UNIQUE FACTORIZATION

LECTURE NOTES: MATH 432, CSUSM, SPRING 2009. PROF. WAYNE AITKEN

In this lecture we consider the theorem that every integer $n > 1$ has an essentially unique prime factorization. This is called the *unique factorization theorem* or the *fundamental theorem of arithmetic*. It was surely known since ancient times, but it was Gauss who first recognized the need for a rigorous proof a few hundred years ago. We will only prove unique factorization for the ring $\mathbb{Z}$, but it holds for certain other rings as well, including polynomial rings. It should be noted, however, that there are other rings used in algebraic number theory where unique factorization fails.[1]

We will use the following three facts from previous lectures and courses:

Proposition 1. *Every integer $n > 1$ has a prime divisor.*

Proposition 2. *Suppose p is a prime, and that p divides a finite product:*

$$p \mid \prod_{i=1}^{k} a_i.$$

Then there is a factor a_i of this product such that $p \mid a_i$.

Proposition 3. *If each of $a_1, \ldots, a_k$ are relatively prime to c, then the product $a_1 \cdots a_k$ is relatively prime to c. In particular, units modulo c are closed under multiplication.*

The following will also be needed:

Lemma 4. *Suppose u and v are relatively prime to the prime p. If $up^k = vp^l$, then $k = l$.*

Proof. Suppose otherwise. For instance, suppose $l > k$. Then $u = vp^{l-k}$. The left hand sides is prime to p, but the right hand side is a multiple of p. This is a contradiction. □

Proposition 5. *Suppose p and q are primes and $p \mid q$. Then $p = q$.*

Proof. Since q is a prime, the only positive divisors of q are 1 and q. Now $p > 1$ since p is a prime. Thus $p = q$. □

1. Main Results

We begin with the existence result.

Lemma 6. *Every integer $n > 1$ is the product of primes. In other words, there are primes $p_1, \ldots, p_k$, where $k \geq 1$, such that*

$$n = p_1 \ldots p_k.$$

Furthermore, we can choose $p_1, \ldots, p_k$ so that $p_i \leq p_j$ whenever $i \leq j$.

Date: Spring 2009. Version of March 10, 2009.

[1]For that reason, Dedekind developed the theory of ideals (or ideal numbers), and showed that unique factorization holds at the level of ideals for a large class of rings.

Proof. (Strong Induction) If n is prime, then just choose $p_1 = n$ and $k = 1$. In particular, the result is true of $n = 2$.

Now assume the result holds for all i with $1 < i < n$. We must prove the result holds for n as well. As mentioned above, if n is prime, the result holds. Thus assume that n is composite. Let p be the largest prime divisor of n. By Proposition 1, and the fact that the set of divisors of n is finite, such a largest prime exists. So $n = mp$ for some integer $1 < m < n$. By the induction hypothesis, m is the product of primes: $m = p_1 \dots p_k$. Hence

$$n = mp = p_1 \dots p_k p.$$

By the induction hypothesis we can assume the p_i are ordered by size, and since each p_i divides n, we have $p_i \leq p$.

By the principle of strong induction, the result holds for all $n > 1$. □

Now we consider uniqueness.

Lemma 7. *Suppose $n > 1$ has two factorizations*

$$n = p_1 \dots p_r = q_1 \dots q_s$$

where each p_i and each q_i is a prime, and such that the primes appear in ascending order in the following sense: $1 \leq i \leq j \leq r$ implies $p_i \leq p_j$ and $1 \leq i \leq j \leq s$ implies $q_i \leq q_j$. Then $r = s$ and $p_i = q_i$ for each $1 \leq i \leq r$.

Proof. (Strong Induction) If n is prime, then $r = 1$ and $s = 1$, so $r = s$. We then have $p_1 = n = q_i$, so the result follows. (This covers the base case where $n = 2$).

Now assume the result holds for factorizations of i with $1 < i < n$. We must prove the result holds for n as well. Assume we are given two factorizations of n as in the hypothesis of the lemma. As mentioned above, if n is prime, the result holds. Thus assume that n is composite. In particular $r > 1$ and $s > 1$. Let p be the largest prime divisor of n. By Proposition 1, and the fact that the set of divisors of n is finite, such a largest prime exists. By Proposition 2, we have $p \mid p_i$ for some i. We have $p = p_i$ by Proposition 5. Finally, $p = p_i \leq p_r$, and p is the largest prime divisor of n, so $p = p_r$. A similar argument gives that $p = q_s$. Now divide n by p giving us n' which has the factorizations

$$n' = p_1 \dots p_{r-1} = q_1 \dots q_{s-1}.$$

By the induction hypothesis, $r - 1 = s - 1$ and $p_i = q_i$ for each i in this factorization. Since $r - 1 = s - 1$ we have $r = s$. So $p_r = p = q_r$. So $p_i = q_i$ for all $1 \leq i \leq r$.

