Chapter 1: The Integers

Greg Knapp

January 12, 2022

1 Introduction

- Fermat's last theorem
- Catalan's Conjecture: If $m, n \in \mathbb{Z}_{\geqslant 2}$, then the only nonzero solution in $\mathbb{Z}$ to $x^m - y^n = 1$ is $3^2 - 2^3 = 1$
  - Cassels showed (using methods you'll be able to understand after one or two terms of this class) that if p and q are prime and $x, y \in \mathbb{Z}$ satisfy $x^p - y^q = 1$, then x is a multiple of q and y is a multiple of p
  - Later, Tijdeman and Langevin (using methods you'll need a lot more study to understand) showed that $|x|, |y|, p, q < \exp\exp\exp\exp\exp(730)$
  - The proof was finished by Mihailescu using methods you'll only need a little bit more study to understand after this course.

2 Section 1.1—Numbers and Sequences

2.1 Number Systems

- First order of business: figure out what numbers we want to study
- Before we can do that, we should probably figure out what types of numbers there are
- At the heart of everything is the number 0. This is the easiest number.
- There are more numbers than 0 of course, but the question is, how can we construct them?
- Let's create a function called "successor"
- This function takes in a number and adds 1, i.e. the successor of 0 is 1, the successor of 1 is 2, and so on.
- Now we've created the set of natural numbers: $\mathbb{N} = \{0, 1, 2, \dots\}$
- $\mathbb{N}$ comes with the nice operation of addition: if you add any two numbers in $\mathbb{N}$, you get another number in $\mathbb{N}$.
- $\mathbb{N}$ also has multiplication in it: if you multiply two numbers in $\mathbb{N}$, you get another number in $\mathbb{N}$.
- What do I mean by operation? Something you can do to numbers to remain in the given set.
- But $\mathbb{N}$ doesn't come with some of the other operations we like: subtraction and division to name two
- To get the negative integers, we could create a "predecessor" function
- Or we could say "let's make every number have an additive inverse" (i.e. if n is a number, let's make there be another number x which makes $n + x = 0$)

- Either way, we get the full range of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- We still have addition, multiplication, subtraction, but not division
- To give ourselves the division operation, we now have to allow ourselves fractions:
- We now define $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}$
- Now we have all the operations that we like!
- Question: have we gotten all the numbers?
- Answer: No. I claim that $\sqrt{2} \notin \mathbb{Q}$
- Proof: (there are lots, including some that are better than this one)
  - Suppose (by contradiction) that $\sqrt{2}$ is irrational
  - Then there exist positive integers a and b so that $\sqrt{2} = a/b$
  - Define the set $S := \{k\sqrt{2} \mid k, k\sqrt{2} \in \mathbb{Z}_{>0}\}$
  - Note that S is nonempty: $b\sqrt{2} = a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, so $b\sqrt{2} \in S$
  - S is subset of $\mathbb{N}$: therefore, it has a least element (this is called the well-ordering property of $\mathbb{N}$—that every nonempty subset of $\mathbb{N}$ has a least element)
  - Call this least element $s = t\sqrt{2}$ for $t \in \mathbb{Z}_{>0}$
  - We claim that there is a smaller element of S than s (and hence, will have a contradiction)
  - Note that $(s-t)\sqrt{2} = s\sqrt{2} - t\sqrt{2} = s\sqrt{2} - s = 2t - s$ is an integer
  - Furthermore, this number is positive because $\sqrt{2} > 1$ (and so $s\sqrt{2} > s$). Therefore, $s - t$ is positive.
  - This implies that $s - t \in \mathbb{Z}_{>0}$ and $(s-t)\sqrt{2} \in \mathbb{Z}_{>0}$.
  - Therefore, $(s-t)\sqrt{2} \in S$.
  - But $(s-t)\sqrt{2} = s\sqrt{2} - s = s(\sqrt{2} - 1) < s$ because $\sqrt{2} - 1 < 1$
  - Hence, we have found a smaller element of S
  - This is a contradiction, so we find that $\sqrt{2}$ is irrational
- Okay, so now we know that the set of real numbers $\mathbb{R}$ (which we're not going to carefully define) is larger than $\mathbb{Q}$.
- There are other irrational numbers too, like π and e.
- Note that $\sqrt{2}$ is the root of a polynomial with integer coefficients: $x^2 - 2$
- Because of this we say that $\sqrt{2}$ is *algebraic*
- **Def:** A number α is *algebraic* if there exists a polynomial $f(x)$ with integer coefficients for which $f(\alpha) = 0$
- **Def:** We denote the set of algebraic numbers by $\bar{\mathbb{Q}}$
- Observe, $\bar{\mathbb{Q}}$ has more numbers than $\mathbb{R}$: i is a root of $x^2 + 1$
- Question: but does $\bar{\mathbb{Q}}$ contain $\mathbb{R}$? (i.e. do we have all of the numbers?)
- Answer: No, but this isn't obvious!

