We describe the set of axioms for the integers which we will use in the class. The axioms are almost the same as what is presented in Appendix A of the textbook, with a couple of differences explained in Remark 1 below.

Near the end, there are also a couple of examples of proof by contradiction. Although we have been careful when using commutativity and associativity in this note, you do not need to invoke them explicitly in your own proofs.

The axioms. The integers, which we denote by \( \mathbb{Z} \), is a set, together with a nonempty subset \( P \subset \mathbb{Z} \) (which we call the positive integers), and two binary operations addition and multiplication, denoted by \(+\) and \(\cdot\), satisfying the following properties:

- **(Commutativity)** For all integers \( a, b \), we have \( a + b = b + a \) and \( a \cdot b = b \cdot a \).
- **(Associativity)** For all integers \( a, b, c \), we have \( a + (b + c) = (a + b) + c \) and \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \).
- **(Distributivity)** For all integers \( a, b, c \), we have \( (a + b) \cdot c = a \cdot c + b \cdot c \).
- **(Identity)** There exist integers 0 and 1, such that for all integers \( a \), we have \( a + 0 = a \) and \( a \cdot 1 = a \).
- **(Additive inverses)** For any integer \( a \), there exists an integer \(-a\) such that \( a + (-a) = 0 \).
- **(Closure for \( P \))** If \( a, b \) are positive integers, then \( a + b \) and \( a \cdot b \) are positive integers.
- **(Trichotomy)** For every integer \( a \), exactly one of the following three possibilities hold: either \( a \) is a positive integer, or \( a = 0 \), or \(-a\) is a positive integer.
- **(Well-ordering)** Every nonempty subset of the positive integers has a smallest element.

For the well-ordering property, we have not yet defined “smallest,” so we can rephrase it more formally as follows: if \( S \) is a nonempty set of positive integers, then \( S \) contains an element \( a \) such that for every \( b \) in \( S \) which is not equal to \( a \), we have \( b - a \) is a positive integer.

Remark 1. There are a couple of differences from the axioms as presented in Appendix A of the textbook. First, the book lists “closure” as an axiom, but we don’t need to state it separately, because when we say that \(+\) and \(\cdot\) are “binary operations” on the integers, this means precisely that they give rules which associate to any pair of integers \( a \) and \( b \) a new integer \( a + b \) (or \( a \cdot b \)).

More significantly, the book lists the “cancellation law” as an axiom, but we will see in Lemma 10 that it actually follows from the other axioms.

We use the conventional order of operations, with multiplications occurring prior to additions. Thus, in the distributive law, \( a \cdot c + b \cdot c \) means \((a \cdot c) + (b \cdot c)\). As usual, we will write \( a - b \) as an abbreviation for \( a + (-b) \).
Uniqueness observations. Notice first that 0 and 1 have been defined implicitly in the axioms, as the additive and multiplicative identities. However, in order to know that there is no ambiguity in defining them this way, we need to know:

**Lemma 2.** 0 and 1 are uniquely defined by the property of being the additive and multiplicative identity, respectively.

*Proof.* Suppose that $0, 0'$ are integers, and both are additive identities, so that for all integers $a$, we have $a + 0 = a = a + 0'$. Then we want to show that we must have $0 = 0'$. But using also commutivity, we have

$$0 = 0 + 0' = 0' + 0 = 0',$$

as desired. The same argument works for 1 with multiplication in place of addition. \(\square\)

Similarly, we want to know that inverses are unique (otherwise, in the statement of trichotomy, we might have to worry about which “$-a$” we are considering.

