Number theory notes

1 Axioms of $\mathbb{Z}$

These are the axioms for the integers, given in class. These axioms are grouped according to their type. Broadly, there are three categories: the axioms of arithmetic, the axioms of an ordering, and the well ordering principle. You should treat using these axioms as a game. Whenever you want to prove something, try to combining them in different ways to prove what you want to achieve.

All axioms are referring to $\mathbb{Z}$; all quantifiers refer to elements of $\mathbb{Z}$ if not otherwise specified.

1.1 Axioms of addition

The first set of these axioms define addition, which makes $\mathbb{Z}$ into what is known as a commutative group. They say there is an operation $+$ and an element $0 \in \mathbb{Z}$ so that the following hold:

1. (0 is an additive identity) $(\forall a)0 + a = a$.

2. (addition is commutative) $(\forall a, b)a + b = b + a$.

3. (inverses exist) $(\forall a)(\exists b)a + b = 0$.

We have been ambiguous about what it means to even be an operation. Properly it is defined as a function of pairs of elements of $\mathbb{Z}$ to $\mathbb{Z}$ with the additional property that for all $a, b, z \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$, the property of associativity.

It is not actually necessary to assume that the inverse is unique, as assumed in class, as it is automatic from the definition:

Lemma 1 (Inverses are unique). For all $a \in \mathbb{Z}$, the inverse is unique. We denote the inverse of $a$ by $-a$.

Proof. We need to prove if there are two inverses for $a$ then they are equal. Suppose there are two inverses, $b$ and $c$. Then

$$b = b + 0 = b + (a + c) = (b + a) + c = (a + b) + c = 0 + c = c.$$
Remark 1. Subtraction is defined in terms of this additive inverse by defining $a - b$ to be $a + (-b)$.

As a warm up, we show that there is a rule of additive cancellation.

**Lemma 2 (Additive cancellation).** For all $a, b, c \in \mathbb{Z}$ if $a + c = b + c$ then $a = b$.

**Proof.** By assumption $a + c = b + c$. Then it follows that $a + c + (-c) = b + c + (-c)$. Therefore, $a + 0 = b + 0$ and so $a = b$. \qed

### 1.2 Axioms of multiplication

We now additionally define multiplication (har-har!). Multiplication stipulates there is an additional operation $\cdot$ and an element $1 \in \mathbb{Z}$ so that the following hold:

1. (1 is an multiplicative identity) $(\forall a) 1 \cdot a = a$.

2. (multiplication is commutative) $(\forall a, b) a \cdot b = b \cdot a$.

3. (no zero divisors) $(\forall a, b) (a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0))$

We additionally include the distributivity rule, which connects addition and multiplication.

1. (distributivity) $(\forall a, b, c) (a + b) \cdot c = a \cdot c + b \cdot c$

Taken together, all these rules together make $\mathbb{Z}$ into what is known as an integral domain. Removing the zero divisors assumption would leave what is called a commutative ring. Further removing the commutativity of multiplication makes a ring. These objects all have amazing properties that can be studied in general, which would be in an Algebra course here at the university.

We’ll prove another simple property about $\mathbb{Z}$ that follows from these axioms.

**Lemma 3 (Multiplicative cancellation).** For all $a, b, c \in \mathbb{Z}$ if $a \cdot c = b \cdot c$ and if $c \neq 0$ then $a = b$.

**Proof.** By assumption $a \cdot c = b \cdot c$. Observe that

$$b \cdot c + (-b) \cdot c = (b - b) \cdot c = 0 \cdot c = 0,$$

so that $(-b) \cdot c$ is the inverse of $b \cdot c$. Then adding this to both sides of $a \cdot c = b \cdot c$, we have $a \cdot c + (-b) \cdot c = 0$.

Using distributivity, this implies $(a - b) \cdot c = 0$. As $c \neq 0$, it must be that $a - b = 0$, by the no zero divisor assumption. Adding $b$ to both sides, we conclude $a = b$. \qed

In the lemma, we needed to show that $-(b \cdot c) = (-b) \cdot c$. There are many identities like this which are good warm-up exercises, and which are a constant nuisance if they are not established early. We leave them here as an exercise.

*Math 3345 Number theory notes* 2 Fall 2016
Exercise 1: Prove the following arithmetic facts about \( \mathbb{Z} \).

(a) The additive identity is unique: \((\exists a \in \mathbb{Z}, a + b = a) \implies b = 0\).

(b) The multiplicative identity is unique: \((\exists a \in \mathbb{Z}, a \cdot b = a, a \neq 0) \implies b = 1\).