2.2 Sequences

- **Def:** A *sequence* is a list of numbers $a_0, a_1, a_2, a_3, \ldots$
- It's often good practice to be able to take the first few terms of the sequence and write down the formula or come up with the pattern
- **Ex:** Guess a formula for a_n if the first few terms of the sequence are $3, 11, 19, 27, 35, 43, \ldots$
- **Def:** This forms a special type of sequence called an *arithmetic progression*: i.e. a sequence of the form $a, a+d, a+2d, a+3d, \ldots$.
- An important feature of an arithmetic progression is that consecutive terms differ by a constant amount: d
- Another important type of sequence is the...
- **Def:** A *geometric progression* is a sequence of the form $a, ar, ar^2, ar^3, \ldots$
- An important feature of a geometric progression is that consecutive terms have a constant ratio: r
- **Ex:** $1, 2, 4, 8, \ldots$ forms a geometric progression
- With these important types of sequences out of the way, we want to focus on why we introduced them: set sizes

2.3 Set Sizes

- **Def:** A set S is *countable* if it is finite OR there exists a function $f : \mathbb{N} \to S$ which is one-to-one and onto (i.e. f is a bijection). A set is *uncountable* if no such function exists.
  - RECALL: $f : X \to Y$ is one-to-one (or injective) if for every $x_1, x_2 \in X$: if $f(x_1) = f(x_2)$, then $x_1 = x_2$ (i.e. every output has a unique input)
  - RECALL $f : X \to Y$ is onto (or surjective) if for every $y \in Y$, there exists $x \in X$ with $f(x) = y$ (i.e. every member of y is an output of f)
- Observe that an infinite set is countable if and only if it can be written as a sequence
  - If S is countably infinite, then there exists a bijection $f : \mathbb{N} \to S$.
  - Define $a_0 = f(0)$, $a_1 = f(1)$,...,$a_n = f(n)$,...
  - Note that because f is surjective, every element of S is in this sequence.
  - If S can be written as a sequence, write its elements as $a_0, a_1, a_2, \ldots$
  - Then define $f : \mathbb{N} \to S$ by $f(n) = a_n$.
  - f is surjective because every element of S is some a_n and it is injective because if $f(n) = f(m)$, then $a_n = a_m$, which implies that $n = m$.
- Now, to analyze set sizes, we'll try to write them as sequences.
- Claim: the integers are countable
- Claim: the rationals are countable

0/1	1/1	-1/1	2/1	-2/1	3/1	-3/1
0/2	1/2	-1/2	2/2	-2/2	3/2	-3/2
0/3	1/3	-1/3	2/3	-2/3	3/3	-3/3

- Claim: the reals are uncountable
- Fact: the algebraic numbers are countable

2.4 Back to Number Systems

- We have the following picture $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ and $\mathbb{Q} \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$
- Number theorists tend to want to answer questions about $\mathbb{N}$
- However, the operations and tools are better in some of the nearby number systems like $\mathbb{Z}$ and $\mathbb{Q}$
- It's not obvious, but there are also nice features of $\bar{\mathbb{Q}}, \mathbb{R}$, and $\mathbb{C}$, too (for the purposes of number theory)
- We won't see many of those uses in this course.

