Math 507 class notes

Randall Holmes

August 27, 2020

1 Wednesday August 26th: some of which is mysterious

In the first lecture, I made a perhaps misguided attempt to give a minimal specification of what the natural numbers are, and an explanation of how the natural numbers might be implemented in terms of set theory, and then how the integers might be implemented given the natural numbers. Nothing really hinges on this, except that it does give an illustraton of the very great power of the proof method of mathematical induction.

1.1 A little about sets

I didn't say this in the lecture, but it might be useful.

We assume in this discussion some basics about sets, none of which should be too unfamiliar.

Membership is a basic notion.

Sets A and B are equal if and only if for all x, $x \in A \leftrightarrow x \in B$.

It is common to view all mathematical objects as sets, but we are leaving open the possibility that there are objects which are not sets. We require that anything which has an element is a set; we note below that there is only one set with no elements.

For any set A and property P of elements of A, there is a set

$$\{x \in A : P(x)\}.$$

Its defining axiom is that for all a, $a \in \{x \in A : P(x)\}$ iff $a \in A$ and $P(a)$.

We say $A \subseteq B$ iff A and B are sets and for any x, if $x \in A$ then $x \in B$: we read this "A is a subset of B". For any set A, there is a set $\mathcal{P}(A)$, the power set of A, whose defining axiom is $B \in \mathcal{P}(A) \leftrightarrow B \subseteq A$: this is called the power set of A, the set of all subsets of A.

For any x there is a set $\{x\}$ such that for all y, $y \in \{x\} \leftrightarrow y = x$.

For any sets A, B there is a set $A \cup B$ such that $x \in A \cup B$ iff $x \in A$ or $x \in B$ or both.

The notation $\{x_1, x_2, \ldots, x_n\}$ for a set given by listing its elements can be understood to abbreviate $\{x_1\} \cup \{x_2\} \cup \ldots \cup \{x_n\}$.

The notation $\emptyset$ refers to the empty set which can be computed as

$$\{x \in A : x \neq x\}$$

for any set A: notice that there can be only one empty set.

1.2 Basic axioms for the natural numbers

We give a minimal set of axioms for the natural numbers. We will *not* require that proofs based on this minimal set be written; we may discuss later what the book's official basic assumptions about the integers must be. We give these to demonstrate that a basic description *can* be given in limited space.

The basic assumptions are as follows

(1) 0 is a natural number

(2) If n is a natural number, $\sigma(n)$ is a natural number (this is simply the successor of n, what we usually write $n+1$, and we will not use this notation outside this introduction to basic axiomatics of the natural numbers).

(3) For any natural number n, $\sigma(n) \neq 0$. 0 is the first natural number.(3)

(4) For any natural numbers m, n, $\sigma(m) = \sigma(n) \rightarrow m = n$. Successor is one-to-one.

(5) The principle of mathematical induction: for any property $P(n)$ of natural numbers n, if we have $P(0)$ and $(\forall k \in \mathbb{N} : P(k) \rightarrow P(\sigma(k)))$, it follows that $(\forall n \in \mathbb{N} : P(n))$. The symbol $\mathbb{N}$ is used here for the set of all natural numbers.

The five basic assumptions we have just given, along with some manipulations of sets, due to Peano (and thus called the Peano axioms can be used to derive all properties of the natural numbers.

But the manipulations of sets required to define the usual operations of addition and multiplication using the very limited information we have are very sophisticated: if we add addition and multiplication as primitive notions with some axioms, the need to appeal to set constructions can be avoided in elementary arithmetic.

Our further axioms follow.

(6) If m, n are natural numbers, $m + n$ and $m \cdot n$ are natural numbers.

(7) For any natural number m, $m + 0 = m$.

(8) For any natural numbers m, n, $m + \sigma(n) = \sigma(m + n)$.

(9) For any natural number m, $m \cdot 0$.

(10) For any natural numbers m, n, $m \cdot \sigma(n) = (m \cdot n) + m$.