(c) \(\forall a \in \mathbb{Z}, -a = (-1) \cdot a\).

(d) \((-1) \cdot (-1) = 1\).

(e) \(\forall a, b \in \mathbb{Z}, -(a + b) = -a - b\).

1.3 Axioms of ordering

The axioms that follow define the natural ordering that appears on \( \mathbb{Z} \). Specifically, they define a comparison operator \(<\) which for two elements of \( \mathbb{Z} \) always evaluate as true or false.

1. (transitivity) \((\forall a, b, c)\) if \(a < b\) and \(b < c\) then \(a < c\).

2. (total ordering) \((\forall a, b)\) exactly one of \(a < b\), \(a = b\) or \(b < a\) holds.

3. (additive invariance) \((\forall a, b, c)\) if \(a < b\) then \(a + c < b + c\).

4. (scale invariance) \((\forall a, b, c)\) if \(a < b\) and \(c > 0\) then \(a \cdot c < b \cdot c\).

5. (non-degeneracy) \(0 < 1\).

The first axiom is essentially all that is needed for an ordering. The second axiom strengthens this statement by saying that all pairs of elements can be compared; in some cases it is convenient to define orderings where not all elements can be compared. These axioms alone have no connection to the structures already defined, in particular to the two operations \(+\) and \(\cdot\). Including these operations almost entirely specifies the usual ordering on \( \mathbb{Z} \), except we must also give it an orientation \((0 < 1)\).

Remark 2. A subtle point, and the reason the last axiom is titled non-degeneracy, is that up to this point, we have not required that \(1 \neq 0\). In fact, with the weaker assumption that \(0 \leq 1\) (i.e. \((0 < 1) \lor (0 = 1))\), all the axioms so far listed would be satisfied by the trivial 1-element ring \(\{0\}\).

As another warm up lemma, we show:

Lemma 4. For all \(a, b \in \mathbb{Z}\) if \(a < b\) then \(-b < -a\).

Proof. Using the additive invariance of \(<\), followed by the axioms of arithmetic

\[
\begin{align*}
a < b & \\
\Rightarrow a - (a + b) < b - (a + b) & \\
\Rightarrow a - a - b < b - a - b & \\
\Rightarrow a - a - b < -a + b - b & \\
\Rightarrow 0 - b < -a + 0 & \\
\Rightarrow -b < -a. &
\end{align*}
\]
Here are some similar exercises to try.

Exercise 2: Prove: for every $n \in \mathbb{Z}$, $n \cdot n \geq 0$.

Exercise 3: Prove: for all $a, b, c \in \mathbb{Z}$ if $a < b$ and $c < 0$ then $a \cdot c > b \cdot c$.

Exercise 4: Prove: for all $a, b \in \mathbb{Z}$ if $a \cdot b = 1$ then either $a = b = 1$ or $a = b = -1$.

### 1.4 The well ordering principle

The final axiom, and the one that is perhaps the most complicated, is the well ordering principle. So far, both $\mathbb{Q}$ and $\mathbb{R}$ satisfy the axioms we’ve posited for $\mathbb{Z}$. This final axiom, is in a sense, the one that makes $\mathbb{Z}$ the integers. Usually, it is stated as a property of the natural numbers $\mathbb{N}$, which we now properly define as

**Definition 1.** Let $\mathbb{N}$ be the set of all positive $\mathbb{Z}$. In symbols,

$$\mathbb{N} = \{a \in \mathbb{Z} : a > 0\}.$$

**Definition 2 (Well ordering principle).** Every nonempty subset of $\mathbb{N}$ has a smallest element. Formally, for $S \subseteq \mathbb{N}$, if there exists $x \in S$ then there exists $x \in S$ so that $\forall a \in S, x \leq a$.

While it is stated for the natural numbers, there are two consequences (in fact equivalent formulations) of it for $\mathbb{Z}$.

**Exercise 5:** Prove the following consequences of the well ordering principle that hold for all nonempty sets $S \subset \mathbb{Z}$

(a) If there exists an $a \in \mathbb{Z}$ so that for all $s \in S, a \leq s$, then there exists an $a \in S$ so that for all $s \in S, a \leq s$.

(b) If there exists an $a \in \mathbb{Z}$ so that for all $s \in S, a \geq s$, then there exists an $a \in S$ so that for all $s \in S, a \geq s$.

This axiom is a little bit strange at first sight. We will see lots and lots of consequences of it, one of which is the principle of mathematical induction. For now, here is a typical application of it.

