4.3 Primes and Greatest Common Divisors

- In this section, we will learn an important theorem, the fundamental theorem of arithmetic (**FTA**) which has many interesting consequences. We note that primes play an essential role in studying cryptographic systems. In addition, we will study the GCD and LCM.

Definition

An integer $p > 1$ is called **prime** if the only positive factors of p are 1 and p. A positive $p > 1$ that is not prime is called **composite**. Note that 1 is neither prime nor composite.

Theorem

The FTA: *Every integer $p > 1$ can be written uniquely as a prime or the product of two or more primes, i.e.,*

$$p = a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m},$$

where $a_1, a_2, \cdots, a_m$ are prime and $n_1, n_2, \cdots, n_m \geq 1$ are integers

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Example1

1. Determine each of the following integers is prime.
(1) 21 (2) 71 (3) 111 (4) 143
2. Find the prime factorization of the following integers.
(1) 88 (2) 126 (3) 1001

Definitions

1. Let $a, b \in \mathbb{Z}$ be nonzero. The largest integer d such that $d \mid a$ and $d \mid b$ is the greatest common divisor **(GCD)** of a and b, denoted by $\gcd(a, b)$.
2. The integers a and b are **relatively prime** if $\gcd(a, b) = 1$.
3. The least common multiple **(LCM)** of the positive integers a and b which is denoted by $\operatorname{lcm}(a, b)$ is the smallest positive integer that is divisible by both a and b.

- How to find the GCD and LCM?
  Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ with all nonnegative integer powers. Then

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)},$$

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}.$$

Definitions

The integers $a_1, a_2, \cdots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

Example2

1. Determine whether the integers in each of the following sets are pairwise relatively prime.
(1) $11, 15, 19$ (2) $12, 17, 31, 37$
2. Find the GCD and LCM of the following pairs of integers.
(1) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$ (2) $3^{13} \cdot 5^{17}$, $2^{12} \cdot 7^{21}$ (3) 1111, 0
(4) 120, 180 (5) 243, 327