By the principle of strong induction, the result holds for all $n > 1$. □

combining the last two lemmas gives the following:

Theorem 8. *Every integer $n > 1$ can be written as the product of primes. The factorization is essentially unique in the following sense: any two prime factorizations when written in ascending order are equal.*

2. Order function

The p-order function Ord_p, whose definition we now discuss, provides another perspective on unique factorization.

Let m be a nonzero integer and let p be a prime. Then m has a finite number of divisors. Some of these divisors are of the form p^n. For instance, p^0 is trivially a divisor of m. Since

there are a finite and nonzero number of divisors of the form p^n, there is a maximum such divisor p^k. By Lemma 4 the exponent k appearing in the divisor p^k is unique (if $p^k = p^l$ then $k = l$). We define $\mathrm{Ord}_p(m)$ to be this nonnegative number k. We summarize this as follows:

Definition 9. If m is a nonzero integer and if p is a prime, then $\mathrm{Ord}_p(m)$ is the largest integer k such that p^k divides m.

The following is an easy consequence of the definition.

Proposition 10. *Let p be a prime and m be a nonzero integer. Then $p \mid m$ if and only if $\mathrm{Ord}_p(m) > 0$.*

Proposition 11. *Let m be a nonzero integer, and p be a prime. Then $\mathrm{Ord}_p(m) = k$ if and only if $m = up^k$ for some u relatively prime to p.*

Proof. First suppose that $\mathrm{Ord}_p(m) = k$. Then by the above definition p^k divides m. So $m = up^k$ for some u. We need to show that u is prime to p. Suppose otherwise, that $u = wp$. Then $m = wp^{k+1}$, contradicting the fact that k is the largest integer such that $p^k \mid m$.

Now suppose $m = up^k$ where u is prime to p. Let $l = \mathrm{Ord}_p(m)$. By the first half of the proof $m = vp^l$ for some v prime to p. Thus $up^k = vp^l$. By Lemma 4, we have $k = l$. So $k = \mathrm{Ord}_p(m)$. □

Corollary 12. *If p is a prime and u is an integer such that $p \nmid u$, then*

$$\mathrm{Ord}_p(up^k) = k.$$

Proposition 13. *Let p be a prime. If $a, b \in \mathbb{Z}$ are non-zero then*

$$\mathrm{Ord}_p(ab) = \mathrm{Ord}_p(a) + \mathrm{Ord}_p(b).$$

More generally, if each $a_1, \ldots, a_n \in \mathbb{Z}$ is nonzero then

$$\mathrm{Ord}_p(a_1 \cdots a_n) = \mathrm{Ord}_p(a_1) + \ldots + \mathrm{Ord}_p(a_n).$$

Proof. Let $k = \mathrm{Ord}_p(a)$ and $l = \mathrm{Ord}_p(b)$. By Proposition 11, $a = p^k m$ and $b = p^l n$ for some $m, n \in \mathbb{Z}$ with $p \nmid m$ and $p \nmid n$. Thus

$$ab = \left(p^k m\right)\left(p^l n\right) = p^{k+l}(mn).$$

By Proposition 3, $p \nmid mn$. Therefore, $\mathrm{Ord}_p(ab) = k + l$ by Corollary 12.

The second statement follows by a straightforward induction argument. □

Proposition 14. *If $a \in \mathbb{Z}$ is non-zero and if $k \geq 0$ then*

$$\mathrm{Ord}_p\left(a^k\right) = k\,\mathrm{Ord}_p(a).$$

Proof. The case $k = 0$ follows from the observation that $\mathrm{Ord}_p(1) = 0$. Now suppose that the result holds for a particular k. Then

$$\begin{aligned}
\mathrm{Ord}_p\left(a^{k+1}\right) &= \mathrm{Ord}_p\left(a^k a\right) && \text{(Law of exponentiation)} \\
&= \mathrm{Ord}_p\left(a^k\right) + \mathrm{Ord}_p\left(a\right) && \text{(Prop. 13)} \\
&= k\,\mathrm{Ord}_p(a) + \mathrm{Ord}_p(a) && \text{(Induction Hyp.)} \\
&= (k+1)\mathrm{Ord}_p(a).
\end{aligned}$$

The result follows from the principle of induction. □

We can use these properites of the order function to prove the following:

Proposition 15. *Suppose $p_1, \ldots, p_k$ are distinct primes. Then*

$$\mathrm{Ord}_p\left(p_1^{m_1} \cdots p_k^{m_k}\right) = \begin{cases} m_i & \text{if } p = p_i \\ 0 & \text{if } p \notin \{p_1, \ldots, p_k\} \end{cases}$$