**Lemma 5.** There does not exist an $x \in \mathbb{Z}$ so that $0 < x < 1$ (that is $(0 < x) \land (x < 1)$).

**Proof.** Define a set $S \subset \mathbb{Z}$ as all those $x \in \mathbb{Z}$ with $0 < x < 1$. In symbols,

$$S = \{x \in \mathbb{Z} : 0 < x < 1\}.$$

We want to show that this set is empty. Suppose the statement of the theorem were not true, so that $S$ is nonempty. Then since all $x \in S$ have $0 < x$, $S \subset \mathbb{N}$. Therefore, by the well ordering principle, there is a smallest element of $S$. Call this element $a$.

To get a contradiction, we will construct an element of $S$ that is smaller than $a$. The trick here is to look at $a^2 = a \cdot a$. On the one hand, we know that $a > 0$. Therefore, $a \cdot a > 0 \cdot a = 0$. 

---

*Math 3345 Number theory notes*  
*Fall 2016*
On the other hand, since $a < 1$ and $a > 0$ we know that $a \cdot a < 1 \cdot a = a < 1$. In summary, $a \cdot a \in S$ as it is an integer between 0 and 1, and also, $a \cdot a < a$, which contradicts that $a$ is the smallest element of $S$. 

Exercise 6: Prove that for all $a, b \in \mathbb{N}$ there exists an $n \in \mathbb{N}$ so that $a \cdot n \geq b$.

2 Divisibility

Most of number theory is devoted to understanding the lack of the multiplicative inverse, and the structure that results: when would division be possible? We start with the definition of the concept:

Definition 3. For $a, b \in \mathbb{Z}$ let $a \mid b$, read as “$a$ divides $b$,” if there exists an integer $k$ so that $ak = b$. In this case, we say that $a$ is a divisor of $b$.

The basic properties of division are similar to axioms of the ordering $<$, with the exception of the total ordering property.

Exercise 7: (a) $\forall d, n, m$ if $d \mid n$ and $n \mid m$ then $d \mid m$.

(b) $\forall d, n, m, a, b$ if $d \mid n$ and $d \mid m$ then $d \mid (an + bm)$.

(c) $\forall a, d, n$ if $d \mid n$ then $ad \mid an$.

(d) $\forall a, d, n$ if $a \neq 0$ and $ad \mid an$ then $d \mid n$.

(e) $\forall d, n > 0$ if $d \mid n$ then $d \leq n$.

While it is not always possible to divide numbers, it is always possible to do division with remainder. This is the essence of what is commonly called the division algorithm.

Theorem 1 (Division algorithm). For all $a, b \in \mathbb{Z}$ with $b > 0$ there are unique $q, r \in \mathbb{Z}$ so that $a = bq + r$ and $0 \leq r < b$.

Here $q$ and $r$ are so named to reflect that one is the quotient and the other the remainder. This is another consequence of the well ordering principle.

Proof. The idea here is to use that $bq$ is the largest multiple of $b$ that is still smaller than $a$. So, define a set

$$S = \{ x \in \mathbb{Z} : bx \leq a \}.$$

We would like to apply the well ordering principle here, specifically the form of the WOP in Exercise 5b. To do this, we must check that $S$ is bounded above and that $S$ is nonempty.

To see that $S$ is bounded above, observe that it suffices to show that there is a $y > 0$ so that $\forall s \in S$ for which $s > 0$ have $s \leq y$. This is because all other $s \in S$ are negative and therefore are also less than $y$. Suppose that $s \in S$ is any element with $s > 0$. Then by definition $sb \leq a$. Since $s > 0$ and $b \geq 1$ (Lemma 5), $sb > s1 = s$. Hence $s \leq a$. This concludes the proof that $S$ is bounded above.
We need to see that $S$ is nonempty as well. Suppose not, i.e. suppose $S$ is empty. Then we have that

$$T = \{ bx : x \in \mathbb{Z} \}$$

is bounded below by $a$. But then there must be a smallest element $u \in T$, which by definition has the form $bv$ for some $v \in \mathbb{Z}$. However, $b(v - 1)$ is smaller than $bv$, since $b > 0$, and so we have reached a contradiction. Thus, we have shown $S$ is nonempty.

Applying the WOP, there exists a $q \in S$ that is maximal. Let $r = a - bq$. We claim that $0 \leq r < b$. On the one hand, since $q \in S$, we know $bq \leq a$. Rewriting, this, we conclude $r = a - bq \geq 0$. On the other hand, since $q \in S$ is maximal, we know that $q + 1$ is not in $S$. Therefore $(q + 1)b > a$. Rewriting this, $r = a - bq < b$, which completes the claim.

