem 2.4 Let S be a modular system such that S is neither $\emptyset$ nor $\{0\}$. Let δ be the smallest positive integer in S. Then $S = \{k\delta : k \in \mathbb{Z}\}$.

Proof. We first note that $k\delta \in S$ for all integers k by Theorem 2.2(ii). Now assume that there exists an integer $n \in S$ such that n is not a multiple of δ. Then we may write

$$n = q \cdot \delta + r, \qquad 0 < r < \delta.$$

This implies that $r = n - q\delta \in S$. But it contradicts to the assumption that δ is the smallest positive integer in S. ■

Theorem 2.5 Let a and b be integers, not both 0. Let $d = (a,b)$. Then

$$\{ax+by : x,y \in \mathbb{Z}\} = \{kd : k \in \mathbb{Z}\}.$$

In other words, an integer n can be written as

$$n = ax+by, \qquad x,y \in \mathbb{Z}$$

if and only if n is a multiple of (a,b).

Proof. We write

$$S_1 = \{ax+by : x,y \in \mathbb{Z}\},$$
$$S_2 = \{kd : k \in \mathbb{Z}\}.$$

(i). Show $S_1 \subset S_2$. That is, if $n = ax+by$, then $n \in S_2$. This is obvious since both a and b are multiples of $d = (a,b)$, so is $ax+by$.

(ii). Show $S_2 \subset S_1$. That is, there exist integers x and y such that $kd = ax+by$ for any $k \in \mathbb{Z}$. Note that it suffices to prove the case $k = 1$, i.e., $d = ax+by$ or $d \in S_1$. We will require the process in the Euclidean algorithm. Note that S_1 is a modular system by Theorem 2.3 and $a,b \in S_1$. By (2.1a), $r_1 \in S_1$, and then by (2.1b), $r_2 \in S_1$. Continuing this process, we find that $d = r_k \in S_1$, as desired.

We conclude that $S_1 = S_2$ since they are subsets of one another. ■

2.3 Proof of the fundamental theorem of arithmetic

Theorem 2.6 If $a \mid bc$ and $(a,b) = 1$, then $a \mid c$.

Proof. By Theorem 2.5, we may find integers x and y such that $1 = ax+by$. Now,

$$c = c \cdot 1 = c \cdot (ax+by) = a \cdot (cx) + (bc) \cdot y.$$

Since bc is a multiple of a, we have $a \mid c$. ■

Corollary 2.7 If a prime $p \mid p_1 p_2 \cdots p_k$ with $p_1, \ldots, p_k$ primes, then $p = p_j$ for at least one j.

Proof. Since $p \mid p_1(p_2 \cdots p_k)$, we have either $p \mid p_1$, which implies $p = p_1$, or $p \mid p_2 \cdots p_k$ by Theorem 2.6 since $(p, p_1) = 1$ for $p \neq p_1$. Now, we repeat the process for the latter case. ■

Now, we are in a position to prove the Fundamental Theorem of Arithmetic in Theorem 1.8.

Fundamental Theorem of Arithmetic Every integer $n \geq 2$ has a unique (up to order of factors) representation as a product of primes.

Proof. In Theorem 1.7, we have shown that every integer $n \geq 2$ is a product of primes. It suffices to establish the uniqueness. Assume that n has prime factorizations

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell.$$

Then $p_1 \mid q_1 q_2 \cdots q_\ell$, and thus by renumbering the q's, we have $p_1 = q_1$ by Corollary 2.7. Dividing by p_1 on both sides, we have

$$p_2 \cdots p_k = q_2 \cdots q_\ell.$$

Repeating this process gives the desired result. ■

R We often write a (positive) integer n in its *canonical form*

$$n = \prod_{j=1}^{k} p_j^{\alpha_j}$$

with p_j its distinct prime factors and $\alpha_j > 0$.

Theorem 2.8 If

$$a = \prod_{j=1}^{r} p_j^{\alpha_j} \qquad \text{and} \qquad b = \prod_{j=1}^{r} p_j^{\beta_j},$$

where p_j's are distinct prime factors of either a or b and $\alpha_j, \beta_j \geq 0$, then

$$(a,b) = \prod_{j=1}^{r} p_j^{\min(\alpha_j, \beta_j)}.$$

Proof. We write

$$(a,b) = \prod_{j=1}^{r} p_j^{\delta_j}.$$

Then $\delta_j \leq \alpha_j$ and $\delta_j \leq \beta_j$ but δ_j is not smaller than both of α_j and β_j. ■

2.4 Least common multiple

Definition 2.5 Let a and b be integers with $a, b \neq 0$. Then the *least common multiple* of a and b is the positive integer m such that

(i) $a \mid m$ and $b \mid m$;

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

We write $m = \text{lcm}(a,b) = [a,b]$.

R The lcm of a and b is the smallest positive integer that is a multiple of both a and b.

Definition 2.6 The least common multiple of $n_1, \ldots, n_k$ is the smallest positive integer that is divisible by all of $n_1, \ldots, n_k$.

Theorem 2.9 If

$$a = \prod_{j=1}^{r} p_j^{\alpha_j} \qquad \text{and} \qquad b = \prod_{j=1}^{r} p_j^{\beta_j},$$

where p_j's are distinct prime factors of either a or b and $\alpha_j,]beta_j \geq 0$, then

$$[a,b] = \prod_{j=1}^{r} p_j^{\max(\alpha_j, \beta_j)}.$$

Proof. This is a direct consequence of the definition of lcm. ■

Theorem 2.10 Let a and b be positive integers. Then

$$[a,b] = \frac{ab}{(a,b)}.$$

Proof. Note that if we write $a = \prod_{j=1}^{r} p_j^{\alpha_j}$ and $b = \prod_{j=1}^{r} p_j^{\beta_j}$, then

$$\begin{aligned}
[a,b]\cdot(a,b) &= \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j)} \cdot \prod_{j=1}^{r} p_j^{\min(\alpha_j,\beta_j)} \\
&= \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j)+\min(\alpha_j,\beta_j)} \\
&= \prod_{j=1}^{r} p_j^{\alpha_j+\beta_j} \\
&= \prod_{j=1}^{r} p_j^{\alpha_j} \cdot \prod_{j=1}^{r} p_j^{\beta_j} \\
&= ab,
\end{aligned}$$

where we make use of the fact that $\max(\alpha,\beta)+\min(\alpha,\beta) = \alpha+\beta$. ■