UNIQUE PRIME FACTORIZATION

Theorem. *A positive integer can be written as a product of primes in only one way, except for the order in which the primes are written.*

There are many ways to prove this Theorem. The one we present avoids the use of Euclid's lemma.

Proof. Let $n > 1$ be the smallest integer that has two different prime factorizations, and let p be the smallest prime that occurs in any prime factorization of n. The prime p can occur only in one prime factorization of n; indeed, if p occurred in two different prime factorizations of n, writing the equation expressing the equality of these two prime factorizations, we could cancel p from both sides and obtain an integer smaller than n with two different prime factorizations. Since $p \mid n$, we have $n = mp$ for some integer m. Let $q_1 q_2 \dots q_k$ be a prime factorization of n in which p does not occur. We have

$$mp = q_1 q_2 \dots q_k,$$

where $q_i > p$ for each i with $1 \le i \le k$. When dividing p into q_i, denote the quotient by l_i, and the remainder by r_i; we have $q_i = l_i p + r_i$ and $0 < r_i < p$. That is

$$mp = (l_1 p + r_1)(l_2 p + r_2) \dots (l_k p + r_k).$$

If we multiply out the right-hand side, all terms will contain p except for the term $r_1 r_2 \dots r_k$. Adding up the terms containing p, we get a multiple of p; write this as ap, where a is an integer. That is

$$mp = ap + r_1 r_2 \dots r_k.$$

Writing $b = m - a$, we have

$$bp = r_1 r_2 \dots r_k.$$

Here $b > 0$, since the right-hand side is positive. Taking the prime factorizations of b and of each r_i for i with $1 \le i \le k$, we obtain two prime factorizations of the number bp; one on the left containing p, one on the right containing primes all smaller than p. As

$$bp = r_1 r_2 \dots r_k < q_1 q_2 \dots q_k = n,$$

we obtained a number smaller than n with two different prime factorizations. This is a contradiction. □

[0]Notes for Course Mathematics 1311 at Brooklyn College of CUNY. Attila Máté, February 16, 2018.