Proof. Using the previously proved properties of the order function gives

$$\mathrm{Ord}_p\left(p_1^{m_1} \cdots p_k^{m_k}\right) = m_1 \mathrm{Ord}_p(p_1) + \ldots + m_k \mathrm{Ord}_p(p_k).$$

Now observe that $\mathrm{Ord}_p(p_i) = 1$ if $p = p_i$, but $\mathrm{Ord}_p(p_i) = 0$ if $p \neq p_i$. The result follows. □

3. Another Version of Unique Factorization

We now use the order function to give another version of the unique factorization theorem. We begin with a useful formula that, as a byproduct, gives the existence of a factorization into prime powers.

Proposition 16 (Product formula)**.** *Let n be a positive integer, and let $p_1, \ldots, p_k$ be a finite sequence of distinct primes that includes every prime divisor of n. Then*

$$n \;=\; \prod_{i=1}^{k} p_i^{\mathrm{Ord}_{p_i}(n)}.$$

Remark. Informally, this can be shown (when $n > 1$) by writing n as the product of primes $q_1 \ldots q_n$, and observing that $\mathrm{Ord}_p(q_1 \ldots q_n)$ is just the number of q_i equal to p. One then groups together equal q_i in the prime factorization of n. What follows is a more formal proof that uses strong induction.

Proof. (Strong induction) If $n = 1$, then $\mathrm{Ord}_{p_i}(n) = 0$ for each p_i. The result now follows from the fact that $p_i^0 = 1$, and the fact that $1 \cdots 1 = 1$.

Now assume that $n > 1$ and that the the result holds for all positive integers less than n. Let $p_1, \ldots, p_k$ be a sequence of distinct primes that includes every prime divisor of n. Let p_u be a prime divisor of n. So $n = m\,p_u$ for some positive integer $m < n$. Observe that every prime divisor of m is a prime divisor of n, so $p_1, \ldots, p_k$ is a sequence of distinct primes that includes every prime divisor of m. By the induction hypothesis,

$$m \;=\; \prod_{i=1}^{k} p_i^{\mathrm{Ord}_{p_i}(m)}.$$

Observe that $\mathrm{Ord}_p(n) = \mathrm{Ord}_p(m) + \mathrm{Ord}_p(p_u)$ holds for all primes p. In particular, if $p \neq p_u$ then $\mathrm{Ord}_p(m) = \mathrm{Ord}_p(n)$, but if $p = p_u$ then $\mathrm{Ord}_p(m) = \mathrm{Ord}_p(n) - 1$. Thus

$$m \;=\; \left(\prod_{i=1}^{u-1} p_i^{\mathrm{Ord}_{p_i}(n)}\right) p_u^{\mathrm{Ord}_{p_u}(n)-1} \left(\prod_{i=u+1}^{k} p_i^{\mathrm{Ord}_{p_i}(n)}\right)$$

(Where we adopt the convention the first term is 1 if $u = 1$, and the last term is 1 if $u = k$). Now multiply both sides by p_u and simplify both sides. This gives

$$n \;=\; m\,p_u \;=\; \left(\prod_{i=1}^{u-1} p_i^{\mathrm{Ord}_{p_i}(n)}\right) p_u^{\mathrm{Ord}_{p_u}(n)} \left(\prod_{i=u+1}^{k} p_i^{\mathrm{Ord}_{p_i}(n)}\right) = \prod_{i=1}^{k} p_i^{\mathrm{Ord}_{p_i}(n)}$$

as desired.

By the principle of strong induction, the result holds for all positive n. □

The following gives a uniqueness result

Proposition 17. *Suppose $N > 1$ is an integer with factorizations*

$$N = p_1^{m_1} \cdots p_r^{m_r} = q_1^{n_1} \cdots q_s^{n_s}$$

where $p_1, \ldots, p_r$ are distinct primes, where $q_1, \ldots, q_s$ are distinct primes, and where each m_i and n_j is positive. Then each p_i is equal to some q_j and $m_i = n_j$. Similarly, each q_j is equal to some p_i and $n_j = m_i$.

Proof. Let $p = p_i$. By Proposition 15, $\mathrm{Ord}_p(N) = m_i$. So $\mathrm{Ord}_p(N) > 0$. By Proposition 15 again, applied to the second factorization, there must be a q_j such that $p = q_j$ and $\mathrm{Ord}_p(N) = n_j$. We have then $p_i = p = q_j$, and $m_i = \mathrm{Ord}_P(N) = n_j$.

A similar argument gives the second result. □