Math 126 Number Theory

Prof. D. Joyce, Clark University

1 Feb 2006

Due Today. From page 26, exercises 2, 3, 4, 5, 6, 11, 12, 13.

Due Monday. From page 32, exercises 5, 7, 12, 13, 15.

For next time. Read through section 2.3.

Last meeting. More on divisibility,greatest common divisors, and the Euclidean algorithm.

Today. The unique factorization theorem, a.k.a., the fundamental theorem of arithmetic, says that each number can only be factored as a product of primes in one way. For instance, 275 is the product $5 \cdot 5 \cdot 11$, and, excepting the order of the factors, that's the only way that 275 can be written as the product of primes.

Now, in order to make this general statement valid we have to extend a little bit what we mean by a product. For example, how do you write a prime number like 7 as a product of primes? It has to be written as the product 7 of only one prime. So we will have to accept a single number as being a product of one factor.

Even worse, what about 1? There are no primes that divide 1. One solution is to accept a product of no factors as being equal to 1. It's actually a reasonable solution to define the empty product to be 1, but until we find another need for an empty product, let's wait on that and restrict this unique factorization theorem to numbers greater than 1. So, here's the statement of the theorem we want to prove. (I'm calling it theorem 5, because we'll reduce it one step at a time to more "primitive" theorems).

Theorem 5. Each integer n greater than 1 can be uniquely factored as a product of primes. That is, if n equals the product $p_1 p_2 \cdots p_r$ of r primes, and it also equals the product $q_1 q_2 \cdots q_s$ of s primes, then the number of factors in the two products is the same, that is $r = s$, and the two lists of primes $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ are the same apart from the order the listings.

Rather than exactly following the form of the proof in the text that uses a proof by contradiction, we'll make it into a direct proof by using a form of induction. The form that we'll use is this:

> In order to prove a statement $S(n)$ is true for all numbers, prove that $S(n)$ follows from the assumption that $S(k)$ is true for all $k < n$.

This principle of induction appears to be stronger than the one we've used before, but, in fact, it is equivalent to it. It's really the same as the minimization principle (i.e. well-ordering principle) applied to the negation of the statement. The advantage in using it is that a proof by contradiction is not needed making the proof more understandable.

We'll prove the unique factorization theorem in two cases. Case 1 will be where n is a prime number itself. Case 2 will be where n is composite.

Case 1: Suppose that n is a prime number. The only way that a prime number can be written as a product of primes is as itself; otherwise it would not be prime, but composite.

Case 2: Suppose that n is a composite number equal to both products of primes $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$. Note that since n is composite, both

r and s are at least 2; otherwise it would not be composite, but prime.

Now look at one of the primes, say p_1. It divides n, so it divides the product of the other primes $q_1 q_2 \cdots q_s$. We suspect that that implies it has to be one of those other primes. Let's put that off for a bit; that is, logically before we prove this theorem 4, we need to prove another theorem, theorem 4, that if a prime divides a product of primes, then it is one of those primes; but we'll actually do that next. Assuming we've done that, then we can conclude that p_1 is one of the q_i's. We can reorder the product $q_1 q_2 \cdots q_s$ to make it q_1 so that p_1 equals q_1. Now, since $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ and the first first factors of the two products are equal, therefore $p_2 \cdots p_r = q_2 \cdots q_s$. Now, by our new induction principle, these are two prime factorizations of a number smaller than n, and hence are the same, except for their order. Therefore, they have the same number of factors, that is, $r = s$, and all the factors are the same except for their order. And the number n is that product times p_1, which equals q_1, therefore the original two products, $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$, are the same except for order. Q.E.D.

Well, that finished the proof except we have to prove another theorem first, namely, theorem 4.

Theorem 4. If a prime divides a product of primes $q_1 q_2 \ldots q_s$, then it equals one of the primes $q_1, q_2, \ldots, q_s$.

We could do that, but we we'll prove a slightly stronger theorem, theorem 3.

Theorem 3. If a prime divides a product of numbers $b_1 b_2 \ldots b_s$, then it divides one of the numbers $b_1, b_2, \ldots, b_s$.

Now the reason theorem 3 implies theorem 4 is because if a prime p divides a product of primes $q_1 q_2 \ldots q_s$, then it divides one of the primes $q_1, q_2, \ldots, q_s$, but the only way that one prime can divide another is if it equals the other.