3 Section 1.3—Mathematical Induction

3.1 The Principle of Induction

- We're familiar with the basic idea of how to prove statements about "all natural numbers" by induction
- Let's start with a more formal statement, however:
- <u>The Principle of Mathematical Induction:</u> Suppose that $S \subseteq \mathbb{N}$ and that $0 \in S$. Additionally, suppose that if $k \in S$, then $k + 1 \in S$. Then $S = \mathbb{N}$.
- Note two things about this
  1. This doesn't look like the "proof by induction method with which we're familiar"
  2. This is stated like a theorem
- To address the first point, how does this principle yield the familiar proof method?
- Do this part in two columns:
  - Say you want to show that $\varphi(n)$ is true for all n (here, I'm using φ to refer to a property, not a function—maybe $\varphi(n)$ is the statement "n is either even or odd")
  - Typically with induction you will first show that $\varphi(0)$ is true, then show that $\varphi(n) \to \varphi(n + 1)$ for all n. Last, you will conclude that $\varphi(n)$ is true for all n
  - To rephrase this process in terms of the principle, suppose you start with your property φ
  - Let $S := \{n \in \mathbb{N} : \varphi(n) \text{ is true}\}$
  - Showing that $\varphi(0)$ is true is equivalent to showing that $0 \in S$
  - Showing that $\varphi(n) \to \varphi(n + 1)$ is equivalent to showing that $n \in S$ implies $n + 1 \in S$
  - Concluding that $\varphi(n)$ is true for all n is equivalent to showing that $S = \mathbb{N}$
- To address the second point, the Principle of Mathematical Induction is actually an axiom.

3.2 Relation to Well-Ordering and Strong Induction

- But it's interesting to note that it is equivalent to the Well-Ordering Principle: the claim that every non-empty set of natural numbers has a least element.
- Proof that well-ordering implies induction
  - Suppose that the well-ordering principle holds: we aim to show induction.
  - Suppose that $S \subseteq \mathbb{N}$ has $0 \in S$ and if $k \in S$, then $k + 1 \in S$
  - By contradiction, assume that $S \neq \mathbb{N}$
  - Then $X = \mathbb{N} \setminus S$ is nonempty and hence, has a least element, say x.
  - Since $0 \in S$, $x \neq 0$

  - Since x is the least member of X, it follows that $x-1 \notin X$ (and $x-1 \in \mathbb{N}$ since $x \neq 0$), so $x-1 \in S$.
  - But since $x-1 \in S$, it follows that $x=(x-1)+1 \in S$.
  - Contradiction. Therefore, $S=\mathbb{N}$

- The other direction is a little more tricky and is easiest if we pass through an intermediary
- The Principle of Strong Induction: Suppose $S \subseteq \mathbb{N}$ with $0 \in S$. Suppose also that $0,1,2,\ldots,k \in S$ implies that $k+1 \in S$. Then $S=\mathbb{N}$.
- Note first that induction implies strong induction (i.e. anything you can prove by induction, you could also prove with strong induction)
- Here's something weird that we see:
- Proof that strong induction implies well-ordering
  - We do this by contrapositive
  - Suppose that $X \subseteq \mathbb{N}$ has no least element and $X \neq \varnothing$
  - Take $S=\mathbb{N} \setminus X$ and note that $0 \in S$ because if 0 were in X, then X would have a least element
  - Suppose now that $0,1,\ldots,k \in S$.
  - Then $k+1 \notin X$ because that would make X have a least element
  - Hence, $k+1 \in S$
  - So S satisfies our strong induction properties.
  - But note that $S \neq \mathbb{N}$ because X (by hypothesis) is nonempty
  - So strong induction fails
- The interesting conclusion here is that strong induction implies regular induction (i.e. anything you can prove with strong induction, you can also prove with weak induction)
- This seems odd because strong induction lets you assume so much more: you don't just get to assume that $n \in S$ when showing that $n+1 \in S$, you also get to assume that $0,1,2,\ldots$ etc. are all in S
- Note that these arguments don't really tell you how to convert a strong induction argument to an induction argument—they just say that it can be done.

3.3 Examples

- Show that for all $n \geqslant 1$, $n^2=\sum_{j=1}^{n}(2j-1)$
- Review sigma notation
- Proof:
  - True for 1
  - Now suppose that $n^2=\sum_{j=1}^{n}(2j-1)$
  - Then $(n+1)^2=n^2+2n+1=\left(\sum_{j=1}^{n}(2j-1)\right)+2n+1=(1+3+5+\cdots+2n-1)+2n+1=\sum_{j=1}^{n+1}2j-1$
- Show that for all $n \geqslant 4$, $2^n<n!$
  - $n=4$ check
  - Suppose that $n \geqslant 4$ and $2^n<n!$
  - Our goal is to show that $2^{n+1}<(n+1)!$

  - If we think about how we get from 2^n to 2^{n+1}, we multiply by 2
  - If we think about how we get from $n!$ to $(n+1)!$, we multiply by $n+1$
  - To formalize this, we use the inequalities: $2^{n+1} = 2^n \cdot 2 < n! \cdot 2 < n! \cdot (n+1) < (n+1)!$

