Fundamental Theorem of Arithmetic

Shef Scholars Competitive Math Academy

August 2025

Introduction

The Fundamental Theorem of Arithmetic tells us that every integer can be written as a product of prime numbers.

Theorem 1. (Fundamental Theorem of Arithmetic). Every natural number n greater than one can be uniquely written in the form

$$n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l},$$

where $p_1 < p_2 < \cdots < p_l$ are prime numbers and $k_1, k_2, \dots, k_l$ are natural numbers.

Proof of Fundamental theorem of arithmetic:
Existence. Assume there exists a natural number not expressible as a product of primes. Let m be the smallest such number. Then m is not prime, so $m = ab$ with $1 < a, b < m$. By minimality, a and b have prime factorizations, so $m = ab$ also does — contradiction. Hence, every number has a prime factorization.

Uniqueness. Assume n has two distinct factorizations:

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l,$$

with primes in non-decreasing order. Cancel all common primes: we get

$$p_1 p_2 \dots p_t = q_1 q_2 \dots q_s,$$

with all remaining primes distinct. Then $p_1 \mid q_1 q_2 \dots q_s$, so $p_1 \mid q_j$ for some j. But this contradicts the fact that $p_i \neq q_j$. Thus, the prime factorization is unique. $\square$

Number of Divisors of a Number

Let n be a natural number with the prime factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $p_1, p_2, \dots, p_k$ are distinct prime numbers and $\alpha_1, \alpha_2, \dots, \alpha_k$ are positive integers.

The number of positive divisors of n, denoted by $d(n)$, is given by the formula:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Proof: Each divisor of n can be written in the form

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

where $0 \leq \beta_i \leq \alpha_i$ for each i. The number of choices for each exponent β_i is $\alpha_i + 1$, so by the multiplication principle, the total number of divisors is the product of these quantities.

Sum of Divisors of a Number

Let n be a natural number with the prime factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers.

The sum of all positive divisors of n, denoted by $\sigma(n)$, is given by the formula:

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Proof: We will prove the statement by induction on the number n of factors in the product.
Base case: $k = 1$. For $n = p_1^{\alpha_1}$,

$$\sigma(n) = 1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}.$$

Inductive step: Assume the formula holds for k primes. Consider

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}},$$

with $k+1$ distinct primes.

Let m be natural number in a form:

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Split the sum of divisors $\sigma(n)$ by considering all divisors of n. Each divisor of n can be written uniquely as a product of a divisor of $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and a power of p_{k+1}:

$$d = d' \cdot p_{k+1}^j,$$

where d' divides m and j is an integer with $0 \leq j \leq \alpha_{k+1}$.

To find the sum of all divisors of n, we sum over all possible j and for each fixed j, sum over all divisors d' of m. Thus, the total sum is:

$$\sigma(n) = \sum_{j=0}^{\alpha_{k+1}} \left(\sum_{d' \mid m} d' \cdot p_{k+1}^j \right).$$

We can rewrite this by factoring out p_{k+1}^j since it does not depend on d':

$$\sigma(n) = \sum_{j=0}^{\alpha_{k+1}} p_{k+1}^j \left(\sum_{d' \mid m} d' \right).$$

Notice that the inner sum $\sum_{d' \mid m} d'$ is just $\sigma(m)$, the sum of divisors of m, which we know by the induction hypothesis.

Therefore, the entire sum becomes:

$$\sigma(n) = \sigma(m) \cdot \left(1 + p_{k+1} + p_{k+1}^2 + \cdots + p_{k+1}^{\alpha_{k+1}}\right).$$

The second factor is a geometric series with sum

$$\frac{p_{k+1}^{\alpha_{k+1}+1} - 1}{p_{k+1} - 1}.$$

Combining both, we get

$$\sigma(n) = \sigma(m) \cdot \frac{p_{k+1}^{\alpha_{k+1}+1} - 1}{p_{k+1} - 1},$$

which completes the inductive step.

Greatest Common Divisor

To find $\gcd(a, b)$ using prime factorization, we write both numbers as a product of the same prime numbers:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n} (1)$$

where a_i, b_i are natural numbers or 0. A prime p may divide only one of the numbers. In such a case, for example, if p_1 is not a factor of b, then $b_1 = 0$.
Now it is clear that:

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

because a and b can have at most $\min(a_i, b_i)$ powers of p_i.

Least Common Multiple

Prime factorization can also be used to find the least common multiple (lcm) of two natural numbers.

