

# BACKGROUND ASSUMPTIONS FOR NUMBER THEORY

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

In this course, we will start by proving things you already know concerning divisibility of integers and the factorization of integers into prime numbers. You know these facts, but you might not know their proofs.

Why do we prove things we already know, and that we usually take for granted? There are several reasons. One is to place our knowledge on a solid foundation: our knowledge becomes based on deductive reasoning and not just on an appeal to authority or trial and error. Second, the proof of something in mathematics gives us insight into *why* it is true, as opposed to just knowing that it is true. This gives us a deeper understanding of what is going on. Third, proving elementary facts gets us warmed up for proving the more advanced results that are new to us. In a few weeks you will start to see results that are new to you, and you will naturally want an explanation or proof. Your experience with the proofs of the simpler results will make it easier for you to understand the proofs of these new, more advanced results. Finally, often a result we know can be generalized to other situations. For example, divisibility results for integers extend to polynomials and to other situations as well. Our best hope in knowing whether or not something generalizes is to understand the structure of the proofs of the result, and check to see that the proof extends to a new situation.

Of course, we will start at the “beginning” of number theory, and build up to more sophisticated results. But where does number theory start? Some writers might begin with basic axioms for the natural numbers, for example Peano’s Axioms, and derive everything from these axioms including the laws of basic arithmetic. Other writers might begin with the axioms of set theory, and define the integers in terms of sets. These approaches are fine if you do not mind spending a lot of time on elementary matters. (In fact, you might come to learn that what you thought was elementary actually has some subtlety to it). In our course, however, we will not take such a radical approach: we don’t want to get too bogged down in basic arithmetic.

## 1. WHERE TO START?

Given that we are not starting from basic axioms of the natural numbers, what will be our starting point? What will be taken as given? What can we use in our proofs?

I will assume that you have a solid grip on logic, elementary set theory, and elementary arithmetic. In our proofs, the following will be allowed:

1. Any technique of deductive logic standard to mathematics (including properties of equality  $=$ ).
2. Any basic result from set theory.
3. Any basic result from elementary arithmetic as discussed in the next section.

4. Any previously proved result from this course.

## 2. ELEMENTARY ARITHMETIC

What do we consider to be “elementary arithmetic”? This is an important question since number theory is, in some sense, just a continuation of arithmetic. In fact, number theory is sometimes called “higher arithmetic”. So if we want to develop number theory in a careful way, we need to be careful in what arithmetic we consider to be already known and available to us. We will admit the following in our proofs:

1. The natural numbers and the integers:  $\mathbb{N}$  and  $\mathbb{Z}$ .
2. Basic properties of addition, multiplication, and subtraction on the integers. (What we need for division we will develop in the course).
3. Basic properties of the order relation  $<$  on the integers.
4. Basic properties of absolute values for integers.
5. Cancellation laws.
6. Induction principles, the well-ordered principle, and the bounded subset principle.

**2.1. The natural numbers and the integers.** First and foremost we assume the existence of, and standard base ten labeling of, the *positive natural numbers*:

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

In set theory, it is common to include 0 as a natural number since 0 is the cardinality of the empty set. So there is another version of the natural numbers:

$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\}.$$

(Our textbook uses  $\mathbb{N}$  for the positive integers, but some books include 0. Thus  $\mathbb{N}$  is a bit ambiguous in modern mathematics. I like to use  $\mathbb{N}_1$  to emphasize that I am starting with 1, and when I want to start with 0, I write  $\mathbb{N}_0$ . When I just write  $\mathbb{N}$ , just assume that I am being consistent with the textbook, and that I mean  $\mathbb{N}_1$ .)

We assume the use of  $\mathbb{N}$  and  $\mathbb{N}_0$  in counting finite sets, including the idea of *cardinality*. (For example, if one set  $A$  has  $m$  elements and another set  $B$  has  $n$  elements, then the union will have  $m + n$  elements as long as  $A$  and  $B$  are disjoint.)

By throwing in a negative integer  $-n$  for every  $n \in \mathbb{N}$ , we get the full ring of integers:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}.$$

We assume the existence and standard labeling of the integers.

**2.2. Addition, multiplication, and subtraction.** We assume the standard definition of addition and multiplication on the set  $\mathbb{Z}$  and will use the standard notation and grouping conventions. Realize that addition and multiplication give functions  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ . Such functions are often called *binary operations*. We assume the standard properties of these binary operations including the associative, commutative, and distributive law. The *associative law* asserts that, for all  $a, b, c \in \mathbb{Z}$ ,

$$(a + b) + c = a + (b + c) \quad \text{and} \quad (ab)c = a(bc).$$

The *commutative law* asserts that, for all  $a, b \in \mathbb{Z}$ ,

$$a + b = b + a \quad \text{and} \quad ab = ba.$$

Finally, the *distributive law* asserts that, for all  $a, b, c \in \mathbb{Z}$

$$a(b + c) = ab + ac$$

where we use the usual grouping conventions:  $ab + bc$  is short for  $(ab) + (bc)$ .

