Math 313/623 Notes 2

David L. Meretzky

Thursday February 7th, 2019

> Plato said, "God is a geometer". Jacobi changed this to, "God is an arithmetician." Then came Kronecker and fashioned the memorable expression, "God created the natural numbers, and all the rest is the work of man."
>
> *Felix Klein*

Recall from last class that the major theorem we obtained was that relative to some modulus, each number has a unique least positive residue. Today we will go over two approaches to one of the first major theorems in multiplicative number theory, that every number has a unique prime factorization. In Gauss's approach, the heavy lifting is relegated to article 13.

2 Congruences of the First Degree

2.1 Preliminary theorems regarding prime numbers, factors etc.

Article 13. The product of two positive numbers each of which is smaller than a given prime number cannot be divided by this prime number. Said another way, let p be prime, and $0 < a < p$, then no positive number $b < p$ can be found such that $ab \equiv 0 \pmod{p}$.

The proof is by contradiction.

Proof. Suppose the theorem is false. Then there is a collection of numbers $b_1, ..., b_n$ such that each $b_i < p$ and $ab_i \equiv 0 \pmod{p}$. Let b be the smallest such number in that collection. It is clear that $b > 1$, because otherwise we run into trouble. If $b = 1$, then $ab = a$ and since $a < p$ by hypothesis, p cannot possibly divide ab. Now p is prime, and therefore b cannot divide it. So p lies between successive multiples of b. There exists some m such that

$$bm < p < b(m + 1). \tag{1}$$

Subtracting bm from equation (1) we obtain

$$0 < p - bm < b.$$

Let $b' = p - bm$. We have that b' is smaller than b. The contradiction in this proof will be that b' must be in the collection of numbers $b_1, ..., b_n$ such that each $b_i < p$ and $ab_i \equiv 0 \pmod{p}$. We compute $ab' = ap - abm$. Since $p \equiv 0 \pmod{p}$ and $ab \equiv 0 \pmod{p}$ it follows by article 7 that $ap \equiv 0 \pmod{p}$ and $abm \equiv 0 \pmod{p}$ and by article 6 that $ap - abm \equiv 0 \pmod{p}$. It follows that $ab' \equiv 0 \pmod{p}$ which is a contradition since b is the smallest such number that has the property $ab' \equiv 0 \pmod{p}$. □

Article 14. If neither a nor b can be divided by a prime number p then the product ab cannot be divided by p.

Proof. Let α and β be the least positive residues of a and b respectively, relative to the modulus p. Now if $ab \equiv 0 \pmod{p}$ then since $ab \equiv \alpha\beta$, we have that $\alpha\beta \equiv 0 \pmod{p}$ which contradicts the previous article. □

The above article can be restated in terms of the contrapositive: If a prime p divides ab then p divides a or p divides b. This is an important characterization of primes. In particular, for all numbers a and b, if a number p divides ab means that p must divide either a or b then p is prime. For suppose p is composite. $p = kl$, then p divides itself, but p divides neither k nor l, since both are strictly less than p. Thus we can take this property to be the definition of primality if we so desire. In some contexts this will be an easier definition to work with.

Article 15. If none of the numbers a, b, c, d, etc. can be divided by a prime p, neither can their product $abcd$ etc.

Proof. by the previous article, ab cannot be divided by p. Then in the previous article if we let $a = ab$ and $b = c$, we have that abc cannot be divided by p. Then in the previous article if we let $a = abc$ and $b = d$, we have that $abcd$ cannot be divided by p. Continue in this manner to obtain the result. □

Unique factorization for the integers.

Article 16. A composite number can be resolved into prime factors in only one way.

Proof. Assume for the time being that such a factorization exists. This is not difficult to prove and we shall do so shortly. Uniqueness is more difficult to prove. Given a number $A = a^\alpha b^\beta c^\gamma$ etc. where a, b, and c etc. are distinct prime numbers and α, β, and γ etc. are positive integers. Suppose that there is some second system of facors which equal A. Clearly, $A|A$ so each system must divide the other. Furthermore, suppose there is a prime factor p which appears in the second system but not in the first. Since p appears in the second system $p|A$. However, p does not appear in the first system. Each prime of the first system is not divisible by anything except 1 and itself, and definitely not p, so by the previous article, $p \nmid A$. So we have a contradiction. The prime factors in both factorization systems must be the same. However, the powers which each prime factor has may differ in each system. Suppose a prime p occurs in a

two factorizations with multiplicity m and n. That is, in one system we have a facor of p^m and in another we have a facor of p^n. Without loss of generality we may assume that $m < n$. Now consider A/p^n. In one system we will have p^{m-n} and in the other we will have no powers of p. Then one facorization does not contain the prime p while the other contains it p^{m-n} times, which contradicts what we showed in the first part of the proof. □

Unique factorization is a big deal. Things really fall apart if we dont have unique factorization. In fact, most of the number systems that we will look at will have unique factorization. We will now switch to notes based on Kenneth Ireland and Michael Rosen's text *A Classical Introduction to Modern Number Theory.*

Unique Factorization

Unique Factorization in $\mathbb{Z}$

We begin by recovering the portion of article 16 which we omitted.