- Show that $\sum_{k=0}^{n} \frac{1}{2^k} = 2 - \frac{1}{2^n}$.
  - $n = 0$ check
  - Suppose true for n
  - We want to show: $\sum_{k=0}^{n+1} \frac{1}{2^k} = 2 - \frac{1}{2^{n+1}}$
  - Note that $\sum_{k=0}^{n+1} \frac{1}{2^k} = \frac{1}{2^{n+1}} + \sum_{k=0}^{n} \frac{1}{2^k} = \frac{1}{2^{n+1}} + 2 - \frac{1}{2^n} = 2 - \frac{1}{2^{n+1}}$
  - Done

- Conjecture a formula for A^n where $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and prove your formula by induction.

4 Section 1.5—Divisibility

4.1 The Basics

- Proof by induction relies heavily on the additive properties of the integers
- You might wonder: is there a similar axiom/theorem that relies on multiplicative properties?
- This is a bit trickier since the natural numbers are additively generated by 1.
- What are the natural numbers multiplicatively generated by?
- **Def:** If $a, b \in \mathbb{Z}$, we say that a *divides* b if there exists $c \in \mathbb{Z}$ so that $ac = b$. In this case, we also say that b is a *multiple* of a and that a is a *divisor* or *factor* of b. We write $a \mid b$ if a divides b and $a \nmid b$ otherwise.
- Some notes: a and b are allowed to be positive or negative.
- E.g. the divisors of 27 are $\pm 1, \pm 3, \pm 9, \pm 27$. Hence, $-3 \mid 27$, but $5 \nmid 27$
- Some essential facts:
  - $1 \mid n$ for every n
  - $0 \nmid n$ for every n
  - $n \mid 1$ if and only if $n = \pm 1$
  - $n \mid 0$ for every $n \neq 0$
  - $a \mid b$ if and only if $a \neq 0$ and $\frac{b}{a}$ is an integer

4.2 Some Results

- **Thm:** If $a, b, c \in \mathbb{Z}$, $a \mid b$, and $b \mid c$, then $a \mid c$.
  - How do we prove this?
  - Start with the conclusion: determine that I want to find a $k \in \mathbb{Z}$ so that $ak = c$
  - Translate what the hypotheses mean: there exists $m, n \in \mathbb{Z}$ so that $am = b$ and $bn = c$
  - Note that I have a c in what I want and a c in my hypotheses: $c = bn$ and try to manipulate the other side to get what we want
  - $c = bn = (am)n = a(mn)$
  - We've now shown that c is a multiple of a and we conclude that $a \mid c$

- **Thm:** If $a, b, c, m, n \in \mathbb{Z}$ and if $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$
  - To think about this theorem, we want to understand what it is saying first
  - If you don't understand it, you can't prove it
  - "If a is a multiple of c and b is a multiple of c, then any (integer) linear combination of a and b is also a multiple of c"
  - For example: taking $a = 10, b = 15$, and $c = 5$, this theorem says that $10m + 15n$ will be a multiple of 5. And of course it will: $10m$ means "move right by 10 units m times" and $15n$ means "move right by 15 units n times" and those movements will always land you on a multiple of 5
  - To formally prove this, however, we have to show that there exists $k \in \mathbb{Z}$ so that $ck = ma + nb$
  - We know for sure that there exists $r, s \in \mathbb{Z}$ so that $cr = a$ and $cs = b$.
  - Note then that $ma + nb = m(cr) + n(cs) = c(mr + ns)$
  - Hence, $k = mr + ns$ works and we have that $c \mid ma + nb$

