Computing Science 204 (B1)
The Fundamental Theorem of Arithmetic
Saturday, July 22

The Fundamental Theorem of Arithmetic states that if $n > 1$ is a positive integer, then n can be written as a product of primes in only one way, apart from the order of the factors.

Definition. An integer n is said to be a **prime** if and only if $n > 1$ and the only positive divisors of n are 1 and n.

In order to prove the fundamental theorem of arithmetic, we need the following lemmas.

Lemma 1. Every integer $n > 1$ is either a prime number or a product of prime numbers.

proof. We will prove this by induction on n. The lemma is clearly true for $n = 2$. Assume now that it is true for every positive integer k with $2 \leq k < n$. If n is not a prime, then it has a positive divisor d with $d \neq 1$ and $d \neq n$. Therefore, $n = m \cdot d$, where $m \neq n$. However, both m and d are less than n and greater than 1, so by the induction hypothesis each of m and d is a product of primes, therefore n is also a product of primes. This completes the induction.

□

Lemma 2. If a prime p does not divide a, then $\gcd(p, a) = 1$.

proof. Let $d = \gcd(p, a)$, then $d \,|\, p$ and p is prime, so that $d = 1$ or $d = p$. However, $d \,|\, a$, so we must have $d \neq p$, since $p \not| a$. Therefore, $d = 1$.

□

Lemma 3. If a prime p divides ab, then $p \,|\, a$ or $p \,|\, b$. More generally, if a prime p divides a product $a_1 a_2 \cdots a_n$, the p divides at least one of the integers a_i, for $1 \leq i \leq n$.

proof. Suppose that $p \,|\, ab$ and that $p \not| a$. We will prove that $p \,|\, b$. From Lemma 2 we have $\gcd(p, a) = 1$, and by the Euclidean algorithm there exist integers x and y such that $1 = xa + yp$, and therefore,

$$b = x \cdot ab + yb \cdot p,$$

so that $p \,|\, b$. For the more general statement, use induction on n.

□

Theorem. *Fundamental Theorem of Arithmetic*

Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.

proof. The proof is by induction on n. The theorem is true for $n = 2$. Assume, then, that the theorem is true for all integers k with $1 < k < n$. We will show that this implies that it is also true for n.

If n is prime, then there is nothing more to prove. Assume, then, that n is composite and that n has two factorizations, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \qquad (*)$$

We want to show that $s = t$ and that each p_i equals some q_j.

Since $p_1 \,|\, q_1 q_2 \cdots q_t$ and p_1 is prime, then by Lemma 3, p_1 must divide some q_j. We may assume then (relabel) that $p_1 \,|\, q_1$, and therefore $p_1 = q_1$ since they are both primes. In $(*)$ we can cancel p_1 on both sides to get

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \dots q_t.$$

If $s > 1$ or $t > 1$, then $1 < \dfrac{n}{p_1} < n$, and by the induction hypothesis the two factorizations of $\dfrac{n}{p_1}$ must be identical, apart from the order of the factors. Therefore $s = t$ and the factorizations in $(*)$ are also identical, apart from the order of the factors. The induction is complete.

$\square$

Note: In the factorization of an integer n, a particular prime p may occur more than once. If the *distinct* prime factors of n are $p_1, p_2, \ldots, p_k$, and if p_i occurs as a prime factor α_i times, for $1 \leq i \leq k$ then we can write

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

that is,

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

and this is called the factorization of n into prime powers. We can also express 1 in this form by taking each exponent $\alpha_i = 0$.

Corollary. If

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

then the set of positive divisors of n is the set of all numbers d of the form

$$d = \prod_{i=1}^{k} p_i^{\beta_i},$$

where $0 \leq \beta_i \leq \alpha_i$ for $i = 1, 2, \ldots, k$, and the number of positive divisors of n, denoted by $\tau(n)$, is given by

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