CHAPTER I

Foundations of Number Theory

1. In the beginning ...

Number theory is, not surprisingly, the study of properties of the **numbers**, which are simply $\{1, 2, 3, \ldots\}$. Sometimes these are called whole numbers, or natural numbers. And sometimes people include 0 as a number, and sometimes they don't. Both definitions are fine, as long as you make sure you know which one is in force whenever you read something. In these notes, when we say "number" without any other description, we'll always mean a positive, nonzero number.

Of course it's hard to study numbers without letting 0 tag along for the ride, and in fact we can even permit all the negatives of the numbers to join in the fun, yielding the **integers** which are $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. On a really permissive day, we might even deign to consider **rational numbers**—fractions with integers as their numerators and denominators (except, of course, 0 cannot be a denominator)—and still call it number theory. But that's where we'll draw the line: no arbitrary real numbers, no imaginary numbers, nothing crazy.

There are a few important properties of numbers that we want to state right away, so we can use them later in our proofs. No mathematics can be done without assuming *something*, so think of the facts in this section as assumptions about numbers, and don't worry about it until/unless you ever take a course in the foundations of mathematics. Here's the first one:

FACT 1.1. *If you have a collection of numbers (with at least one number in the collection), then the collection has a smallest number.*

As it turns out, this property is actually a sneaky way of restating the principle of induction. (See the Glossary for a definition of induction, or of any other term you might find unfamiliar while reading these notes.) Certainly this property doesn't hold for *negative* integers, since the collection $\{-1, -2, -3, \ldots\}$ does not have a smallest member. Notice that this property doesn't hold for rational numbers (or real numbers) either: the collection $\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$ also fails to have a smallest member.

FACT 1.2. *If we start writing down a sequence of (positive) numbers one by one, and each number is smaller than the previous one, then eventually we will write down the number 1 (at which point we must stop, of course, if we're only allowing ourselves positive numbers). Very similarly, if we start writing down a sequence of nonnegative integers one by one, and each number is smaller than the previous one, then eventually we will write down the number 0.*

Again, this turns out to be yet another way of stating the principle of induction. So if you're willing to believe Fact 1.1, you're probably willing to believe Fact 1.2 (a fact which seems pretty natural, after all).

We said that we wouldn't dirty our hands with real numbers in our study of number theory, but there is one thing about them that we probably should point out:

FACT 1.3. *If x is any positive real number, no matter how small, and y is any positive real number, no matter how large, then there is a number n such that $nx > y$.*

In other words, no matter how small your steps are, if you take enough of them you'll eventually overtake even the biggest giant who only takes one step. Not too controversial.

We'll also take for granted all of the mundane, intuitive facts about numbers from our everyday exposure to them: you can add and multiply two numbers and get another number, you can subtract two integers and get another integer, every number except 1 comes after another number, and so on. (Notice we didn't mention division here! As you know, when you restrict yourself to whole numbers, division has some twists to it ... which leads very well into the next section of the notes.)

2. Divisibility

An integer a is **divisible** by another integer b, if there is some third integer c such that $a = b \times c$. There are many ways of phrasing this relation:

- a is divisible by b;
- b divides a;
- a is a multiple of b;
- b is a divisor of a;
- b is a factor of a.

We write $b \mid a$ as a shorthand notation for "b divides a". Let's get our feet wet by stating and proving a few facts about divisibility.

FACT 1.4. *A factor of a factor of an integer is itself a factor of the integer: If $b \mid a$ and $c \mid b$, then $c \mid a$.*

Proof: This is just an exercise in using the definition of divisibility. Since $b \mid a$, there is some integer m such that $a = mb$. Also, since $c \mid b$, there is some integer n such that $b = nc$. Combining these two equations, we have

$$a = mb = m(nc) = (mn)c.$$

We see that there is an integer, namely mn, that we can multiply c by to get a, and that tells us that $c \mid a$. $\square$

FACT 1.5. *If two integers are divisible by a certain factor, then so is their sum and difference: If $b \mid a$ and $b \mid a'$, then $b \mid (a + a')$ and $b \mid (a - a')$.*

The proof is left as an exercise for you. $\diamond$

FACT 1.6. *A divisor of an integer divides any multiple of that integer: If $b \mid a$, then $b \mid na$ for any integer n.*