We have not finished the proof! We claimed that $q$ and $r$ are unique. So, we need to show that any other factorization must be the same. Suppose that $q', r' \in \mathbb{Z}$ have $0 \leq r' < b$ and $a = q'b + r'$. Then we have two, possibly different, factorizations

$$qb + r = a = q'b + r'.$$

Now, we don’t know anything about what $q$ and $q'$ must do, but $r$ and $r'$ have restrictions on their behavior, so we’ll try to exploit this. Let’s rearrange this equation as

$$b(q - q') = r' - r. \quad (0-1)$$

Now in this form, we can estimate the right hand side by

$$-b < -r \leq r' - r \leq r' < b.$$

Therefore

$$-b < b(q - q') < b.$$ 

Since $b > 0$ we can cancel $b$ from all sides of this equation (actually it would work here if $b < 0$ as well, since we have upper and lower bounds) to get

$$-1 < q - q' < 1.$$ 

The only integer in this range is 0, though, and so $q = q'$. From this and equation $(0-1)$, we conclude

$$r' - r = b(q - q') = 0,$$

which completes the proof. \qed

### 3 The greatest common divisor

With the division algorithm in hand, we turn to the concept of the greatest common divisor ($gcd$) of two integers. This is a very useful concept, which will allow us to show, together with the division algorithm, the irrationality of $\sqrt{2}$ among other things. The important and
strange Bézout’s lemma, which characterizes the gcd, will be an important building block of what follows.

For two integers $a, b \in \mathbb{Z}$ define the set of common divisors by

$$C(a, b) = \{k \in \mathbb{Z} : k|a, k|b\}.$$ 

In the manner in which we have defined it, this set will contain positive and negative numbers. For example, one can check that the common divisors of 14 and 21 are

$$C(14, 21) = \{±1, ±7\}.$$ 

The notation here should be read as $±1 = 1, -1$. A formal proof of a fact like this might be tedious, or even impossible (do we have to check every integer?), without some basic facts.

The first fact to observe is that $C(a, b)$ is always nonempty: it contains 1 and $-1$, which divide all integers. The second fact to observe is that $C(a, b)$ has no element larger than $|a|$ nor smaller than $-|a|$ (the same holds for $|b|$ and $-|b|$) because of Exercise 7e. Strictly speaking, we would use the slightly more general statement

$$\forall d, n \in \mathbb{Z}, (n \neq 0, d|n) \Rightarrow |d| \leq |n|,$$

but this is just a small generalization of 7e.

Because $C(a, b)$ is nonempty and bounded above, the well ordering principle implies that $C(a, b)$ has a largest element. This is the greatest common divisor.

**Definition 4.** The greatest common divisor, denoted gcd, of two integers $a, b$ at least one of which is nonzero is given by

$$\text{gcd}(a, b) = \max C(a, b).$$

We exclude the case $a = b = 0$, as in this case $C(a, b) = \mathbb{Z}$. In this case, we’ll define gcd$(0, 0) = 1$.

One of the features of the greatest common divisor is its very existence shows every rational number can be written in reduced form.

**Theorem 2.** Every rational number $r \in \mathbb{Q}$ can be written in the form $r = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ have that $q > 0$ and gcd$(p, q) = 1$.

**Proof.** Let $r$ be rational. By definition, this implies that $r = \frac{p'}{q'}$ for some $p', q' \in \mathbb{Z}$ with $q' \neq 0$. Let $k = \text{gcd}(p', q')$ if $q' > 0$, and let $k = -\text{gcd}(p', q')$ if $q' < 0$. Then by definition of divisibility, there are $p, q \in \mathbb{Z}$ so that we have $p' = pk$ and $q' = qk$. By how we chose the signs, $q > 0$. Then $r = \frac{p}{q}$.

To see that gcd$(p, q) = 1$, let’s suppose not and look for a contradiction. Let $\ell = \text{gcd}(p, q)$, and let’s suppose $\ell > 1$. Then $k\ell$ divides $p'$ and $q'$, but $k\ell > k$ which contradicts that $k$ is the greatest common divisor.
3.1 Irrationality of $\sqrt{2}$

We will take a small detour from our path to proving the fundamental theorem of arithmetic to proving the irrationality of $\sqrt{2}$, which we can now tackle.

**Definition 5.** An integer $z \in \mathbb{Z}$ is **even** if and only if $2 | z$. Otherwise, we say $z$ is **odd**.

Unpacking the definition, the statement $z$ is even means that $z = 2k$ for some integer $k$. Intuitively, we would like $z$ being odd to mean that $z = 2k + 1$ for some integer $k$, but this does not follow from the definition. It does however follow from the division algorithm.