The reader will notice that instead of the full list of familiar rules of arithmetic, we have given recursive definitions of addition and multiplication based on the notions of zero and successor. It turns out that in combination with mathematical induction, this is enough to define all familiar notions of arithmetic and prove all familiar theorems.

We note that Peano actually had 1 as the first natural number. The reader might want to think about what formal changes would be needed in the axioms: they are straightforward.

The familiar natural numbers are of course defined as $1 = \sigma(0); 2 = \sigma(1)$, etc. You might notice (in the interest of familiar notation) that it is very direct to prove that for any natural number n, $n+1 = n+\sigma(0) = \sigma(n+0) = \sigma(n)$.

1.3 Proving the commutative law of addition

We demonstrate the familiar commutative law "for all natural numbers m, n,

$$m + n = n + m\text{''}.$$

Fix m. We prove "for all natural numbers n, $m + n = n + m$" by mathematical induction.

There are two things to prove: the basis step is $m + 0 = 0 + m$. The induction step is "If for a fixed natural number k, $m + k = k + m$, it follows that $m + \sigma(k) = \sigma(k) + m$.

We prove the basis step $m + 0 = 0 + m$ by induction (how else?) on m. The new basis is $0 + 0 = 0 + 0$, which is obvious. The new induction step is "Assuming that $k+0 = 0+k$, show that $\sigma(k)+0 = 0+\sigma(k)$". We write out the proof of the new induction step: Assume $k + 0 = 0 + k$ (the inductive hypothesis). Now $\sigma(k) + 0 =_{(7)} \sigma(k) =_{(7)} \sigma(k + 0) =_{(\texttt{ind hyp})} \sigma(0 + k) =_{(8)}$

$0 + \sigma(k)$. We annotated each equation with the reason for its validity (an axiom or the inductive hypothesis).

Now we have to prove the main induction step, "If for a fixed natural number k, $m + k = k + m$, it follows that $m + \sigma(k) = \sigma(k) + m$. Assume $m+k = k+m$ (inductive hypothesis). Now $m+\sigma(k) =_{(8)} \sigma(m+k) =_{(\mathtt{ind\,hyp})} \sigma(k + m) =_{(???)} \sigma(k) + m$. Of course, this isn't a proof yet because we have a step labelled `???` which hasn't been justified. If we can prove $\sigma(k + m) = \sigma(k) + m$, which looks like axiom 8 but applied on the left instead of the right, we would complete our proof. So, we prove this lemma.

We prove $\sigma(k + m) = \sigma(k) + m$ by induction on m. The basis step is $\sigma(k + 0) = \sigma(k) + 0$. This is direct: $\sigma(k + 0) =_{(7)} \sigma(k) =_{(7)} \sigma(k) + 0$. The induction step is "Given $\sigma(k + p) = \sigma(k) + p$, we can deduce $\sigma(k + \sigma(p)) = \sigma(k) + \sigma(p)$". Notice that we have to introduce a new variable p for the induction step as the variable k is already used by the induction step this proof is embedded in! Assume $\sigma(k + p) = \sigma(k) + p$ (inductive hypothesis). Now $\sigma(k + \sigma(p)) =_{(8)} \sigma(\sigma(k + p)) =_{(\mathtt{ind\,hyp})} \sigma(\sigma(k) + p) =_{(8)} \sigma(k) + \sigma(p)$, which completes the verification of the missing step labelled with `???` above, and so completes the entire proof. Whew.

We are going to assume the commutative law of addition in our development of number theory, and similarly assume the validity of other basic laws of algebra, without appealing to proofs from the minimalist Peano axioms. There are two reasons to provide this kind of information: one is to remind us that we do have basic assumptions, and we need to be able to back up and work from an explicit formulation of our basic assumptions when we need to. We need to whenever the concern is raised that we might be assuming what we are trying to prove, for example. The second reason why this digression is useful is that it gives an extended example of mathematical induction, which *will* be very important in our work in this class.

