Math 126 Number Theory

Prof. D. Joyce, Clark University

27 Jan 2006

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

For next time. Finish reading section 2.1 and begin section 2.2.

Last meeting. We discussed Dedekind's concept of numbers. Dedekind realized that the names of the numbers aren't relevant to defining them, and came up with the following axioms to define a simply infinite set, which was his definition for a set $\mathbf{N}$ of natural numbers.

Definition. (Dedekind) A set $\mathbf{N}$ is said to be *simply infinite* when there exists a one-to-one function $\mathbf{N} \xrightarrow{\prime} \mathbf{N}$ called the *successor function*, such that there is an element, called the *initial element* and denoted 1, that is not the successor of any element, and if a subset S of $\mathbf{N}$ contains 1 and is closed under the successor function, then $S = \mathbf{N}$.

Such a simply infinite set $\mathbf{N}$ is characterized by an element 1 and a transformation $\mathbf{N} \xrightarrow{\prime} \mathbf{N}$ satisfying the following conditions:

1. $\forall n, m, n \neq m$ implies $n' \neq m'$.
2. $\forall n, 1 \neq n'$.
3. If $S \subseteq \mathbf{N}$, $1 \in S$, and ($\forall n, n \in S$ implies $n' \in S$), then $S = \mathbf{N}$.

The Dedekind/Peano axioms are this last characterization involving 1, the successor function, and the three conditions.

Today. Some elementary properties of divisibility, greatest common divisors, and the Euclidean algorithm.

We'll restrict our discussion of numbers today to $\mathbf{N}$, the natural numbers, that is, the set of positive integers.

Recall that an integer m *divides* an integer n, written $m|n$, if there exists an integer k such that $mk = n$. A few basic properties of divisibility follow directly from this definition. Euclid uses some of these in Book VII of his *Elements*.

1. 1 divides every number. $1|n$.
2. Each number divides itself. $n|n$.
3. If one number m divides another number n, then m divides any multiple of n. $m|n$ implies $m|kn$.
4. Divisibility is a transitive relation, that is, $m|n$ and $n|k$ imply $m|k$.
5. If one number divides two other numbers, then it divides both their sum and difference. $m|n$ and $m|k$ imply $m|(n+k)$ and $m|(n-k)$.
6. Cancellation law. One number divides another if and only if any multiple of that one number divides the same multiple of the other number. $m|n \iff kn|kn$.

The divisors of a number can be displayed graphically in what is called a Hasse diagram of the lattice of divisors. We'll look at a few of those in class.

More on prime numbers. We know that there are infinitely many primes, and that every number is a product of primes. Now let's prove those statements. We'll start by proving something that will help us prove these two statements. If a theorem is not particularly interesting, but is useful in proving an interesting statement, then it's often called a lemma. This one is found in Euclid's *Elements.*

Lemma. Every number greater than 1 has at least one prime divisor.

Proof: Let n be an integer greater than 1. We'll find a prime divisor of n. Let m be the smallest divisor of n greater than 1. (Note that we're using the minimization principle, also called the well-ordering principle, to conclude that such an m exists.) We'll show that m is prime thereby proving the lemma. We'll do that with a proof by contradiction, and that means that first we'll suppose that m is not prime, then derive a contradiction, and that will imply that m must be prime.

Suppose m is not prime, but composite. Them m is the product of two integers, j and k, each greater than 1. Now, $k|m$ and $m|n$, so $k|n$. But $k < m$. That gives us a divisor of n which is even smaller than m but still greater than 1. That contradicts the fact that m is the smallest divisor of n greater than 1. Thus, m is prime, and it's a divisor of n. Q.E.D

Now we can prove one of the two statements.

Theorem. Every number greater than 1 is either a prime or the product of primes.

Proof: This will be another proof by contradition that uses the well-ordering principle.

Suppose that the theorem is false. Then there is some composite number greater than 1 that that is not the product of primes. Let N be the smallest such. By our lemma, this N has some prime divisor, call it p. Then $n = N/p$ is a number smaller than N but larger than 1, so, by the minimality of N, n is either prime or the product of primes. In the first case, when n is prime, then $N = pn$ is the product of two primes. In the second case when n is a product of primes, then $N = pn$ is also a product of primes. In any case, N is the product of primes, a contradiction. Thus, the theorem is true. Q.E.D

Next, let's prove the other statement, that there are infinitely many primes. This is Euclid's proof.

Theorem. There are infinitely many primes.

Proof: Again, this is a proof by contradiction.

Suppose that there are only finitely many primes, namely, $p_1, p_2, \ldots, p_k$. Let n be one more than the product of these primes,

$$n = p_1 p_2 \cdots p_k + 1.$$

By our lemma n has a prime factor, call it p. Since $p_1, p_2, \ldots, p_k$ are all the primes, therefore p must be one of them. Being one of them p divides their product $p_1 p_2 \cdots p_k$. But p also divides $n = p_1 p_2 \cdots p_k + 1$. Therefore, p divides the difference 1. But the prime p can't divide 1 since $p > 1$. From that contradiction, we conclude that there are infinitely many primes. Q.E.D

The Euclidean algorithm. Last time we outlined the Euclidean algorithm, an algorithm to compute the greatest common divisor of two numbers m and n.

Euclid defined the *greatest common divisor* of two numbers m and n, often denoted $\text{GCD}(m, n)$ or more simply just (m, n), is defined as the largest number d which is at the same time a divisor of m and a divisor of n.

There are two forms of the Euclidean algorithm. The first form, as Euclid stated it, repeatedly subtracts the smaller number from the larger replacing the larger by the difference, until the two numbers are reduced to the same number, and that's the greatest common divisor. (Note that the process has to stop by the well-ordering principle since at each step the larger number is reduced.)

The other form speeds up the process. Repeatedly divide the smaller number into the larger replacing the larger by the remainder. (This speeds up the process because if the smaller number is much smaller than the larger, you don't have to subtract it from the larger many times, just divide once and take the remainder which is the same as what you'd get if repeatedly subtracted it.)

We saw that this Euclidean algorithm works to produce the GCD, and the argument only depended on the principle mentioned above that if one number divides two other numbers, then it divides both their sum and difference.

Sometimes the GCD of two numbers turns out to be 1, and in that case we say the two numbers are *relatively prime*.

We can get more out of the Euclidean algorithm than just the GCD of two numbers, and we'll see what that is next time.