ANSWER on Question #82163 – Math – Combinatorics – Number Theory

QUESTION

Prove that every composite number in $\mathbb{Z}$ is reducable.

SOLUTION

Theorem 1.1 (Unique Factorization in $\mathbb{Z}$). Every integer $n > 1$ can be written as a product of primes. Moreover, the prime factorization of n is unique: if $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ where the p_i's and q_j 's are prime then $r = s$ and after relabeling the factors we have $p_i = q_i$ for all i.

Theorem 1.1 is really two statements about each $n > 1$: (i) a prime factorization of n exists and (ii) there is only one prime factorization for n up to the order of multiplication of the prime factors.

To prove Theorem 1.1, we will prove these two statements separately.

When we talk about a product of primes in Theorem 1.1, we allow a "product" with a single term in it, so a prime number is a product of primes using only itself in the product. If we didn't allow this, then we'd have to say every $n > 1$ is a prime or a product of primes. By allowing a product with a single term, our language becomes simpler.

Theorem 2.1. Every $n > 1$ has a prime factorization: we can write $n = p_1 \cdots p_r$, where the p_i are prime numbers.

Proof. We will use induction, but more precisely strong induction: assuming every integer between 1 and n has a prime factorization we will derive that n has a prime factorization. Our base case is $n = 2$. This is a prime, so it is a product of primes by our convention that a prime is a product of primes with one term.

Now assume $n > 2$ and (here comes the strong inductive hypothesis) for all m with $1 < m < n$ that m is a product of primes. To show n is a product of primes, we take cases depending on whether m is prime or not. Case 1: The number n is prime.

In this case, n is a product of primes with just one term. (This is the easy case.)

Case 2: The number n is not prime.

Since $n > 1$ and n is not prime, there is some nontrivial factorization $n = ab$ where $1 < a < n$ and $1 < b < n$. By our strong inductive hypothesis, both a and b are products of primes. Since n is the product of a and b, and

both a and b are products of primes, n is a product of primes by stringing together the prime factorizations of a and b. More explicitly, writing $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$ where p_i and q_j are all prime, we have

$$n = ab = p_1 \cdots p_r \cdot q_1 \cdots q_s$$

which is a product of primes.

Q.E.D.

Lemma 2.2. If p is a prime number and $p|ab$ for some integers a and b, then $p|a$ or $p|b$.

Proof. We will assume $p|ab$ and the conclusion is false: p does not divide a or p does not divide b. If p does not divide a then $(p, a) = 1$ because p is prime. A basic consequence of Bezout's identity tells us that from $p|ab$ and $(p, a) = 1$ we have $p|b$. If p does not divide b, then by switching the roles of a and b (which is okay since $ab = ba$) we can conclude that $p|a$.

Q.E.D.

A generalization of **Lemma 2.2** is that for any finite list of integers $a_1, \ldots, a_k$, if $p|a_1 \cdots a_k$ then $p|a_i$ for some i. This is trivial for $k = 1$, and for $k \geq 2$ it is true by induction on k with **Lemma 2.2** being the base case $k = 2$. Now we can prove prime factorization is unique.

Theorem 2.3. If $p_1 \cdots p_r = q_1 \cdots q_s$ where the p_i's and q_j's are prime, then $r = s$ and after relabeling the factors we have $p_i = q_i$ for all i.

Proof. The key mathematical step is this: when $p_1 \cdots p_r = q_1 \cdots q_s$, p_1 must equal some q_j. This is because $p_1 \cdots p_r = q_1 \cdots q_s \Longrightarrow p_1|q_1 \cdots q_s \Longrightarrow p_1|q_j$ for some j, where the second implication is the generalization of **Lemma 2.2** that we mentioned above. That uses primality of p_1. Since q_j is prime and $p_1|q_j$, we must have $p_1 = q_j$ (a prime has no factor greater than 1 other than itself). To prove our theorem, we will induct on the total number of prime factors in the two equal prime factorizations, which is $(r + s)$. We allow repeated primes. The base case is $(r + s) = 2$, when the equal prime factorization turns into $p_1 = q_1$. Here the conclusion of the theorem is obvious (there is no relabeling needed, since each side has one factor).

Suppose next that $(r + s) > 2$ and the theorem is true for any two equal prime factorizations for which the total number of primes being used is less than $(r + s)$. If we have $p_1 \cdots p_r = q_1 \cdots q\_s$ then $r > 1$ and $s > 1$: if $r = 1$ or $s = 1$ then one side is a prime number and therefore the other side has to be a prime number, so $r = s = 1$, but $(r + s) > 2$. From $p_1 \cdots p_r = q_1 \cdots q_s$ we explained at the start of the proof that p_1 must be some q_j. By relabeling the factors on the right, which is okay since the order of multiplication doesn't matter, we can assume $p_1 = q_1$. Then our equal prime factorization becomes $p_1 p_2 \cdots p_r = p_1 q_2 \cdots q_s$. Canceling the

common factor p_1 on both sides, we get $p_2 \cdots p_r = q_2 \cdots q_s$ (2.1). In this equation of equal prime factorizations, the total number of primes appearing on both sides is $(r-1)+(s-1) = r+s-2$, which is less than $(r+s)$. By our inductive hypothesis we conclude $r-1 = s-1$ (there are $r-1$ primes on the left and $s-1$ primes on the right), so $r = s$, and after relabeling the primes in (2.1) we have $p_i = q_i$ for all $i \geq 2$. Combining this with $p_1 = q_1$ we have $p_i = q_i$ for all i.

Q.E.D.