THE FUNDAMENTAL THEOREM OF ARITHMETIC

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

This handout considers material covered on September 7th and September 12th. To prove our results we will need the following handy fact (proved earlier in the semester).

Lemma 1. *Let a, b, c be integers. If $a|b$ and $a|c$, then a divides any linear combination of b and c. In other words, $a|ub + vc$ for all $u, v \in \mathbb{Z}$.*

We begin with an important application of Bezout's identity:

Proposition 1. *If p is a prime number and if $p \mid ab$ where $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.*

Proof. Assume that p is a prime dividing ab. We divide the proof into cases:

CASE 1. $p|a$. Then we are done since the desired conclusion, $p \mid a$ or $p \mid b$, holds.

CASE 2. $p \nmid a$. Claim: the GCD of p and a is 1. To justify this claim observe that the positive divisors of p are p and 1 since p is a prime. The divisor p of p is not a divisor of a by assumption (for case 2), leaving 1 as the only possible common divisor.

By Bezout's identity $1 = up + va$ for some $u, v \in \mathbb{Z}$. Multiply both sides of the equation by b giving the equation $b = b(up + va) = (bu)p + v(ab)$. Since $p \mid p$ and $p \mid ab$, we know $p \mid b$ by the above lemma. □

Here is a concise version of the proof:

Proof. If $p|a$ we are done, so assume $p \nmid a$. In this case, p and a are relatively prime so $1 = up + va$ for some $u, v \in \mathbb{Z}$ (Bezout). Thus $b = (bu)p + v(ab)$. Since $p \mid ab$, we get $p \mid b$. □

The above proposition generalizes from two factors to any finite number:

Proposition 2. *If p is a prime number and if $p \mid a_1 a_2 \cdots a_n$, where each $a_i \in \mathbb{Z}$, then $p \mid a_i$ for some i.*

Proof. (Induction on n). We must first prove the statement when $n = 1$ (the "basis step"). Well if $p|a_1$ then of course $p|a_i$ with $i = 1$.

("Induction step"). Now we get to assume the statement is true for $n = k$ (the "inductive hypothesis") and we must prove the statement for $n = k + 1$. In other words, we must show that if p is a prime number and if $p \mid a_1 a_2 \cdots a_{k+1}$ then $p \mid a_i$ for some $i \in \{1, \ldots, k + 1\}$.

So assume $p \mid a_1 a_2 \cdots a_k a_{k+1}$. In other words, $p \mid b a_{k+1}$ where $b = a_1 a_2 \cdots a_k$. By the previous proposition, either $p|b$ or $p|a_{k+1}$.

CASE 1: $p|b$. So $p|a_1 a_2 \cdots a_k$ since $b = a_1 a_2 \cdots a_k$. By the induction hypothesis, this implies that $p|a_i$ for some i, and we are done.

CASE 2: $p|a_{k+1}$. We are done since $p|a_i$ with $i = k + 1$. □

Here is a concise version of the proof:

Date: Fall 2005. Version of October 1, 2005.

Proof. (Induction on n). The base case $n = 1$ is obvious. So assume the result holds for $n = k$. If $p \mid a_1 \cdots a_k a_{k+1}$ then $p|a_1 \cdots a_k$ or $p|a_{k+1}$ by the previous proposition. The result follows by the induction hypothesis in the first case, and is obvious in the second. □

The next result will be needed in the proof of the Fundamental Theorem of Arithmetic.

Lemma 2. *If $p|q$ where p and q are prime numbers, then $p = q$.*

Proof. The only positive divisors of q are 1 and q since q is a prime. Since p is also a prime, we have $p > 1$. So p is a positive divisor of q not equal to 1. Thus p must be q □

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *Let $n \geq 2$ be an integer. Then n can be written as the product of one or more primes. If $n = p_1 \cdots p_s$ and $n = q_1 \cdots q_t$ then $s = t$ and, after rearranging the q_i's, we have $p_i = q_i$ for each $i \in \{1, \ldots, s\}$. In other words, the factorization is unique up to the order of the prime factors.*

Proof. EXISTENCE OF FACTORIZATION. We prove this by contradiction. Suppose there is at least one integer $n \geq 2$ which is not the product of one or more primes. Let S be the set of such integers. This set is bounded from below (by 0 say), so by the Boundedness Principle, there is a minimum element in S since we are assuming S is not empty. Let n be the minimum element of S: so n is the smallest integer (≥ 2) which is not the product of primes.

If n is a prime then n is the product of just one prime: n itself. This gives our contradiction. If n is composite, then $n = ab$ where both a and b are integers strictly greater than 1 and strictly smaller than n. Since n is the smallest integer that is not the product of primes, it follows that $a = p_1 \cdots p_s$ and $b = q_1 \cdots q_t$ where each p_i and q_i is prime. Thus $n = p_1 \cdots p_s q_1 \cdots q_t$, a contradiction.

UNIQUENESS OF FACTORIZATION. Again we prove this by contradiction. Suppose there is at least one integer $n \geq 2$ with two different prime factorizations (in other words, two factorizations such that the second cannot be rearranged to be identical to the first). Let S be the set of such integers. This set is bounded from below (by 0 say), so by the Boundedness Principle, there is a minimum element in S since we are assuming S is not empty. Let n be the minimum element of S.