1.4 Defining the natural numbers as sets

It is possible to define the natural numbers as sets and give a definition of the set $\mathbb{N}$ (whose existence will have to be assumed as an axiom in addition to our system of set theoretic assumptions above; we do not make heavy weather of this, but set theory is always in the background of advanced work in mathematics).

The usual implementation of natural numbers may look a bit weird. But any implementation will look weird. We implement 0 as $\emptyset$, the empty set.

For each set x, we define $\sigma(x)$ as $x \cup \{x\}$. The effect of this is that $1 = \sigma(0) = 0 \cup \{0\} = \emptyset \cup \{0\} = \{0\}; 2 = \sigma(1) = 1 \cup \{1\} = \{0\} \bigcup \{1\} = \{0, 1\}$, and generally we implement each natural number n as the set $\{0, \ldots, n-1\}$ of all smaller natural numbers. Any such definition is rather artificial (there are alternatives!): this one has the nice feature that n is a set with n elements.

We look at the axioms. Axiom 3 certainly holds: $\sigma(x) = x \cup \{x\}$ is not 0, the empty set, because it has at least x as an element. Axiom 4 requires an additional comment about our set theory: suppose $x \cup \{x\} = y \cup \{y\}$ but $x \neq y$. Then we would have to have $x \in y$ and $y \in x$. We simply rule this out as an axiom of set theory: for any sets x, y, either $x = y$ or $x \notin y$ or $y \notin x$. One way of understanding this is that we assert that sets are constructed in some order, and the elements of a set must be sets constructed before it in that order.

We arrange for axiom 5 to be true by the way we define the set $\mathbb{N}$ of natural numbers. We say that a set I is inductive if $0 \in I$ and

$$(\forall x : x \in I \rightarrow \sigma(x) \in I).$$

We abbreviate this as $\texttt{inductive}(I)$. Note that all natural numbers should belong to an inductive set if our definitions work. Now we assert as an axiom that there is an inductive set I. We then define

$$\mathbb{N} = \{n \in I : (\forall J : \texttt{inductive}(J) \rightarrow n \in J)\}.$$

In other words, we define the set of natural numbers as the set of things which satisfy every property which can be proved by mathematical induction: we make axiom 5 true by force!

I'll spare you the formal development of addition and multiplication, unless you are curious! It can be done, and it doesn't even take up that much space, but it requires some further abstract work.

1.5 Defining the integers as sets

The book takes the integers as the basic data of number theory. It is also quite possible to take the natural numbers, or the positive natural numbers, as the basic data. But we certainly want to be able to talk about the integers. We actually assume basic familiarity with the integers and their properties, but we do briefly indicate here how we would implement them in set theory.

The basic idea is that the integers are obtained by closing up the natural numbers under subtraction.

We define a relation $\sim$ on pairs of natural numbers. $(m, n) = (r, s)$ is defined as holding if $m + s = n + r$. If we allow ourselves to peek at the back of the book, we know that this implies that $m - n = r - s$ (where $m - n$ and $r - s$ are general integers). We turn this on its head: for any natural numbers m, n, we define the integer $m - n$ as $\{(r, s) \in \mathbb{N} \times \mathbb{N} : (m, n) \sim (r, s)\}$, the equivalence class of (m, n) under the relation $\sim$. We further define $(m-n)+(m'-n')$ as $(m+m')-(n+n')$ and $(m-n)\cdot(r-s)$ as $(mr + ns) - (ms + nr)$.

There are things to prove to show that this works. One needs to prove, using properties of the natural numbers alone, that $\sim$ is an equivalence relation. One further needs to prove that the operations of addition and multiplication defined above actually have the properties expected of addition and multiplication of integers. There is a further technical irritation that the natural number 1 (for example) and the integer 1 are not the same object. Problems with this can generally be avoided by always being careful what kind of object we are talking about. Generally, if we are not really looking at implementations of numbers as sets, we can harmlessly identify the natural numbers with the corresponding non-negative integers, and we will always do so.

1.6 The division algorithm theorem

We now take the standpoint we will usually take, that we are aware of basic properties of the natural numbers and the integers, and prove a very basic theorem. We note that this theorem itself might be regarded as one of those basic properties, so we have a little work to do to isolate what the book's basic assumptions really are (which we may or may not completely do).

