

The Fundamental Theorem of Arithmetic

THEOREM 1: If a, b , and c are positive integers such that $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof: By Theorem 2 from Section 3.3, there are integers s and t such that $sa + tb = (a, b)$. Since $(a, b) = 1$, we get

$$sa + tb = 1$$

Multiplying both sides by c , we obtain

$$sac + tbc = c \tag{1}$$

Since $a \mid bc$ and $a \mid sac$, it follows that $a \mid (sac + tbc)$ by Theorem 2 from Section 1.5. This and (1) give $a \mid c$. ■

THEOREM 2: If p divides $a_1a_2 \dots a_n$, where p is a prime and a_1, a_2, \dots, a_n are positive integers, then there is an integer i with $1 \leq i \leq n$ such that p divides a_i .

Proof: We prove this result by induction.

Step 1. The case where $n = 1$ is trivial.

Step 2. Assume that the result is true for some $n = k, k \geq 1$, that is, if p divides $a_1a_2 \dots a_k$, then it must divide at least one of the factors a_i .

Step 3. We prove that it is true for $n = k+1$. Consider a product of $k+1$ integers $a_1a_2 \dots a_k a_{k+1}$ that is divisible by the prime p . Put

$$c = a_1a_2 \dots a_k, \quad d = a_{k+1}$$

Since p is a prime number, then either $(p, c) = 1$ or $(p, c) = p$. If $(p, c) = 1$, then by the Theorem above, $p \mid d = a_{k+1}$. On the other hand, if $(p, c) = p$, then $p \mid c = a_1a_2 \dots a_k$, therefore by Step 2 there is an integer i with $1 \leq i \leq k$ such that $p \mid a_i$. Consequently, $p \mid a_i$ for some i with $1 \leq i \leq k+1$. ■

COROLLARY: If p is a prime and $p \mid a^n, n \geq 1$, then $p \mid a$.

Proof: Put $a_1 = a_2 = \dots = a_n = a$ in Theorem 2. ■

EXAMPLE: Prove that if a and b are positive integers with $(a, b) = 1$, then $(a^2, b^2) = 1$ for all positive integers n .

Proof: Assume to the contrary that $(a^2, b^2) = n > 1$. Then by the Lemma from Section 3.1, there is a prime p that divides n and therefore by Theorem 1 from Section 1.5, $p \mid a^2$ and $p \mid b^2$. From this by the Corollary, $p \mid a$ and $p \mid b$, therefore $(a, b) \geq p$. This is a contradiction. ■

THEOREM 3 (The Fundamental Theorem of Arithmetic): Assume that an integer $a \geq 2$ has factorizations

$$a = p_1 \dots p_m \quad \text{and} \quad a = q_1 \dots q_n$$

where the p 's and q 's are primes. Then $n = m$ and the q 's may be reindexed so that $q_i = p_i$ for all i .

Proof: We prove by induction on ℓ , the larger of m and n , i. e. $\ell = \max(m, n)$.

Step 1. If $\ell = 1$, then the given equation in $a = p_1 = q_1$, and the result is obvious.

Step 2. Suppose the theorem holds for some $\ell = k \geq 1$.

Step 3. We prove it for $\ell = k + 1$. Let

$$a = p_1 \dots p_m = q_1 \dots q_n \tag{2}$$

where

$$\max(m, n) = k + 1 \tag{3}$$

From (2) it follows that $p_m \mid q_1 \dots q_n$, therefore by Theorem 2 there is some q_i such that $p_m \mid q_i$. But q_i , being a prime, has no positive divisors other than 1, therefore $p_m = q_i$. Reindexing, we may assume that $q_n = p_m$. Canceling, we have $p_1 \dots p_{m-1} = q_1 \dots q_{n-1}$. Moreover, $\max(m-1, n-1) = k$ by (3). Therefore by Step 2 q 's may be reindexed so that $q_i = p_i$ for all i ; plus, $m-1 = n-1$, hence $m = n$. ■

COROLLARY: If $a \geq 2$ is an integer, then there are unique distinct primes p_i and unique integers $\alpha_i > 0$ such that

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

Proof: Just collect like terms in a prime factorization. ■

EXAMPLE: $120 = 2^3 \cdot 3 \cdot 5$

THEOREM 4: Let $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \dots p_n^{\beta_n}$ be positive integers. Then

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \dots p_n^{\min(\alpha_n, \beta_n)}$$

EXAMPLE: Since

$$720 = 2^4 \cdot 3^2 \cdot 5 \quad \text{and} \quad 2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$$

it follows that

$$(720, 2100) = 2^2 \cdot 3 \cdot 5 = 60$$

DEFINITION: The **least common multiple** of two positive integers a and b is the smallest positive integer that is divisible by a and b .

The least common multiple of a and b is denoted by $[a, b]$.

EXAMPLE: We have the following least common multiples: $[15, 21] = 105$, $[24, 36] = 72$, $[2, 20] = 20$, and $[7, 11] = 77$.

Once the prime factorizations of a and b are known, it is easy to find $[a, b]$. If

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \quad \text{and} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

where p_1, p_2, \dots, p_n are the primes occurring in the prime-power factorizations of a and b (where we might have $\alpha_i = 0$ or $\beta_i = 0$ for some i), then for an integer to be divisible by both a and b , it is necessary that in the factorization of the integer, each p_j occurs with a power at least as large as α_j and β_j . Hence, $[a, b]$, the smallest positive integer divisible by both a and b , is

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_n^{\max(\alpha_n, \beta_n)}$$

where $\max(x, y)$ denotes the larger, or maximum, of x and y .

Finding the prime factorization of large integers is time-consuming. Therefore, we would prefer a method for finding the least common multiple of two integers without using the prime factorizations of these integers. We will show that we can find the least common multiple of two positive integers once we know the greatest common divisor of these integers. The latter can be found via the Euclidean algorithm. First, we prove the following lemma.

LEMMA: If x and y are real numbers, then

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

Proof: If $x \geq y$, then

$$\min(x, y) = y \quad \text{and} \quad \max(x, y) = x$$

so that

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

Similarly, If $x < y$, then

$$\min(x, y) = x \quad \text{and} \quad \max(x, y) = y$$

and again we find that

$$\max(x, y) + \min(x, y) = x + y \quad \blacksquare$$

We use the following theorem to find $[a, b]$, once (a, b) is known.

THEOREM 5: If a and b are positive integers, then

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

where $[a, b]$ and (a, b) are the least common multiple and greatest common divisor of a and b , respectively.

Proof: Let a and b have prime-power factorizations

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \quad \text{and} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

where the exponents are nonnegative integers and all primes occurring in either factorization occur in both, perhaps with zero exponents. Now let

$$M_j = \max(\alpha_j, \beta_j) \quad \text{and} \quad m_j = \min(\alpha_j, \beta_j)$$

Then, we have

$$\begin{aligned}a, b &= p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n} p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \\ &= p_1^{M_1+m_1} p_2^{M_2+m_2} \cdots p_n^{M_n+m_n} \\ &= p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n} \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} \\ &= ab\end{aligned}$$

since

$$M_j + m_j = \max(\alpha_j, \beta_j) + \min(\alpha_j, \beta_j) = \alpha_j + \beta_j$$

by the Lemma above. ■