The associative law allows us to be lazy about parentheses when only addition or only multiplication is involved, since the result of a series of additions or a series of multiplications does not depend on grouping. So expressions such as

$$a + b + c + d \quad \text{or} \quad p_1 p_2 \cdots p_l$$

are well-defined. (*Well-defined* means that you get the same result regardless of the choices you make; in this case, choices about grouping.)

The element 0 is the additive identity and 1 is the multiplicative identity: for all  $a \in \mathbb{Z}$

$$0 + a = a \quad \text{and} \quad 1 \cdot a = a.$$

In addition, for all  $a \in \mathbb{Z}$ ,

$$0 \cdot a = 0.$$

The sets  $\mathbb{N}$  and  $\mathbb{N}_0$  are subsets of  $\mathbb{Z}$  which are closed under addition and multiplication. This means that if you add or multiply two positive (non-negative) integers the result will also be a positive (non-negative) integer. In addition, the product of a positive integer with a negative integer is negative. The product of two negative integers is positive.

Every  $a \in \mathbb{Z}$  has an additive inverse  $-a$ :

$$a + (-a) = 0,$$

(Warning: only 1 and  $-1$  have *multiplicative* inverses in  $\mathbb{Z}$ ). If  $n \in \mathbb{N}$  is positive, then  $-n$  is the corresponding negative integer added to  $\mathbb{N}_0$  in the process of forming  $\mathbb{Z}$ . The additive inverse of  $-n$  is  $n$ : in other words,  $-(-n) = n$ .

The results described above can be summarized by the assertion that  $\mathbb{Z}$  is a *commutative ring with unity*. (We will see the definition of *ring* later in the course.)

Subtraction  $a - b$  is defined to be  $a + (-b)$ : subtracting is really just addition where the second term is replaced by its additive inverse. Warning: subtraction is not commutative, nor is it associative, and  $\mathbb{N}$  (and  $\mathbb{N}_0$ ) are not closed under subtraction. However, the distributive law holds: for all  $a, b, c \in \mathbb{Z}$ ,

$$a(b - c) = ab - ac$$

where  $ab - ac$  is short for  $(a \cdot b) + (-(a \cdot c))$ . We have, for all  $a, b \in \mathbb{Z}$ ,

$$-a = (-1)a, \quad -(ab) = (-a)b = a(-b), \quad \text{and} \quad -(-a) = a.$$

*Exponentiation* is regarded as iterated multiplication: if  $a \in \mathbb{Z}$  and  $n \in \mathbb{N}$  then  $a^n$  is defined to be  $a \cdot a \cdots a$  where  $a$  is understood to occur  $n$  times in the product. By convention  $a^0 = 1$  if  $a \neq 0$ . (We might consider the rational numbers  $\mathbb{Q}$  in some parts of the course, where it makes sense to use negative powers, but ignore negative powers for now). It follows from the definition of exponentiation, and the laws of multiplication above, that for all  $a, b \in \mathbb{Z}$  and  $n, m \in \mathbb{N}_0$

$$a^1 = a \quad (ab)^n = a^n b^n, \quad a^{n+m} = a^n a^m, \quad \text{and} \quad (a^n)^m = a^{nm}.$$

**2.3. Order properties.** We assume the usual order relation  $<$  on  $\mathbb{Z}$ . (We define the relations  $\leq$ ,  $>$ , and  $\geq$  in terms of  $<$  and equality  $=$  in the usual way. For example,  $a > b$  is defined as  $b < a$  and  $a \leq b$  is defined as “ $a < b$  or  $a = b$ ”.)

We assume the standard properties: for example, if  $a, b, c \in \mathbb{Z}$  such that  $c > 0$  and  $a < b$  then  $ac < bc$ . We symbolize this law with the following diagram:

$$\frac{a < b}{c > 0} \\ ac < bc$$

The following symbolizes this and related laws:

$$\frac{a < b}{a + c < b + c} \quad \frac{c > 0}{a < b} \quad \frac{c < 0}{a < b} \\ ac < bc \quad ac > bc$$

$$\frac{a \leq b}{a + c \leq b + c} \quad \frac{c \geq 0}{a \leq b} \quad \frac{c \leq 0}{a \leq b} \\ ac \leq bc \quad ac \geq bc$$

We also have *transitivity laws*:

$$\frac{a < b}{b < c} \quad \frac{a \leq b}{b \leq c} \quad \frac{a > b}{b > c} \quad \frac{a \geq b}{b \geq c} \\ a < c \quad a \leq c \quad a > c \quad a \geq c$$

The *trichotomy law* asserts that given  $a, b \in \mathbb{Z}$ , exactly one of the following occurs:

$$a < b, \quad a = b, \quad \text{or} \quad b < a.$$

Of course,  $\mathbb{N}$  consists of the integers satisfying  $a > 0$  and  $\mathbb{N}_0$  consists of the integers satisfying  $a \geq 0$ . The expression  $n$  *positive* means  $n > 0$ , and  $n$  *negative* means  $n < 0$ .