Theorem: For each integer a and each integer $b > 0$, there are uniquely determined integers q, r (for quotient, remainder such that $a = bq + r$ and $0 \leq < r < b$.

Proof: We first prove (*) "for each integer $a \geq 0$ and each integer $b > 0$, there are integers q, r (for quotient, remainder such that $a = bq+r$ and $0 \leq b < r$: we restrict ourselves to natural numbers a and we do not for the moment try to prove that q, r are unique.

We prove this (of course!) by induction on a. We first fix $b > 0$.

The basis step: if $a = 0$ we let $q = 0$, $r = 0$ and we do have $a = 0 = b \cdot 0 + 0 = bq + r$ and $0 \leq r < b$ because $r = 0$.

The induction step: Fix $k > 0$. We assume as the induction hypothesis that $k = bq_0 + r_0$ and $0 \leq r_0 < b$. Our goal is to show that there are q, r such that $k+1 = bq+r$ and $0 \leq r < b$. You should recognize that when we complete the proof of this induction step we will have proved (*). Note the care I take naming the witnesses to the induction hypothesis and the induction goal, which cannot harmlessly be supposed to be the same.

There are two cases: either $r_0 < b - 1$ or $r_0 = b - 1$.

If $r_0 < b - 1$ then $r_0 + 1 < b$ and we can let $q = q_0$ and $r = r_0 + 1$, and we have $k + 1 = (bq_0 + r_0) + 1 = bq_0 + (r_0 + 1) = bq + r$ and $0 \leq r = r_0 + 1 < b$.

If $r_0 = b - 1$ then let $q = q_0 + 1$ and $r = 0$ and we have $k + 1 = (bq_0 + r_0) + 1 = bq_0 + (b - 1) + 1 = b(q_0 + 1) + 0 = bq + r$, and certainly $0 \leq 0 = r < b$.

Since we get q and r with desired properties in both cases, we can always find such q, r, and the proof of (*) by induction is complete.

Now we need to generalize to all integers a, and we need to verify uniqueness of q and r.

Suppose $a < 0$. It follows that $-a \geq 0$, so we can find q_0, r_0 such that $-a = bq_0 + r_0$ and $0 \leq r_0 < b$.

There are two cases. If $r_0 = 0$, let $q = -q_0$ and let $r = 0 = r_0$. We then have $-a = -(bq_0 + r_0) = -bq_0 = bq = bq + r$ and of course $0 \leq 0 = r < b$.

If $r_0 \neq 0$, then let $q = -(q_0 + 1)$ and let $r = b - r_0$. We then have $-a = -(bq_0+r_0) = -(b(q_0+1)-b+r_0) = b(-(q_0+1))+(b-r_0) = bq+r$ and $0 \leq r = b - r_0 < b$ holds because $r_0 < b$ and $r_0 > 0$.

A concrete example serves to remind us of the need for caution with negative a. $100 = (3)(33)$ $+1$ ($a = 100, b = 3, q = 33, r = 1$). But while it is true that $-100 = (3)(-33) + (-1)$, -1 cannot be r. The correct result is $-100 = (3)(-34) + 2$.

Now we need to prove uniqueness. Suppose that $a = bq + r = bq' + r'$ and $0 \leq r' \leq r < b$ (we can choose $r \leq r'$ without loss of generality. Now observe that $0 = b(q - q') + (r - r')$. Suppose $r \neq r'$. We then have $0 < r - r' < b$. This puts $b(q - q')$ strictly between 0 and b, and so puts $q - q'$ strictly between 0 and 1, which is impossible.

Thus $r = r'$, whence we have $bq + r = bq' + r$, from which we readily get $q = q'$, so we have established that the witnesses q, r found in the proof of the division algorithm theorem are unique.

So, I have a question about this proof in the spirit of the earlier material. Can you get an idea of what basic properties of the integers we are allowing ourselves to use in this proof? I shall try at some point to make a convincing list.