**Lemma 6.** An integer $z$ is odd if and only if $z = 2k + 1$ for some integer $k$.

**Proof.** By the division algorithm, for any $z \in \mathbb{Z}$ we can write $z = 2q + r$ for integers $q$ and $r$ where $0 \leq r < 2$. Therefore $r$ is either 0 or 1.

If $z$ is odd and $r = 0$, then $z = 2q$. By definition, this makes $z$ even as well, a contradiction.

So if $z$ is odd, then $r = 1$. So far we have only claimed one implication.

If $z = 2k + 1$ for some $k \in \mathbb{Z}$ and $z$ is even, then $2 | z$ and $2 | 2k$ implies that $2 | (z - 2k)$. This implies that $2 | 1$. However, divisors are less than that which they divide (Ex 7e), a contradiction. Therefore $z$ must be odd.

The corollary of this, which uses this lemma and a case-by-case analysis, is:

**Corollary 1.** For all $a, b \in \mathbb{Z}$, if $ab$ is even then at least one of $a$ or $b$ is even.

**Proof.** Let $a, b \in \mathbb{Z}$ be arbitrary. We use the contrapositive. Suppose now that $a$ and $b$ are odd. Then there are $k, \ell \in \mathbb{Z}$ so that $a = 2k + 1$ and $b = 2\ell + 1$. Then

$$ab = 2k(2\ell + 1) + 2\ell + 1 = 2(2k\ell + k + \ell) + 1,$$

which is odd. 

This leads us to the proof of the irrationality of $\sqrt{2}$.

**Theorem 3.** There is no rational $r \in \mathbb{Q}$ so that $r \cdot r = 2$.

**Proof.** Suppose not. Then we can write this rational $r$ in reduced form, $r = \frac{p}{q}$ with $\gcd(p, q) = 1$. Rewriting $r \cdot r = 2$,

$$p \cdot p = 2 \cdot q \cdot q.$$

This implies that $p \cdot p$ is even. By Corollary 1, this implies that $p$ is even. So $p = 2k$ for some $k \in \mathbb{Z}$. This implies that

$$(2 \cdot 2)k \cdot k = 2 \cdot q \cdot q.$$ 

Cancelling a factor of 2, we have that

$$2k \cdot k = q \cdot q.$$

By the same argument, made for $p$, we conclude that $q$ is even as well. This makes 2 a common factor of $p$ and $q$, which implies their gcd is larger than 1. However, this contradicts that the $\gcd(p, q) = 1$. 

Math 3345 Number theory notes Fall 2016
3.2 Bézout’s Lemma

The final feature of the greatest common divisor that we need is Bézout’s lemma, which at first look is a very strange way to view the greatest common divisor. However, it’s a very powerful tool, which we’ll need to prove the fundamental theorem of arithmetic. It’s also very useful for establishing basic properties about the greatest common divisor.

**Lemma 7 (Bézout’s Lemma).** For all \(a, b \in \mathbb{Z}\), at least one of which is nonzero, we have that \(\gcd(a, b)\) is the smallest nonnegative linear combination of \(a\) and \(b\). That is, if we let

\[
S = \{ z \in \mathbb{N} : \exists s, t \in \mathbb{Z}, z = sa + tb \},
\]

then \(\gcd(a, b) = \min S\).

**Proof.** The set \(S\) is bounded below and always contains both \(|a|\) and \(|b|\), so we can apply the WOP. Let \(g\) be this minimal element. By definition, we have that \(g = sa + tb\) for some \(s, t \in \mathbb{Z}\). Therefore, if \(\ell \in C(a, b)\) then

\[
g = sk_1\ell + tk_2\ell
\]

for some \(k_1, k_2 \in \mathbb{Z}\). This means \(\ell | g\), and in particular that \(|\ell| \leq g\). So \(g\) is at least as large as every element of \(C(a, b)\). However, we still don’t know if \(g\) is a common divisor of \(a\) and \(b\), which we show next.

By the division algorithm, there are integers \(q\) and \(r\) with \(0 \leq r < g\) so that \(a = qg + r\). Turning this around,

\[
r = a - qg = a - q(sa + tb) = (1 - qs)a + (-t)b.
\]

Therefore if \(r > 0\), then \(r \in S\). However, \(g\) is the smallest element of \(S\), which is a contradiction with \(r < g\). Therefore \(r = 0\), or in other words, \(g | a\). The same argument shows that \(g | b\), and we have concluded the proof.