**2.4. Absolute values.** We assume knowledge of the absolute value  $|a|$  of an integer  $a$ . Realize that this is a function  $\mathbb{Z} \rightarrow \mathbb{N}_0$ . This function is *multiplicative*:  $|ab| = |a| \cdot |b|$  for all  $a, b \in \mathbb{Z}$ . Also, if  $n \in \mathbb{N}_0$ , then  $|n| = n$  and  $|-n| = n$ . In any case, for  $a \in \mathbb{Z}$ , we have  $|a| = |-a|$  and  $|a| \geq 0$ . For addition, all we have is the *triangle inequality*:  $|a + b| \leq |a| + |b|$ .

**2.5. Cancellation laws.** We admit the standard cancellation laws symbolized as follows:

$$\frac{c \neq 0}{ac = bc} \quad \frac{c > 0}{ac \leq bc} \quad \frac{c > 0}{ac < bc} \quad \frac{c < 0}{ac \leq bc} \quad \frac{c < 0}{ac < bc} \\ a = b \quad a \leq b \quad a < b \quad a \geq b \quad a > b$$

**2.6. Induction, well-ordered, and bounded subset principles.** We admit standard induction as symbolized below:

$$\frac{P(1) \quad \forall n \in \mathbb{N}(P(n) \Rightarrow P(n+1))}{\forall n \in \mathbb{N}, P(n)} \quad \text{or} \quad \frac{S \subseteq \mathbb{N} \quad 1 \in S \quad \forall n \in \mathbb{N}(n \in S \Rightarrow n+1 \in S)}{S = \mathbb{N}}$$

Here  $P$  denotes a property of integers, and  $P(n)$  indicates that  $P$  holds for  $n$ . Actually, we do not have to start at 1, we can start at any integer. For example, starting at 0 gives the following.

$$\frac{P(0) \quad \forall n \in \mathbb{N}_0 (P(n) \Rightarrow P(n+1))}{\forall n \in \mathbb{N}_0, P(n)} \quad \text{or} \quad \frac{S \subseteq \mathbb{N}_0 \quad 0 \in S \quad \forall n \in \mathbb{N}_0 (n \in S \Rightarrow n+1 \in S)}{S = \mathbb{N}_0}$$

Sometimes *strong induction* is more useful. Here is a version for  $\mathbb{N}$  (where quantification is over  $\mathbb{N}$ ):

$$\frac{S \subseteq \mathbb{N} \quad \forall n ((\forall m < n, m \in S) \Rightarrow n \in S)}{S = \mathbb{N}}$$

Closely related to strong induction is the fact that  $\mathbb{N}$  and  $\mathbb{N}_0$  are *well-ordered*. This can be symbolized as follows:

$$\frac{S \subseteq \mathbb{N} \quad S \neq \emptyset}{S \text{ has a minimum}}$$

A minimum of  $S$  is an element  $n \in S$  which is smaller than any other element of  $S$ : in other words,  $n \leq m$  for all  $m \in S$ .

The well-orderedness is actually just a special case of the *boundedness properties of  $\mathbb{Z}$*  symbolized as follows:

$$\frac{S \subseteq \mathbb{Z} \quad S \text{ has a lower bound} \quad S \neq \emptyset}{S \text{ has a minimum}} \quad \frac{S \subseteq \mathbb{Z} \quad S \text{ has an upper bound} \quad S \neq \emptyset}{S \text{ has a maximum}}$$

Actually, the boundedness property implies all the other properties (well-ordered, induction, strong induction). We will see examples of this in the exercises below.

### 3. EXERCISES

**Exercise 1.** Show that if  $ab = c$  where  $a, b \in \mathbb{N}$  then  $a \leq c$ . Show that if  $b > 1$  then  $a < c$ .

**Exercise 2.** Show that if  $ab = 1$  and if  $a, b \in \mathbb{N}$  then  $a = b = 1$ .

**Exercise 3.** Show that well-orderedness principle follows from the boundedness principle.

**Exercise 4.** Show that the induction principle follows from the well-orderedness principle. (Hint: let  $P$  be a property satisfying the hypotheses for induction. Let  $S$  be the set of  $n \in \mathbb{N}$  such that  $P(n)$  is false. Suppose  $S$  is not empty, and derive a contradiction.)

**Exercise 5.** Show that the strong induction principle follows from the well-orderedness principle. (Hint: this is very similar to the previous exercise).

**Exercise 6.** Show that the induction principle follows from the strong induction principle.

**Exercise 7.** Show that the boundedness principle follows from the induction principle.