Number Theory I

Margaret M. Fleck

11 September 2009

This lecture covers elementary number theory concepts found in sections 3.4 and 3.5 of Rosen.

1 Recap

Quiz next Wednesday (16th).

Latex getting-started session 2-4pm this Saturday (12th) in 2405 Siebel.

2 Number Theory

We've now covered most of the basic techniques for writing proofs. So we're going to start applying them to specific topics in mathematics, starting with number theory.

Number theory is a branch of mathematics concerned with the behavior of integers. It has very important applications in cryptography and in the design of randomized algorithms. Randomization has become an increasingly important technique for creating very fast algorithms for storing and retrieving objects (e.g. hash tables), testing whether two objects are the same (e.g. MP3's), and the like. Much of the underlying theory depends on facts about which numbers evenly divide one another and which numbers are prime.

3 Factors and multiples

You've undoubtedly seen some of the basic ideas (e.g. divisibility) somewhat informally in earlier math classes. However, you may not be fully clear on what happens with special cases, e.g. zero, negative numbers. We also need clear formal definitions in order to write formal proofs. So, let's start with

> Definition: Suppose that a and b are integers. Then a divides b if $b = an$ for some integer n. a is called a factor or divisor of b. b is called a multiple of a.

If b is non-zero and a is zero, clearly we can't have $b = an$. However, there is disagreement about how to handle the case where both a and b are both zero. Some authors allow zero to be a divisor and/or multiple of itself; some explicitly restrict one or both definitions so as to require a to be non-zero. I'll leave the definition in its simpler form, which disagrees with Rosen. This won't be a big problem because we won't have much use for this special case.

The shorthand for a divides b is $a \mid b$. Be careful about the order. The divisor is on the left and the multiple is on the right.

Some examples:

- $7 \mid 77$
- $77 \nmid 7$
- $7 \mid 7$ because $7 = 7 \cdot 1$
- $7 \mid 0$ because $0 = 7 \cdot 0$, zero is divisible by any integer.
- $0 \nmid 7$ because $0 \cdot n$ will always give you zero, never 7.
- $(-3) \mid 12$ because $12 = 3 \cdot -4$
- $3 \mid (-12)$ because $-12 = 3 \cdot -4$

A number p is even exactly when $2 \mid p$. The fact that zero is even is just a special case of the fact that zero is divisible by any integer.

4 Direct proof with divisibility

We can prove basic facts about divisibility in much the same way we proved basic facts about even and odd.

Claim 1 *For any integers a,b,and c, if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.*

> Proof: Let a,b,and c and suppose that $a \mid b$ and $a \mid c$.
>
> Since $a \mid b$, there is an integer k such that $b = ak$ (definition of divides). Similarly, since $a \mid c$, there is an integer j such that $c = aj$. Adding these two equations, we find that $(b + c) = ak + aj = a(k + j)$. Since k and j are integers, so is $k + j$. Therefore, by the definition of divides, $a \mid (b + c)$. $\square$

When we expanded the definition of divides for the second time, we used a fresh variable name. If we had re-used k, then we would have wrongly forced b and c to be equal.

The following two claims can be proved in a similar way:

Claim 2 *For any integers a,b,and c, if $a \mid b$ and $b \mid c$ then $a \mid c$. (Transitivity of divides.)*

Claim 3 *For any integers a,b, and c, if $a \mid b$, then $a \mid bc$.*

You've probably seen "transitivity" before in the context of inequalities. E.g. if $a < b$ and $b < c$, then $a < c$. We'll get back to the general notion of transitivity later in the term.

5 Prime numbers

We're all familiar with prime numbers from high school. Firming up the details:

> Definition: an integer $q \geq 2$ is prime if the only positive factors of q are q and 1. An integer $q \geq 2$ is composite if it is not prime.

For example, among the integers no bigger than 20, the primes are 2, 3, 5, 7, 11, 13, 17, and 19.

A key fact about prime numbers is

> Fundanmental Theorem of Arithmetic: Every integer ≥ 2 can be written as the product of one or more prime factors. Except for the order in which you write the factors, this prime factorization is unique.

The word "unique" here means that there is only one way to factor each integer.

For example, $260 = 2 \cdot 5 \cdot 13$ and $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

We won't prove this theorem right now, because it requires a proof technique called "induction," which we won't see for three weeks.

There are quite fast algorithms for testing whether a large integer is prime. However, even once you know a number is composite, algorithms for factoring the number are all fairly slow. The difficulty of factoring large composite numbers is the basis for a number of well-known cryptographic algorithms (e.g. the RSA algorithm).

6 gcd and lcm

If c divides both a and b, then c is called a **common divisor** of a and b. The largest such number is the **greatest common divisor** of a and b. Shorthand for this is $\gcd(a, b)$.

You can find the GCD of two numbers by inspecting their prime factorizations and extracting the shared factors. For example, $70 = 2 \cdot 5 \cdot 7$ and $130 = 2 \cdot 5 \cdot 13$. So $\gcd(70, 130)$ is $2 \cdot 5 = 10$. Next week, we'll see a more efficient way to compute the GCD.

Similarly, a common multiple of a and b is a number c such that $a|c$ and $b|c$. The least common multiple (lcm) is the smallest such number. The lcm can be computed using the formula:

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

For example, $\text{lcm}(70, 130) = \frac{70 \cdot 130}{10} = 910$.

If two integers a and b share no common factors, then $\gcd(a, b) = 1$. Such a pair of integers are called **relatively prime**.

7 There are infinitely many prime numbers

We can now prove a classic result about prime numbers. So classic, in fact, that it goes back to Euclid, who lived around 300 B.C.

> Euclid's Theorem: There are infinitely many prime numbers.

This is a lightly disguised type of non-existence claim. The theorem could be restated as "there is no largest prime" or "there is no finite list of all primes." So this is a good situation for applying proof by contradiction.

> Proof: Suppose not. That is, suppose there were only finitely many prime numbers. Let's call them p_1, p_2, up through p_n.
>
> Consider $Q = p_1 p_2 \cdots p_n + 1$.
>
> If you divide Q by one of the primes on our list, you get a remainder of 1. So Q isn't divisible by any of the primes p_1, p_2, up through p_n. However, by the Fundamental Theorem of Arithmetic, Q must have a prime factor (which might be either itself or some smaller number). This contradicts our assumption that p_1, p_2,$\ldots p_n$ was a list of all the prime numbers. □