The proof reveals even more than was claimed

**Corollary 2.** For all \(a, b \in \mathbb{Z}\), then \(k \in C(a, b)\) if and only if \(k | \gcd(a, b)\).

4 Induction

One of the critical techniques for formulating proofs is the principle of mathematical induction, or just induction for short. We will need this, and its cousin “strong induction” to start proving the statements about prime numbers that we need.

Formally, we could completely skip induction, as it is actually just the well ordering principle in disguise. However, it provides a convenient way to formulate proofs.

The principle of mathematical induction, as a statement in formal logic, goes as follows.

**Theorem 4.** Fix an integer \(n_0\), and suppose that \(P(n)\), for each \(n \in \mathbb{Z}\) having \(n \geq n_0\), is a statement. Suppose that
Base case: $P(n_0)$ is true.

Inductive hypothesis: $\forall n \geq n_0, P(n) \Rightarrow P(n + 1)$.

Then $(\forall n \geq n_0) P(n)$.

Proof. Define a set $S \subset \mathbb{Z}$ by

$$S = \{ n \in \mathbb{Z} : n \geq n_0, P(n) \text{ false} \}.$$ 

We want to show that $S$ is empty. Suppose not. Then by the well ordering principle, $S$ has a smallest element, $s \in S$. Since $P(n_0)$ is true, $s > n_0$, and so $s - 1 \geq n_0$. By definition of how $s$ was chosen, $P(s - 1)$ is true. However, $P(s - 1) \Rightarrow P(s)$, by assumption. So $P(s)$ is true, a contradiction. \[\square\]

We will see induction in action in later sections, when we apply it to prime numbers. One of the other great uses of induction, though, is to prove formulas and estimates for recurrences.

Theorem 5. For all $n \in \mathbb{N}$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}.$$ 

Proof. We will use induction to prove this statement holds for all $\mathbb{N}$. Let $P(n)$ be the statement

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}.$$ 

We always need to prove two things to establish induction: the base case and inductive hypothesis. Typically, the base case will be almost trivial, which is what happens. Since we want to prove something for all $\mathbb{N}$ our base case will be $P(1)$.

Base case: $P(1)$ is true. In this case the desired formula is just

$$1 = \frac{1(2)}{2}.$$ 

Induction hypothesis: $P(n) \Rightarrow P(n + 1)$. Here we assume we’ve established $P(n)$ already, and we want to prove $P(n + 1)$. Writing out one side of the equation in $P(n + 1)$, we have

$$1 + 2 + \cdots + n + (n + 1) = (1 + 2 + \cdots + n) + (n + 1).$$

The point of rewriting the sum this way is to observe that one side of $P(n)$ appears on the right hand side. Since we’re assuming $P(n)$, we can write

$$1 + 2 + \cdots + n + (n + 1) = \frac{n(n + 1)}{2} + (n + 1).$$
The next step is to perform some algebra to make one fraction:

\[ 1 + 2 + \cdots + n + (n + 1) = \frac{n^2 + n + 2n + 2}{2}. \]

The numerator of this right hand side can be factored, though, as

\[ \frac{n^2 + n + 2n + 2}{2} = \frac{(n + 1)(n + 2)}{2} = \frac{(n + 1)((n + 1) + 1)}{2}. \]

Therefore, we have shown \( P(n + 1) \). This concludes the inductive hypothesis. Therefore, by the principle of mathematical induction, we have proved the theorem. \( \square \)

Many similar identities are possible.

Exercise 8: Prove that for all \( n \in \mathbb{N} \),

\[ 1^2 + 2^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}. \]

Exercise 9: Prove that for all \( n \in \mathbb{N} \)

\[ 1 + 3 + 5 + \cdots + (2n - 1) = n^2. \]

Exercise 10: Prove that for all \( n \geq 5 \),

\[ 2^n > 5n. \]

### 4.1 Strong induction

Occasionally, problems appear that where \((n + 1)\)-st case doesn’t neatly depend on the \( n \)-th case, but it instead depends on establishing the statement for all smaller naturals. A simple example is the following exercise:

Exercise 11: Let \( a(1), a(2), \cdots \) be a sequence having the properties:

(i) \( a(1) = 1 \).

(ii) \( \forall n \in \mathbb{N}, a(2n) \leq 3a(n) \).

(iii) \( \forall n \in \mathbb{N}, a(2n + 1) \leq 3a(n) \).

Prove that \( a(n) \leq n^2 \).

