Notes on Number Theory, Fall 2022

Randall Holmes

October 3, 2022

Im posting these on Monday 10/3; I still need to add more to cover the lecture the previous Wednesday. The notes on that lecture should be complete sometime today, to be expanded to cover what I lecture today (10/3). The homework assigned for 10/3 will also appear as an update to this file.

The mathematical system we are interested in is officially the set of integers, whose official name is $\mathbb{Z}$ (this stands for **Zahlen**, numbers, in German).

I'm going to state a definition of the set of integers as a subset of the real numbers $\mathbb{R}$, just because I would like you to know in the back of your mind that things like this can be done. This definition is not examinable, but it might in some ways be useful to understand it.

Definition (integer-closed set of reals): A set A of real numbers is said to be "integer-closed" if and only if $0 \in A$ and for every real number x, if $x \in A$ then $x + 1$ and $x - 1$ are both in A.

There are lots of integer-closed subsets of $\mathbb{R}$: $\mathbb{R}$ itself is integer-closed; the set of rationals is integer-closed; the set of all fractions with denominator 2 is integer closed (it contains all integers n and also contains $n + \frac{1}{2}$ for each integer n).

Definition of $\mathbb{Z}$: $\mathbb{Z}$ is defined as $\{x \in \mathbb{R} :$ for every set A, if A is integer closed then $x \in A\}$. It really works...think about it.

There is something odd about this definition, because it presupposes that we know what the reals are. But if you get to an advanced course where a formal definition of the natural numbers, integers, and reals is actually given, you might get an idea of what I'm up to. Really, I just want to be able to say something more accurate than $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2 \ldots\}$.

The mathematical system of the integers does not have the set of integers as its only component. It also has operations and relations for which we will state axioms. These operations and relations are familiar. The constants 0 and 1, the operations of addition, multiplication, and additive inverse, and the relation "less than" are the basics in our presentation.

First set of axioms (basic algebra): commutative laws: For any integers a, b, $a + b = b + a$ and $a \cdot b = b \cdot a$.

associative laws: For any integers a, b, c, $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

distributive law: For any integers a, b, c, $a(b + c) = a \cdot b + a \cdot c$.

distributive laws? (comment): We could give another distributive law $(a+b)c = ac+bc$ too, but we do not need to, since $(a+b)c = c(a+b) = ca+cb = ac+bc$ justifies the alternative distributive law in terms of the one we give and commutativity of multiplication.

It is useful to notice that matrix algebra is a familiar system (to some of you, at least) in which both forms of the distributive law have to be given, because matrix multiplication is not commutative.

identity laws: For any integer a $a + 0 = a$ and $a \cdot 1 = a$; $0 \neq 1$

additive inverse law: For any integer a, $a + (-a) = 0$.

multiplicative cancellation: For any integers a, b, c, If $c \neq 0$ and $ac = bc$, then $a = b$.

Normally, we would prove multiplicative cancellation (in the reals or rationals) using the existence of a multiplicative inverse (reciprocal) a^{-1} of each nonzero real number a such that $a \cdot a^{-1} = 1$. But this property doesn't hold in the integers. Notice that we can prove additive cancellation using the additive inverse property (if $a + c = b + c$ then $a = b$: try to demonstrate this).

Observation: All of these axioms hold in the systems of reals or rationals familiar to you. We will also study systems of modular arithmetic which look very different from the reals or rationals (they are finite systems!) in which all of the axioms of the first set hold.

A second set of axioms rules out the modular arithmetic systems.

Second set of axioms (properties of order): $<$ is transitive: For all integers a, b, c, if $a < b$ and $b < c$, then $a < c$.

trichotomy: For any integers a, b, exactly one of the following is true: $a < b, a = b, b < a$.

additive monotonicity: For any integers a, b, c, if $a < b$ then $a + c < b + c$ (it is actually if and only if, because you can add the additive inverse to go the other way).

multiplicative monotonicity: For any integers a, b, c, if $c > 0$ and $a < b$, then $ac < bc$.

The other version, if $c < 0$ and $a < b$, then $bc < ac$, is provable from the axioms we already have.

Definitions: $a > b$ means $b < a$. $a \leq b$ means $a < b$ or $a = b$. $a \geq b$ means $b \leq a$. These relations all have similar properties to $<$, which you are already informally familiar with.

Observation: These axioms all hold in the familiar systems of reals and rationals. The axiom which separates the integers from the reals or rationals is something we have already discussed.

Axiom of Mathematical Induction: Let $P(n)$ be a statement about an integer variable n and let b be an integer. If $P(0)$ is true and for every integer $k \geq b$ such that $P(k)$ is true, it follows that $P(k + 1)$ is true, we can conclude that $P(n)$ is true for every integer $n \geq b$.

The axiom of mathematical induction drives a wedge between the integers and the reals or rationals. For example, we can prove that there is no multiplicative inverse of 2.

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

Proof: We prove by mathematical induction that for every integer $x \geq 0$, either $x = 0$ or $x \geq 1$.

Basis: $0 = 0$ or $0 \geq 1$ is true because $0 = 0$.

Induction: Suppose $k = 0$ or $k \geq 1$. In either case we have $k \geq 0$. $k + 1 \geq 1$ follows by additive monotonicity, so we have either $k + 1 = 0$ or $k + 1 \geq 1$ because we have the latter.

Theorem: There is no integer x such that $2x = 1$.

Proof: Suppose there is such an x. We have to establish $x > 0$: clearly x is not 0 ($2 \cdot 0 = 0 \neq 1$). If $x < 0$ we would have $2x < 0$ by multiplicative monotonocity, so $1 < 0$, which is absurd. So $x > 0$. It follows by additive monotonicity that $x + x > x$, so $1 > x$. But then $0 < x < 1$, which we have just shown is not possible.

Sanity check ($1 > 0$): We have in our axioms that $1 \neq 0$. Thus we can only have $1 > 0$ (which we believe) or $1 < 0$. Suppose that $1 < 0$. Add -1 to both sides to get $0 < -1$, so $-1 > 0$. Then we can use $-1 > 0$ and multiplicative monotonicity: it follows that $(-1)(-1) > 0$, $1 > 0$, contradicting the assumption that $1 < 0$ (by an appeal to trichotomy). So we have ruled out $1 < 0$ and $1 > 0$ is the only possibility.

Again, Im appealing to common sense in the equation $(-1)(-1) = 1$. We may look into how to prove that.

This is an example of a general point. You have seen something like these axioms before, and you have been told that all of your ninth-grade algebra knowledge (say) follows from these principles. But you weren't really shown this, and proofs of "easy and obvious" things from basic sets of axioms in any area of math may turn out to be tricky.

Challenge Problem: Prove from the axioms that for any integer a, $a \cdot 0 = 0$. It is rather tricky! (Notice that we used this fact freely in our discussion above.)