

Uniqueness of prime factorization

I give an elementary proof of the uniqueness of prime factorization, stolen from Davenport's book, avoiding the circle of ideas centring on the Euclidean algorithm. I hasten to add that embracing these ideas is the **best** way of thinking about unique factorization. This proof is not.

Each $n \in \mathbf{N}$ with $n \geq 2$ can be written as

$$n = \prod_{j=1}^r p_j = p_1 p_2 \dots p_r \quad (*)$$

where $r \geq 1$, $p_1, \dots, p_r$ are all prime and $p_1 \leq p_2 \leq \dots \leq p_r$. The unique factorization theorem asserts that this factorization is unique, that is, if also

$$n = \prod_{j=1}^s q_j = q_1 q_2 \dots q_s \quad (\dagger)$$

where $s \geq 1$, $q_1, \dots, q_s$ are all prime and $q_1 \leq q_2 \leq \dots \leq q_s$, then $r = s$ and $q_j = p_j$ for all j .

To prove this, we argue by contradiction. Suppose that there is an n with two distinct factorizations $(*)$ and $(\dagger)$. We'll call such n *bad* and so numbers n which have unique prime factorizations we call *good*. Suppose for sake of contradiction that there is a bad number. Then there is a smallest bad number n , and so all numbers m with $2 \leq m < n$ are good. Consider $(*)$ and $(\dagger)$ for this n . Certainly n cannot be prime, so $r \geq 2$ and $s \geq 2$. The first thing to notice is that $p_1 \neq q_1$, for if $p_1 = q_1$ then

$$n/p_1 = \prod_{j=2}^r p_j = p_2 \dots p_r = n/q_1 = \prod_{j=2}^s q_j = q_2 \dots q_s < n$$

and n/p_1 is good. This means that these two prime factorizations of n/p_1 are the same, and so $(*)$ and $(\dagger)$ are the same: contradiction. Hence $p_1 \neq q_1$.

By reversing the roles of the p s and the q s we may assume that $p_1 < q_1$. I claim that $q_1 \leq \sqrt{n}$. This follows as

$$n = q_1 q_2 \dots q_s \geq q_1 q_2 \geq q_1^2$$

as $q_2 \geq q_1$. Taking square roots gives $\sqrt{n} \geq q_1$. Hence $p_1 < \sqrt{n}$ and so $p_1 q_1 < \sqrt{n} \sqrt{n} = n$. Define

$$m = n - p_1 q_1.$$

Then m is a positive integer; also $m < n$ and so n is good. As p_1 is a factor of n then p_1 is a factor of m . Hence m has a prime factorization involving p_1 .

Similarly q_1 is a factor of m and so m has a prime factorization involving q_1 . As m is good, its unique prime factorization must involve both p_1 and q_1 . Hence $m = p_1 q_1 M$ for some positive integer M , and so

$$n = p_1 q_1 + m = p_1 q_1 (1 + M).$$

As $1 < n/q_1 < n$, n/q_1 is good, and

$$n/q_1 = p_1(1 + M) = q_2 \cdots q_s.$$

But by breaking up $M + 1$ as a product of a sequence of primes, we get a prime factorization of n/q_1 involving p_1 . As n/q_1 is good, then p_1 must occur in the factorization $n/q_1 = q_2 \cdots q_s$. But this is false: $p_1 < q_1 \leq q_j$ for each j so $p_1 < q_j$. We finally get a contradiction to the existence of a bad number: all numbers must be good, and we have proved unique factorization.

RJC 1/2/2005