Class Lecture Notes for Math 305, Spring 2022

Dr Holmes

January 12, 2022

These are notes on what I say in class in Math 305.

1 Tuesday, January 11, 2022

Administrative preliminaries.

I discussed the definitions of $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Z}^+$:

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of integers;

$\mathbb{N} = \{0, 1, 2, \ldots\}$, the set of natural numbers (there is no general agreement in mathematical literature as to whether 0 is a natural number, but this book includes it), or non-negative integers;

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, the set of positive integers. In all of these, the use of dots is really cheating: giving a rigorous definition of these sets is rather difficult, and we appeal instead to your pre-formal understanding of these concepts.

I stated a set of axioms for the integers which I will include here (based on the axioms in the Math 287 book with two alternative approaches to order).

We begin with a set of purely algebraic axioms. Our variables range over the set $\mathbb{Z}$ of integers; we assume special integers 0 and 1 and primitive operations or addition ($+$) multiplication ($\cdot$) and additive inverse ($-$, used as a prefix unary operator).

commutative laws: For any $x, y \in \mathbb{Z}$, $x + y = y + x$ and $x \cdot y = y \cdot x$.

associative laws: For any $x, y, z \in \mathbb{Z}$, $(x+y)+z = x+(y+z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. I should add that we are only allowed to write things like $x + y + z$ or $x \cdot y \cdot z$ because we know these operations are associative.

In proofs in section 1.2 you should write parentheses, and explicitly use the associative laws to move them.

You *may* use standard order of operations and read $x \cdot y + z$ as meaning $(x \cdot y) + z$ wihtout writing out the parentheses (multiplication binds more tightly than addition, unary minus binds more tightly than either).

distributive law: For any $x, y, z \in \mathbb{Z}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

identity laws: For any $x \in \mathbb{Z}$, $x + 0 = x$ and $x \cdot 1 = x$. $0 \neq 1$.

multiplicative cancellation: For any $x, y, z \in \mathbb{Z}$, if $x \neq 0$ and $x \cdot y = x \cdot z$, then $y = z$. This amounts to the ability to divide both sides of an equation by the same thing, but we do not have a full division operation in the integers as we do in the rationals or reals.

This is not a full axiomatization of the integers. Of course, systems like the rationals and the reals which extend the integers satisfy these axioms, but there are also systems (even ones familiar to you) which satisfy these axioms and are quite different from the integers. Arithmetic mod p where p is prime satisfies these axioms, and the domain of "numbers" in mod p arithmetic is finite (the remainders $0, 1, \ldots p - 1$ mod p).

Additional axioms appropriate for the integers which rule out the system described being modular arithmetic are axioms of order. We present these (just for fun) in two different ways.

We can axiomatize order by introducing the set of positive integers $\mathbf{Z}^+$ as a primitive notion, providing some of its properties as axioms, and using it to define order relations.

1. $0 \notin \mathbb{Z}^+$.
2. For each $m \in \mathbb{Z}$ with $m \neq 0$ either $m \in \mathbb{Z}^+$ or $-m \in \mathbb{Z}^+$.
3. For each $m, n \in \mathbb{Z}^+$, we have $m + n \in \mathbb{Z}^+$ and $m \cdot n \in \mathbb{Z}^+$
4. Define $m < n$ as $n + (-m) \in \mathbb{Z}^+$.

This is a very elegant set of axioms, and it should be straightforward for you to see that they are true in the familiar system of integers, but it may be less obvious that they are enough. This might be a homework exercise.

Here is a more familiar set of axioms for order. They do follow as consequences of the algebraic and positive integer axioms if we define $<$ as above, but for this approach we "forget" about $\mathbf{Z}^+$ and take $<$ as a primitive relation (and we define $\mathbb{Z}^+$ in terms of $<$).

transitivity: For any $m, n, p \in \mathbb{Z}$, if $m < n$ and $n < p$ then $m < p$.

trichotomy: For any $m, n \in \mathbb{Z}$, exactly one of $m < n, m = n, n < m$ is true.

additive monotonicity: For any $m, n, p \in \mathbb{Z}$, if $m < n$ then $m + p < n + p$.

multiplicative monotonicity: For any $m, n, p \in \mathbb{Z}$, if $p \neq 0$ and $m < n$, then $m \cdot p < n \cdot p$. Our axioms are enough to show that the right things happen if p is zero or negative (that might be a homework exercise).

definition of positive integers: We define $\mathbb{Z}^+$ as $\{x \in \mathbb{Z} : 0 < x\}$.

I stated the Well-Ordering Principle and proved two sample theorems, "each positive integer is either even or odd", and "there is no integer strictly between 0 and 1".

If S is a set of integers, x is a smallest element of S iff $x \in S$ and $(\forall y \in S : x \leq y)$. You could try proving that a nonempty set with a smallest element has just one smallest element.

Well-Ordering Principle: Any nonempty set S of positive integers has a smallest element.

I proved a couple of sample theorems using the Well-Ordering Principle in class. Proofs using this principle are usually indirect (proofs by contradiction); pay attention to the logical structure of what I say.

Definition: An integer m is even iff there is an integer x such that $m = 2 \cdot x$.

An integer m is odd iff there is an integer x such that $m = 2 \cdot x + 1$.

Theorem: Each positive integer is either even or odd.

Proof: Suppose otherwise, so there are integers which are neither even nor odd. Let S be the set of all integers which are neither even nor odd. By our assumption, it is nonempty, so by the Well-Ordering Principle

it has a smallest element w. This number w will be the smallest integer which is neither even nor odd.

The integer w is not 1, because $1 = 2 \cdot 0 + 1$ is odd.

So $w - 1$ is a positive integer, and because it is less than w it must be either even or odd.

If $w - 1 = 2 \cdot x$ is even, then $w = 2 \cdot x + 1$ is odd.

If $w - 1 = 2 \cdot x + 1$ is odd, then $w = 2 \cdot x + 2 = 2 \cdot (x + 1)$ is even.

In either case, we get that w is either odd or even, which is a contradiction, so there can be no such w and the theorem must be true.

Observation: At a crucial point in the argument above, I cheated (or at least I appealed to your intuition), and the fact is used is important and should be proved. How do I know that if $w \neq 1$ is a positive integer that $w-1$ is a positive integer? If we have $w > 1$, we do have $w-1 > 0$. We need to rule out the possibility that $0 < w < 1$ (which, since we know what the integers are, is hard to even take into account).

Theorem: There is no integer x such that $0 < x < 1$.

Proof: If there is such an integer than the set $S = \{x \in \mathbb{Z} : 0 < x < 1\}$ is nonempty and so by the Well-Ordering Principle has a smallest element w.

So we have $0 < w < 1$. By multiplicative monotonicity (because $w > 0$) we have $0 < w^2 < w$ and of course we then have $0 < w^2 < w < 1$. Using transitivity we see that $0 < w^2 < 1$ and $w^2 < w$, so w^2 belongs to the set S but is smaller than w, which is a contradiction.