Suppose that

$$n = p_1 \cdots p_s \qquad n = q_1 \cdots q_t$$

are two distinct prime factorizations of n (and assume that they remain distinct even after rearranging the order of the product). Since n is a multiple of p_s it follows that $p_s|n$. So $p_s|q_1 \cdots q_t$ since $n = q_1 \cdots q_t$. Thus $p_s|q_i$ for some i by Proposition 2. By the above lemma, $p_s = q_i$. By rearranging the prime factors so that q_i is moved to the end (and relabeling the q_j's), we can assume that $p_s = q_t$. In other words,

$$n = p_1 \cdots p_{s-1} p_s = q_1 \cdots q_{t-1} p_s.$$

We divide into two cases:

CASE 1. $s > 1$ and $t > 1$. Then let $n' = p_1 \cdots p_{s-1}$. By the cancellation law applied to the equation $p_1 \cdots p_{s-1} p_s = q_1 \cdots q_{t-1} p_s$ we get

$$n' = p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}.$$

Since $n' < n$, we know that unique factorization applies to n'. So $t - 1 = s - 1$, in other words $s = t$, and, after rearranging factors, each $p_i = q_i$ for $i \in \{1, \ldots, s-1\}$. We also saw that $p_s = q_s$ above (remember $s = t$). So the two factorization of n are not distinct: a contradiction.

CASE 2. $s = 1$ or $t = 1$. In this case, n is prime. Since n is not composite, *both* s and t are 1. Thus $s = t = 1$. Of course, this implies that $n = p_1 = q_1$ contradicting the assumption that the two factorization were distinct. □

Here is a concise version of the proof:

Proof. Let $n \geq 2$ be the smallest integer that is not the product of primes. In particular, n is not itself a prime, so $n = ab$ where $2 < a < n$ and $2 < b < n$. Since a and b are smaller than n, they are both products of primes, so $n = ab$ is also a product of primes. Contradiction.

Now we prove uniqueness. Let $n \geq 2$ be the smallest integer with a non-unique factorization. Clearly primes satisfy unique factorization, so n is composite. Let $n = p_1 \cdots p_s = q_1 \cdots q_t$ be two distinct prime factorizations of n. Since n is not prime, both $s \geq 2$ and $t \geq 2$. Observe that $p_s | q_1 \cdots q_t$. Thus $p_s = q_i$ for some i by Proposition 2 and the above lemma. Rearrange and relabel the q_j so that $p_s = q_t$. Cancel p_s giving us $p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}$. Since $p_1 \cdots p_{s-1} < n$, we have $s - 1 = t - 1$ and, after rearranging, $p_i = q_i$ for all i. This contradicts the assumption of two distinct factorizations of n. □

Remark. This result generalizes easily to negative integers: each negative integer factors as -1 times the product of primes, and the factorization is unique up to the order of the prime factors. It holds also in the case $n = 1$: the prime factorization is considered to have no primes (and the product of zero factors is considered to be 1, just like the sum of zero terms is considered to be 0). So the Fundamental Theorem of Arithmetic holds for any non-zero integer. In fact, there is an easy generalization to non-zero rational numbers which uses possibly negative powers.

Remark. It is common to group together equal primes, and write the prime factorization of an integer n as $p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. We can even allow $e_i = 0$ when we want to emphasize that p_i does not occur in the prime factorization of n. For example,

$$12 = 2^2 3^1 = 2^2 3^1 5^0 \qquad 45 = 3^2 5^1 = 2^0 3^2 5^1.$$

The use of zero exponents is useful in the calculation of GCDs and LCMS. As we will see, the GCD is obtained by taking the minima of corresponding exponents, and the LCM is obtained by taking the maxima:

$$GCD(12, 45) = 2^0 3^1 5^0 = 3 \qquad LCM(12, 45) = 2^2 3^2 5^1 = 180.$$

The use of $e_i = 0$ can be used to give 1 a prime factorization: $1 = 2^0 = 3^0$, et cetera. The factorization is unique since in each case the primes truly involved form the empty set. By allowing $e_i < 0$ we can obtain the prime factorization of any non-zero rational number.

The prime factorization can be used to determine if an integer is a square:

Proposition 3. *Let $n \geq 2$ be an integer. Then n is a perfect square if and only if each prime p occurring in the prime factorization of n occurs an even number of times.*

Proof. Suppose $n = c^2$ is a perfect square. (We can assume that $c \geq 2$ since if c is negative we replace c with $|c|$, and $|c|$ cannot be 0 or 1 since $n \geq 2$). Write c as the product of primes: $c = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. So

$$n = c^2 = \left(p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}\right)^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_s^{2e_s}.$$

Thus each prime occurs an even number of times in the prime factorization of n.

Conversely, suppose each prime p_i occurring in the prime factorization of n occurs an even number of times: $2e_i$ times, say. Then

$$n = p_1^{2e_1} p_2^{2e_2} \cdots p_s^{2e_s} = \left(p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}\right)^2.$$

So n is a perfect square. □

Dr. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA
E-mail address: waitken@csusm.edu