Definition 1. The least common multiple of a and b, denoted by $[a, b]$, is the smallest natural number divisible by both a and b.

If we represent a and b as in the previous form, then it is clear that

$$[a, b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}.$$

Theorem 2. For natural numbers a and b, it holds that

$$[a, b] \cdot \gcd(a, b) = ab.$$

Proof. Let the factorizations of a and b be as in (1), and define $m_j = \min(a_j, b_j)$ and $M_j = \max(a_j, b_j)$ for $j = 1, \dots, n$. Then,

$$M_j + m_j = a_j + b_j,$$

so we get

$$[a, b] \cdot \gcd(a, b) = \prod_{j=1}^{n} p_j^{M_j} \cdot \prod_{j=1}^{n} p_j^{m_j} = \prod_{j=1}^{n} p_j^{M_j+m_j} = ab, \quad \text{q.e.d.}$$

Proof that There Are Infinitely Many Prime Numbers

Assume, for contradiction, that there are only finitely many prime numbers. Let them be

$$p_1, p_2, \ldots, p_n.$$

Consider the number

$$N = p_1 p_2 \cdots p_n + 1.$$

This number N is greater than 1, so it must have a prime divisor. However, none of the primes $p_1, p_2, \ldots, p_n$ divides N, since each divides the product $p_1 p_2 \cdots p_n$, but not $N = p_1 p_2 \cdots p_n + 1$ (the remainder is 1).

Therefore, N must be divisible by a prime not in the list, contradicting the assumption that all primes are listed. Hence, there are infinitely many prime numbers.

Proof that There Are Infinitely Many Primes of the Form $4n + 3$

Assume, for contradiction, that there are only finitely many primes of the form $4n + 3$. Let these primes be

$$p_0, p_1, \ldots, p_k,$$

all of the form $4n + 3$.

Consider the number

$$Q = 4p_0 p_1 \cdots p_k - 1.$$

Note that Q is also of the form $4n + 3$.

Since Q is greater than 1, it must have at least one prime divisor. By assumption, all primes of the form $4n + 3$ are in the list $p_0, p_1, \ldots, p_k$.

If all prime factors of Q were of the form $4m + 1$, then their product would also be of the form $4m + 1$ because:

$$(4r + 1)(4s + 1) = 4(4rs + r + s) + 1.$$

But Q is of the form $4n + 3$, so it must have at least one prime factor of the form $4n + 3$.

Therefore, Q must be divisible by some p_i from the list. However, $Q = 4p_0 p_1 \cdots p_k - 1$ leaves remainder -1 when divided by any p_i, so none divides Q.

This contradiction shows that there are infinitely many primes of the form $4n + 3$.

Problems

1. Prove the inequality:

$$\operatorname{lcm}(x, y) \cdot \operatorname{lcm}(y, z) \cdot \operatorname{lcm}(z, x) \geq \left(\operatorname{lcm}(x, y, z)\right)^2$$

2. Natural numbers a, b, c, d are all divisible by $ad - bc$. Prove that $|ad - bc| = 1$.

3. Let $1 = d_1 < d_2 < \cdots < d_k = n$ be all positive divisors of the number n. Find all n for which:

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2.$$

4. Let $m, n \in \mathbb{N}$. If the number:

$$\frac{m^2 + n^2 - m}{mn}$$

is an integer, prove that m is a perfect square.

5. Let n be a natural number. Let $a, b, c, m \in \mathbb{N}$ be such that $a \mid b^n$, $b \mid c^n$, and $c \mid a^n$, and $abc \mid (a + b + c)^m$. Determine the greatest possible value of m.

6. Let $b, n > 1$ be natural numbers. If for every $k > 1$ there exists an integer a_k such that:

$$k \mid b - a_k^n$$

Prove that $b = B^n$ for some integer B.

7. If a natural number n can be written as a sum of two squares in two different ways, prove that n is composite.

8. Let $m, n \in \mathbb{N}$ with $m < n$ and $m \mid n$. Prove that

$$\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}.$$

9. A natural number n is called *perfect* if

$$\sigma(n) = 2n,$$

where $\sigma(n)$ denotes the sum of all positive divisors of n. Show that if $n > 28$ is perfect and $7 \mid n$, then $49 \mid n$.

10. Let $1 = d_1 < d_2 < \cdots < d_k = n$ be all positive divisors of a natural number $n > 1$. Define

$$D = \sum_{i=1}^{k-1} d_i d_{i+1}.$$

    (a) Prove that $D < n^2$.

    (b) Determine all n for which $D \mid n^2$.