Lemma 1. Every nonzero integer can be written as a product of primes.

Proof. Assume the collection of integers which cannot be written as a product of primes is not empty. Then N be the smallest positive integer which cannot be written as a product of primes. Since N cannot be prime $N = mn$, where $1 < n, m < N$. Since both n and m are smaller than N, they must each be a product of primes. Thus their product, $mn = N$, is a product of primes which is a contradiction. There is also a direct proof by induction. □

Definition 1. Let $n \in \mathbb{Z}$ and p be prime. Then if n is not zero, there is a nonnegative integer a such that $p^a | n$ but $p^{a+1} \not| n$. Roughly, a is the number of times that p divides n. If $p \not| n$ then $a = 0$ because $p^0 = 1$ which divides everything. We call a the order of p in n and denote it $ord_p(n) = a$. If $n = 0$, set $ord_p(n) = \infty$.

By lemma 1, every number n can be written as

$$n = (-1)^{\epsilon(n)} p_1^{a_1} p_2^{a_2} ... p_m^{a_m}$$

where $\epsilon(n)$ is 0 if n is positive and 1 if n is negative.

Here is a restatement and sharpened form of unique factorization.

Theorem 1. For every nonzero integer n there is a prime factorization

$$n = (-1)^{\epsilon(n)} \prod_p p^{a(p)},$$

with the exponents uniquely determined by n. In fact $a(p) = ord_p(n)$.

Such a factorization exists because of the previous lemma. The uniqueness is more difficult.

Lemma 2. If $a, b \in \mathbb{Z}$ and $b > 0$, there exists $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.

Proof. Consider the set $a + b\mathbb{Z}$. This set contains positive elements. Let $r = a - bq$ be the least positive element. (These elements are actually the residues of a modulo b). We claim that $0 \leq r < b$, for if not, then $r = a - bq > b$ and so $0 \leq a - (q+1)b < r$, which contradicts the minimality of r. □

Note that the above lemma will play exactly the same role in the proof of unique factorization that every number has a unique least positive residue. It follows that r is this number. So lemma 2 is analogous to article 3.

Definition 2. If $a_1, ..., a_n$ are integers, then let $(a_1, ..., a_n)$ denote the collection of all integers of the form $x_1a_1 + ... + x_na_n$. Integers of this form are called linear combinations of the list $a_1, ..., a_n$. Collections of this form are called ideals of $\mathbb{Z}$. Note that if $c, d \in (a_1, ..., a_n)$, then $c - d$ and $c + d$ are also in $(a_1, ..., a_n)$. Letting all $x_i = 0$, we see that $0 \in (a_1, ..., a_n)$. Note that $(a) = a\mathbb{Z}$.

Lemma 3. For any $a, b \in \mathbb{Z}$, there exists a $d \in \mathbb{Z}$ such that $(a, b) = (d)$.

Proof. Let d be the least positive element of (a, b). Then $d = x_1a + x_2b$ for some x_1 and x_2. Clearly, any element of (d) is of the form $x_3d = x_3(x_1a + x_2b) = x_3x_1a + x_3x_2b \in (a, b)$. Thus $(d) \subset (a, b)$.

To show the reverse inclusion, let c be any positive element of (a, b). Since d is the least positive element of (a, b) we have $d < c$. We can then apply lemma 1 to obtain q, r such that $c = qd + r$ where $0 \leq r < d$. Since c and qd are both in (a, b), $c - qd \in (a, b)$ and therefore, $r \in (a, b)$. Since d is the least postive element, $r = 0$ and $c = qd \in (d)$. □

Definition 3. Let $a, b \in \mathbb{Z}$, their greatest common divisor is a number d such that $d|a$ and $d|b$ and if a and b have any other common divisor, c, such that $c|a$ and $c|b$, then $c|d$.

Lemma 4. Let $a, b, d \in \mathbb{Z}$ such that $(a, b) = (d)$, then d is the greatest common divisor of a and b.