**Lemma 3.** If $a$ is any integer, then $-a$ is uniquely defined by the property that $a + (-a) = 0$.

*Proof.* Suppose that $b, b'$ are integers and $a + b = 0 = a + b'$. We want to see that $b = b'$. But using commutivity and associativity,

$$b = b + 0 = b + (a + b') = (b + a) + b' = b' + (a + b) = b' + 0 = b',$$

as desired. \(\square\)

It then makes sense to say the following:

**Proposition 4.** $-0 = 0$.

*Proof.* $0 + 0 = 0$ by definition of 0, so by definition of additive inverse we see that 0 is the additive inverse of itself, which is to say that $-0 = 0$. \(\square\)

**Ordering and consequences.** We will define ordering on the integers using the set of positive integers:

**Definition 5.** If $a, b$ are integers, we say $a$ is **greater than** $b$, and write $a > b$, if $a - b$ is positive. We say $a$ is **smaller than** $b$, and write $a < b$, if $b - a$ is positive. As usual, we write $a \geq b$ to mean that either $a > b$ or $a = b$, and similarly with $a \leq b$.

Notice in particular that $a > 0$ if and only if $a$ is positive. This is not our definition, but we see that it is the same using Proposition 4!

We take for granted what are sometimes called “properties of equality”: for instance, if $a = b$, then for any $c$ we have $a \cdot c = b \cdot c$. This is because $a = b$ means that $a$ and $b$ are the same integers, and by definition multiplication is a well-defined operation on integers, so if we write a given integer two different ways, that doesn’t affect what happens when we multiply it. However, inequalities are a different matter: because we have defined them in terms of the set of positive integers (about which in principle we know nothing beyond what is stated in the axioms), we ought to check that the familiar properties of inequalities still hold in the integers. For instance, we have:

**Proposition 6.** Suppose that $a, b, c$ are integers with $a > b$ and $c > 0$. Then $a \cdot c > b \cdot c$.

This turns out to require some intermediate steps!

**Lemma 7.** If $a$ is any integer, then $a \cdot 0 = 0$. 2
Proof. Using distributivity, we have
\[ a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0. \]

If we add \(-(a \cdot 0)\) to both sides, we get
\[ 0 = (a \cdot 0) + -(a \cdot 0) = (a \cdot 0 + a \cdot 0) + -(a \cdot 0) = a \cdot 0 + (a \cdot 0 + -(a \cdot 0)) = a \cdot 0 + 0 = a \cdot 0, \]
as desired. □

**Lemma 8.** If \(a\) is any integer, then \(-(-a) = a\).

**Proof.** By definition of additive inverse, we want \((-a) + a = 0\), but \(a + (-a) = 0\) by definition, so this follows from commutativity. □

**Lemma 9.** If \(a, b, c\) are any integers, then:

(i) \(-a = a \cdot (-1)\);
(ii) \((-a) \cdot b = -(a \cdot b) = a \cdot (-b)\);
(iii) \((-a) \cdot (-b) = ab\);
(iv) \((a - b) \cdot c = a \cdot c - b \cdot c\);

**Proof.** For (i), we want \(a + a \cdot (-1) = 0\). But using distributivity and Lemma 7,
\[ a + a \cdot (-1) = a \cdot 1 + a \cdot (-1) = a \cdot (1 + (-1)) = a \cdot 0 = 0. \]

For (ii), we apply (i) repeatedly to find
\[ a \cdot (-b) = a \cdot (b \cdot (-1)) = (a \cdot b) \cdot (-1) = -(a \cdot b). \]

Using this (with \(a\) and \(b\) reversed) we also see that
\[ (-a) \cdot b = b \cdot (-a) = -(b \cdot a) = -(a \cdot b), \]
proving (ii). For (iii), we use (ii) and Lemma 8 to see that
\[ (-a) \cdot (-b) = -(a \cdot (-b)) = -(a \cdot b) = a \cdot b. \]

Finally, for (iv) we can use (ii) and distributivity to get
\[ (a - b) \cdot c = (a + (-b)) \cdot c = a \cdot c + (-b) \cdot c = a \cdot c + (-b \cdot c) = a \cdot c - b \cdot c, \]
as desired. □