The proof is left as an exercise for you. $\diamond$

CONSEQUENCE 1.7. *If $b \mid a$ and $b \mid a'$, then b divides every integer of the form $ma + na'$.*

Proof: This is even too simple to be left as an exercise: we just combine Facts 1.5 and 1.6! If $b \mid a$ then $b \mid ma$, and if $b \mid a'$ then $b \mid na'$ (both by Fact 1.6); then b must also divide their sum $ma + na'$ (by Fact 1.5). $\square$

There's a moral to this story: after going through the trouble to write down and prove a little fact, let's exploit that fact whenever we can (rather than redoing the argument each time). This is really what proof-based mathematics is all about! And later on, after building up a "toolbox" full of little facts like this, we'll be able to prove some really beautiful things about numbers.

FACT 1.8. *A nonzero multiple of an integer is as least as large as the integer itself: If $b \mid a$ and $a \neq 0$, then $|a| \geq |b|$.*

Proof: Since $b \mid a$, there is some integer m such that $a = mb$, and so $|a| = |mb| = |m||b|$. We are assuming that a is not zero, and so neither is m; since m is an integer, we know that $|m| \geq 1$. Therefore $|a| = |m||b| \geq 1|b| = |b|$, as claimed. $\square$

Another way of stating Fact 1.8 is that every divisor of an integer n is no bigger (in absolute value) than $|n|$. From this fact you can easily deduce another obvious statement: if two (positive) numbers divide each other, then they are equal.

3. The Division Algorithm

There is little doubt that you have known how to perform long division for quite some time. On the other hand, your grade 3 teacher probably didn't take the time to *prove* that long division always works. Just so you can sleep at night, let's prove it now.

Theorem 1.9. (The Division Algorithm) *Let n and d be two integers. Then we can divide d into n to get a quotient and a remainder: There exist integers q and r, with $0 \leq r < d$, such that $n = qd + r$.*

Again, this seems like the sort of thing that's so obvious that it doesn't need a proof. Nevertheless, we can prove it from the properties of integers stated earlier.

Proof: Consider the collection of all numbers m such that $md > n$. From Fact 1.3, there exists at least one number m such that $md > n$, so this collection contains at least one number. Therefore, by Fact 1.1, this collection has a smallest number; let's call it s. Now define $q = s-1$ and $r = n - qd$. The thing we have to show is that $0 \leq r < d$.

Because s is in the collection described above, we know that $sd > n$, or $n - sd < 0$. This shows that $r = n - qd = n - (s-1)d = n - sd + d < 0 + d = d$. On the other hand, q is smaller than s, so it can't be in the collection (otherwise s would not be the smallest number in the collection). Therefore it is impossible for $qd > n$; in other words, $qd \leq n$, and so $r = n - qd \geq 0$. $\square$

We admit to having cheated a little: the proof we gave only works when n is positive (because we used Fact 1.1). Nevertheless, the Division Algorithm works for any integers n and d, as long as d is not zero (try finding a number r with $0 \leq r < 0$), and it just takes a little longer to consider the cases where n and/or d is negative. One word of caution: even if n and/or d is negative, when we apply the Division Algorithm we never get a negative remainder r, even though the quotient q might well be negative.

You already know that one number is a multiple of another if, when you divide the second number into the first, you don't get a remainder. This is worth recording in our toolbox of facts:

CONSEQUENCE 1.10. *If n and d are two integers, with d nonzero, then d is a divisor of n if and only if, when you apply the Division Algorithm to n and d to get a quotient q and a remainder r, the remainder equals 0.*

The proof is left as an exercise for you. ◇

Problems for Chapter I

1.1. Write down all of the divisors of 10; of 48; of 210.

1.2. Show that 1 and -1 are divisors of every integer. Show that every integer is a divisor of 0.

1.3. Apply the Division Algorithm to find a quotient and remainder when:
a. 2345 is divided by 123;
b. 123 is divided by 2345;
c. 100 is divided by 10;
d. 89 is divided by 12;
e. -89 is divided by 12;
f. 89 is divided by -12;
g. -89 is divided by -12.

1.4. Provide a proof of Fact 1.5.

1.5. Provide a proof of Fact 1.6.

1.6. Provide a proof of Consequence 1.10.

1.7. Let n and d be numbers. If we divide n by d, we get a quotient q and a remainder r. If we divide the negative number $-n$ by d, we get another quotient s and another remainder t. How are q and s related? How are r and t related?