This problem, and problems like it, are not naturally set up to apply induction immediately, since the statement \( a(n) \leq n^2 \) can’t naturally be understood in terms of the same statement with \( n \) one less.

Strong (or complete) induction is specifically designed for tasks like this.

Theorem 6. Fix an integer \( n_0 \), and suppose that \( Q(n) \), for each \( n \in \mathbb{Z} \) having \( n \geq n_0 \), is a statement. Suppose that
Base case: $Q(n_0)$ is true.

Weak inductive hypothesis: $\forall n \geq n_0, [(\forall k, n_0 \leq k \leq n)Q(k)] \Rightarrow Q(n + 1)$.

Then $(\forall n \geq n_0)Q(n)$ is true.

The same proof as was given for the principle of mathematical induction would work here as well. However, we give a slightly different proof, intended to illustrate the strong induction actually follows from induction. In this way, strong induction isn’t actually any stronger than induction. In reality, though, both are just versions of the well ordering principle, and it is possible to formalize number theory without the WOP but with induction and subsequently deduce the WOP from induction. In this sense, these are all truly equivalent.

Proof. For each integer $n \geq n_0$, let $P(n)$ be the statement

$$P(n) = (\forall k, n_0 \leq k \leq n)Q(k).$$

We wish to apply the principle of mathematical induction to prove that all $P(n)$, for $n \geq n_0$, are true. This would imply the conclusion of the theorem.

The base case is already one of our assumptions, since $P(n_0)$ is logically equivalent to $Q(n_0)$. We need to show the inductive hypothesis for $P(n)$ from the weak inductive hypothesis for $Q(n)$. The weak inductive hypothesis can be restated as $(\forall n \geq n_0)(P(n) \Rightarrow Q(n + 1))$. However, $P(n + 1)$ is equivalent to $P(n) \land Q(n + 1)$. Since $P(n) \Rightarrow P(n)$, tautologically, we have $(\forall n \geq n_0)(P(n) \Rightarrow P(n + 1))$. Therefore, by the principle of mathematical induction, we have completed the proof. \qed

5 Prime numbers

We now turn to the crown jewel of everything we’ve been building here, the elementary theory of prime numbers. To start, we give the definition of primes.

Definition 6. A number $p \in \mathbb{N}$ is prime if $p > 1$ and the only divisors of $p$ are $\pm 1$ and $\pm p$. Otherwise, we refer to $p$ as composite.

One of the best applications of strong induction is to prove the “easy” half of the fundamental theorem of arithmetic, which we’ll need going forward.

Theorem 7 (Fundamental theorem of arithmetic (existence)). Every $n \in \mathbb{N}$ can be expressed as a product of primes.

The other half of the fundamental theorem of arithmetic states that this expression as a product of primes is unique (up to reordering the product). Note that the case $n = 1$ is included in the statement of this theorem. This is written as an empty product, which one can reason must be 1 for the notion of a product over all elements in a set to be well-defined.

Proof. We use strong induction, the statement $P(n)$ being that “$n$ is expressible as a product of primes.” For the base case, we use the note above the proof.
For the inductive hypothesis, we assume that all of $P(j)$ for $1 \leq j \leq n$ are true and we show that $P(n+1)$ holds. This we do in cases. First, if $n+1$ is prime, then we are done, as it is trivially a product of primes. Otherwise, $n+1$ is composite, and so there are $k$ and $\ell \in \mathbb{N}$ so that $n+1 = k\ell$ and both $k, \ell \leq n$. Since both $k$ and $\ell$ are less than $n$, by assumption, both are expressible as products of primes. Hence

$$n + 1 = (p_1 p_2 \cdots p_r)(q_1 q_2 \cdots q_s),$$

for some primes $p_1, p_2, \cdots$ and $q_1, q_2, \cdots$. Thus $n+1$ is a product of primes, completing the proof by strong induction.

This provides another immediate reward: Euclid’s proof of the infinitude of the primes.

**Theorem 8 (Infinitely many primes).** There are infinitely many prime numbers.

**Proof.** This is another classic contradiction argument. Suppose not. Then there are finitely many primes $p_1, p_2, \cdots, p_\ell$ for some $\ell \in \mathbb{N}$. Let

$$N = p_1 p_2 \cdots p_\ell + 1.$$  

By the existence half of the fundamental theorem of arithmetic, we know that $N$ is a product of primes. Further, it is larger than 1, so it can not be the empty product. This implies there is a prime factor of $N$. By assumption, this is one of the listed primes. Let $p_j$ be this prime, so that $p_j|N$. However, $p_j$ also divides the product $p_1 p_2 \cdots p_\ell$. So, it divides $N - p_1 p_2 \cdots p_\ell$, i.e. it divides 1. This is impossible ($p_j > 1$!), and so we have reached a contradiction.