**Proof of Proposition 6.** By definition, \(a \cdot c > b \cdot c\) is the same as saying \(a \cdot c - b \cdot c\) is positive. But using Lemma 9 law we have
\[ a \cdot c - b \cdot c = (a - b) \cdot c, \]
and \(a > b\) and \(c > 0\) mean that \(a - b\) and \(c\) are positive, so by the closure axiom \((a - b) \cdot c\) is also positive, and we conclude that \(a \cdot c > b \cdot c\), as desired. □

However, it’s impractical to prove every property of inequality, and most of them are more straightforward: for instance, that \(a > b\) and \(b > c\) implies \(a > c\) follows easily from the closure of \(\mathbb{P}\), and \(a > b\) implies \(-b > -a\) is also easy from what we’ve done. So while it’s a good habit to think carefully about which properties of inequalities are being used and why they’re true, we’ll generally take them for granted.

3
Cancellation. As asserted above, the cancellation law can actually be deduced from our axioms. We are now ready to prove this. Having built up some familiarity with basic proofs, our arguments will use a couple of steps at a time now.

Lemma 10 (Cancellation law). Suppose that $a, b, c$ are integers, and $c \neq 0$. Then if $a \cdot c = b \cdot c$, it follows that $a = b$.

Proof. Given that $a \cdot c = b \cdot c$, we have from Lemma 9 (iv) that

$$0 = a \cdot c - b \cdot c = (a - b) \cdot c.$$ 

This shows that $a - b$ must be zero. By trichotomy, there are three cases to consider: either $a - b = 0$, or $a - b$ is positive, or $-(a - b)$ is positive. Similarly, since $c \neq 0$, either $c$ is positive or $-c$ is positive. First suppose $a - b$ is positive, and $c$ is positive. Then by closure $(a - b) \cdot c$ is positive, contradicting that it is equal to 0. If $a - b$ is positive and $-c$ is positive, then by Lemma 9 (ii) we have that $(a - b) \cdot (-c) = -(a - b) \cdot c$ is positive, so again $(a - b) \cdot c$ is not zero. The two cases that $-(a - b)$ is positive are handled similarly, and we conclude that the only possibility is that $a - b = 0$, as desired. □

The smallest positive integer. We defined 1 to be the multiplicative identity, but it is also the smallest positive integer, as we now explain.

Proposition 11. 1 is the smallest positive integer.

Proof. By the well-ordering principle, we know that there is some smallest positive integer; let’s call it $a$. First suppose that $a < 1$. By Proposition 6, we have $a^2 < 1 \cdot a = a$. But if $a$ is positive, $a^2$ is also positive by closure, and this contradicts that $a$ is the smallest positive integer. In order to rule out $a > 1$, we just need to know that 1 is positive. But if $-1$ were positive, then for any positive $a$ we’d have $-a = a \cdot (-1)$ also positive, contradicting trichotomy. Also, if we have $1 = 0$, then for any positive $a$ we’d have $a = a \cdot 1 = a \cdot 0 = 0$, again contradicting trichotomy. We thus conclude by trichotomy that 1 is positive, and hence is the smallest positive integer. □

Although such specific definitions won’t really come up for us during the class, we could now define 2 to be the smallest positive integer which isn’t 1, and 3 to be the smallest positive integer which isn’t 1 or 2, etc.

More symbols. In this note, we’ve tried to minimize use of symbols to make it friendlier. However, usually in math we use more symbols, including $\in$ for ‘in’, $\forall$ for ‘for all’, and $\exists$ for ‘there exists’. We would thus write the closure axiom for positive integers as: “for all $a, b \in \mathbb{P}$, we have $a + b \in \mathbb{P}$ and $a \cdot b \in \mathbb{P}$,” or even more briefly, as “$\forall a, b \in \mathbb{P}$, we have $a + b \in \mathbb{P}$ and $a \cdot b \in \mathbb{P}$.”