Proof. We need to verify the previous definition.

Since $a \in (d)$ and $b \in (d)$, there exist $k, l \in \mathbb{Z}$ such that $a = kd$ and $b = ld$, thus $d|a$ and $d|b$ suppose that c is any common divisor of a and b. Then $c|a$ and $c|b$ furthermore, for any $x, y \in \mathbb{Z}$, $c|xa$ and $c|yb$, therefore, by exercise 7 at the end of lecture 1 we have $c|(xa + yb)$ and therefore, c divides any element of (a, b). Since $d \in (a, b)$, $c|d$ as desired. □

Definition 4. We say that two integers a and b, are relatively prime if their greatest common divisor is 1 or -1, that is $(a, b) = (1)$ or $(a, b) = (-1)$. Note that $(1) = (-1) = 1\mathbb{Z} = \mathbb{Z}$.

For instance, 14 and 25 are relatively prime. Also 7 and 3 are relatively prime. However, 4 and 6 are not.

Proposition 1. Suppoe $a|bc$ and that $(a, b) = (1)$, then $a|c$.

Proof. Since $(a, b) = (1)$, there exist $r, s \in \mathbb{Z}$ such that $ar + bs = 1$, then $acr + bcs = c$. Since we are assuming $a|bc$, then since $a|acr$ and $a|bcs$ we have $a|(acr + bcs)$ and therefore, $a|c$. □

Corollary 1. If p is a prime and $p|bc$ then $p|b$ or $p|c$.

Proof. Left as an exercise, or look in the text. When you are finished, see article 14 and the discussion following it. □

Corollary 2. Suppose that p is prime and that $a, b \in Z$, then $ord_p(ab) = ord_p(a) + ord_p(b)$.

Try to prove yourself. This is straightforward. The function ord should remind you of the log function. Think about how they are related.

Proof. Let $\alpha = ord_p(a)$ and $\beta = ord_p(b)$. Then $a = p^\alpha c$ where $p \not| c$ and $b = p^\beta d$ where $p \not| d$ because otherwise $p^{\alpha+1}|a$ and $p^{\beta+1}|b$. Then $ab = p^{\alpha+\beta}cd$ and by the previous corollary, $p \not| cd$, thus $ord_p(ab) = \alpha + \beta = ord_p(a) + ord_p(b)$. □

We can now prove the uniqueness in theorem 1. All that we have to do is prove that the exponents $a(p) = ord_p(n)$.

Proof. Let q be any prime. Apply ord_q to both sides of the equation

$$n = (-1)^{\epsilon(n)} \prod_p p^{a(p)},$$

to obtain

$$ord_q(n) = ord_q((-1)^{\epsilon(n)} \prod_p p^{a(p)}) = ord_q((-1)^{\epsilon(n)}) + \sum_p ord_q(p^{a(p)}). \quad (1)$$

Clearly, $ord_q((-1)^{\epsilon(n)}) = 0$ and

$$ord_q(p^{a(p)}) = a(p) ord_q(p)$$

by the log-like property following from corollary 2. Note that by definition however, $ord_q(p) = 1$ if $q = p$ and $ord_q(p) = 0$ if $q \neq p$. Thus equation (1) becomes $ord_q(n) = a(p)$ when $q = p$. □

Exercises

1. Prove corollary 1 and 2 without looking.

2. For every number n and prime number p prove there exists a p-adic representation, that is, n can be put into the form $n = a_0p^0 + a_1p^1 + a_2p^2 + ... + a_kp^k$. Hint: Use lemma 2.

3. Make a number of examples for yourself of $ord_p(n)$ and $log_p(n)$ for different primes p and different n.

4. State and prove the relationship between $ord_p(n)$ and the p-adic representation of n.

5. State and prove the relationship between $log_p(n)$ and the p-adic representation of n.

6. Let a, b, and c be integers. Then $(a + cb, b) = (a, b)$.

7. Prove that if e and d are integers and $e = dq+r$ where q and r are integers, then $(e, d) = (d, r)$. Hint: use a lemma.

8. Let a and b be integers such that $0 < b \leq a$. Prove that if we apply lemma 2 over and over again such that first we have $a = bq_1 + r_1$, then by lemma 2 we next get $b = r_1q_2 + r_2$, then again by the lemma we have $r_1 = r_2q_3 + r_3$ and so on, show that eventually some $r_n = 0$, and furthermore, the last non-zero r_i is the greatest common divisor of a and b, that is, $(a, b) = (r_{n-1})$. Hint: use the previous exercise.

9. Do the other exercises within these notes.