## 5.1 Uniqueness in the FTA

Our final subject is uniqueness in the FTA, up to reordering. That is, we want to show that if there are two ways of expressing $n \in \mathbb{N}$ as products of primes, those two ways must be the same. Here we need to clarify what we mean by same, since, for example, $2 \cdot 3 = 6 = 3 \cdot 2$.

**Theorem 9 (Fundamental theorem of arithmetic (uniqueness)).** Let $n \in \mathbb{N}$ be arbitrary. Then $n$ has at most one factorization as a product of primes. This means the following. If there are two expressions of $n$ in terms of primes

$$n = q_1 q_2 \cdots q_s$$

$$n = p_1 p_2 \cdots p_t,$$

then $s = t$ and there is a reordering $\pi$ (a function from $\{1, 2, \cdots, s\}$ to itself for which $\pi(i) = \pi(j) \Rightarrow i = j$) so that $q_j = p_{\pi(j)}$.

This theorem will also follow by strong induction on $n$. However, we need a tool before we can proceed. Here we use Bézout’s lemma in a nontrivial way.

**Lemma 8 (Euclid’s lemma).** Suppose $p, a, b \in \mathbb{Z}$ are integers and that $p$ is prime. If $p|ab$ then $p|a$ or $p|b$. 

*Math 3345 Number theory notes* 

Fall 2016
Proof. Let $g = \gcd(p,a)$. As $g|p$, we have that $g = 1$ or $g = p$. If $g = p$, then since $g|a$, we are done. Otherwise, $g = 1$. By Bézout’s lemma, there are integers $s,t \in \mathbb{Z}$ so that

$$1 = sp + ta.$$ 

Multiplying through by $b$, we get

$$b = bsp + tab.$$ 

Now since $p|ab$, there is a $k \in \mathbb{Z}$ so that $pk = ab$. In conclusion

$$b = (bs + kt)p,$$

so that $p$ divides $b$.

This generalizes nicely to the case where $p$ divides a product of multiple terms.

**Corollary 3.** Let $p,k \in \mathbb{N}$ and suppose $p$ is prime. For any collection $a_1,a_2,\cdots,a_k$ of integers, if $p|a_1a_2\cdots a_k$ then there is a $j$ with $1 \leq j \leq k$ so that $p|a_j$.

**Proof.** We prove the statement in the lemma by induction on $k$. The statement with $k = 1$ is tautological.

Suppose the statement of the lemma is proven for $k$. We show that the lemma holds for $k + 1$. Suppose that $a_1,a_2,\cdots,a_k,a_{k+1}$ are any integers for which

$$p|[(a_1a_2\cdots a_k)a_{k+1}].$$

Then $p$ divides $a_{k+1}$ or it divides the product $a_1a_2\cdots a_k$, by Euclid’s lemma. In the former case, we are done. In the latter case, by the inductive hypothesis, we conclude $p$ divides some $a_j$.

This is all the more machinery we need to complete the proof of the FTA.

**FTA Uniqueness.** We prove the statement by strong induction. We need to show something for all $n \in \mathbb{N}$. Let $P(n)$ be the statement that $n$ has a unique factorization as a product of primes. The base case, when $n = 1$, is trivial as any nonempty product of primes will be larger than 1.

For the inductive hypothesis, suppose we have shown that any factorization is unique for all $1 \leq k \leq n$. We now show that any factorization of $n+1$ is unique. Suppose there are two factorizations

$$q_1q_2\cdots q_s = n + 1 = p_1p_2\cdots p_t.$$ 

Then we have that $q_s$ divides the right hand side. By Euclid’s lemma (or the corollary to it), it therefore divides one of $p_j$. By swapping the ordering of the $(p_1,p_2,\cdots,p_t)$, we can assume it divides $p_t$.

Since $p_t$ is prime and $q_s|p_t$, it must be that $q_s = p_t$ using the definition of primality for $p$. Then, we can cancel $q_s$ from both sides of this product. This produces

$$q_1q_2\cdots q_{s-1} = p_1p_2\cdots p_{t-1}.$$ 

By the inductive hypothesis, we therefore conclude $s - 1 = t - 1$, and the reordering $\pi$ exists. Extending this reordering to let $\pi(s) = s = t$, we have completed the proof. 

---

Math 3345 Number theory notes Fall 2016