Now we're down to proving theorem 3. A product of s numbers $b_1 b_2 \ldots b_s$ is actually a series of binary products. It's b_1 times $b_2 \ldots b_s$, and $b_2 \ldots b_s$ is b_2 times $b_3 \cdots b_s$, etc, where the last product is $b_{s-1} b_s$ is the product of b_{s-1} times b_s. That means that if we knew theorem 2, then, using ordinary induction, we could conclude theorem 3.

Theorem 2. If a prime divides a product of two numbers, then it divides one of the numbers.

Now, we could prove theorem 2 directly, but it turns out that there is a slightly stronger version that we can use in other places, so let's prove it, theorem 1, instead, and show theorem 2 follows from theorem 1.

Theorem 1. If n and a are relatively prime, and $n|ab$, then $n|b$.

Proof that theorem 1 implies theorem 2: Suppose that a prime p divides ab. If p doesn't divide a, then it's relatively prime to a, so by theorem 1, it divides b. Therefore, either $p|a$ or $p|b$. Q.E.D.

Proof of theorem 1: Suppose that $(n, a) = 1$. Then 1 is a linear combination of n and a, that is, there exist numbers t and u such that

$$1 = tn + ua.$$

Multiply that equation by b to get

$$b = tnb + uab.$$

Now, if $n|ab$, then n divides the right hand side of the equation, but that equals the left hand side, so $n|b$. Q.E.D.

Discussion. This presentation is in reverse order of that in the book. Typically in a mathematics book those theorems that come first logically are presented first. Here we started with our goal and discovered the theorems that were needed to prove the goal. (Actually, I made the list longer than it needed to be by strengthening a couple of them because the stronger versions are more useful, something you can only tell with hindsight.)

The advantage to presenting theorems in their logical order is that it is easier to follow the logic. The disadvantage is that the motivation for the preliminary theorems is not apparent until the final theorem, the interesting one, is reached.

We didn't follow the text in a couple of other ways, too. For one, we proved the main theorem, theorem 5, directly using a form of induction, while the text proved it indirectly with a proof by contradiction. Generally, proofs by contradiction are easier to come up with, but they're harder to follow. Another difference is that the text used a different theorem in place of our theorem 2. The text's theorem is a little stronger than ours. It says that if a number is relatively prime to two numbers, then it's relatively prime to their product. That's actually a useful fact, so it should be noted.

Usually when we write the prime factorization of a number, we used exponents on those primes that are repeated. For instance, the number 40 had the prime factorization $2 \cdot 2 \cdot 2 \cdot 5$. An abbreviated form for this factorization is $2^3 \cdot 5$. We say that the prime 2 occurs with multiplicity 3, while the prime 5 occurs with multiplicity 1. The multiplicities are the exponents. So, in general, a number n has the prime factorization

$$n = p_1^{e_1} p_2^{e_1} \cdots p_k^{e_k}$$

where the primes $p_1, p_2, \ldots, p_k$ are all distinct, and their multiplicities are the exponents $e_1, e_2, \ldots, e_k$, respectively.

Immediate corollaries to the unique factorization theorem. A corollary is a theorem that logically follows very simply from a theorem. Sometimes it follows from part of the proof of a theorem rather than from the statement of the theorem. In any case, it should be easy to see why it's true. We can draw a couple of corollaries from the unique factorization theorem.

Corollary. The only primes that can divide a number n are the ones that appear in its prime factorization $p_1^{e_1} p_2^{e_1} \cdots p_k^{e_k}$.

Corollary. If the prime factorizations of m and n are $m = p_1^{e_1} p_2^{e_1} \cdots p_k^{e_k}$ and $n = p_1^{f_1} p_2^{f_1} \cdots p_k^{f_k}$ (where here some of the e_i's and f_i's equal 0 so we can use the same list of primes for both numbers), then their greatest common divisor $d = (m, n)$ has the prime factorization $d = p_1^{g_1} p_2^{g_1} \cdots p_k^{g_k}$ where each exponent g_i is the minimum of the corresponding exponents e_i and f_i.

As an example of the last corollary, if $m = 180 = 2^2 3^2 5^1$ and $n = 600 = 2^3 3^1 5^2$, then their GCD equals $2^2 3^1 5^1 = 60$.