4.3 Integral Division

- We said earlier that $b \mid a$ iff $b \neq 0$ and $\frac{a}{b} \in \mathbb{Z}$
- But what can we say when $b \nmid a$? Or when we don't know if $b \mid a$?
- You're probably familiar with long division, but let me remind you of the algorithm:
- E.g. Divide 127 by 3
- We want to generalize this to "Divide a by b," though there are two questions:
  1. What do we get?
  2. How do we know we're going to get it?
- Rather than worry too much about how to formalize the algorithm and prove its results (do that in a CS class), we're going to use this algorithm as inspiration for a theorem
- We first need to figure out what we get
- Note that the previous result gave us $\frac{127}{3} = 42 + \frac{1}{3}$
- It's important that the numerator of the fraction is
  1. Positive (if it were, say $42 + \frac{-1}{3}$, then we would rather write $\genfrac{}{}{0pt}{}{41}{+}\frac{2}{3}$)
  2. Smaller than 3 (if it were, say $42 + \frac{5}{3}$, then we would rather write $43 + \frac{2}{3}$)
- With this in mind, we don't really like the equation $\frac{127}{3} = 42 + \frac{1}{3}$ because it isn't about natural numbers.
- So let's clear denominators and write $127 = 42 * 3 + 1$
- Here, 42 is the quotient and 1 is the remainder.
- **Thm:** If $a, b \in \mathbb{Z}$ with $b > 0$, then there are unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leqslant r < b$
  - For proof, let $T = \{a - bk \in \mathbb{N} : k \in \mathbb{Z}\}$
  - Note that $T \subseteq \mathbb{N}$
  - Also note that $T \neq \varnothing$ since we can pick any $k \in \mathbb{Z}$ with $k \leqslant \frac{a}{b}$ and get that $a - bk \geqslant 0$
  - By the well ordering principle, we conclude that T has a least element, say $r = a - bq$
  - We've now shown that $a = bq + r$ for some r and q; we still need to show that $0 \leqslant r < b$

- $r \geqslant 0$ by the fact that $T \subseteq \mathbb{N}$
- Suppose, by contradiction, that $r \geqslant b$.
- Then $r - b \geqslant 0$ and so we write $a = bq + b + (r - b)$ and we have $r - b = a - b(q + 1)$.
- But then $r - b \in T$, contradicting the minimality of r
- Hence, $r < b$
- To see what's going on, draw the number line
- Next up: check uniqueness.
- The standard way to show uniqueness is to suppose that you have two ways of doing something, then show that they're actually the same
- Suppose that $a = bq_1 + r_1$ and $a = bq_2 + r_2$ where $0 \leqslant r_1, r_2 < b$
- Then $0 = b(q_1 - q_2) + (r_1 - r_2)$, so $b(q_1 - q_2) = r_2 - r_1$
- Hence, $b \mid r_2 - r_1$
- Since $0 \leqslant r_2 < b$, we can subtract r_1 and get $-b < -r_1 \leqslant r_2 - r_1 < b - r_1 \leqslant b$.
- The only multiple of b between $-b$ and b is 0, so $r_2 - r_1 = 0$.
- Hence, $q_2 = q_1$ and we are done.

- Why is this important?
  - One main reason is that we often like to take a positive integer d and classify numbers according to their remainders when divided by d
  - For instance "even" means remainder 0 when divided by 2 and "odd" means remainder 1 when divided by 2
  - Clocks operate on the same principle: to convert from 24 hour time to 12 hour time, you look at the remainder when divided by 12

4.4 Some Divisibility Examples

- **Ex:** Show that every $n \in \mathbb{Z}$ falls into one of the following four categories:
  1. Even: n is even
  2. Threven: $3 \mid n$
  3. Plus one: The remainder when dividing n by 6 is 1
  4. Plus five: The remainder when dividing n by 6 is 5

  Are the categories disjoint?

- Proof
  - Can try to prove with induction, but that's a mess
  - Instead, take n divided by 6 and observe...
  - $n = 6k + 0$: even
  - $n = 6k + 1$: plus one
  - $n = 6k + 2$: even
  - $n = 6k + 3$: threven
  - $n = 6k + 4$: even
  - $n = 6k + 5$: plus five
  - Note that the categories are not disjoint; the only overlap occurs at the multiples of 6 which are both even and threven.

- **Ex:** Show that for all $n \in \mathbb{Z}$, $6 \mid n(n+1)(2n+1)$
- Proof:
  - To show that $n(n+1)(2n+1)$ is a multiple of 6, it suffices to show that it is a multiple of 2 and a multiple of 3 (see previous example)
  - For any n, either n or $n+1$ is even, so $2 \mid n(n+1)(2n+1)$
  - But it's not clear that one of $n, n+1$, and $2n+1$ is a multiple of 3.
  - Let's investigate further. If n has the form [blank] (on division by 3) then $n+1$ and $2n+1$ have the form [blank]

n	$n+1$	$2n+1$
$3k$	$3k+1$	$6k+1$
$3k+1$	$3k+2$	$6k+3$
$3k+2$	$3k+3$	$6k+5$

  - Note that there is a multiple of 3 in each row, so one of n, $n+1$, and $2n+1$ is a multiple of 3

4.5 GCDs

- If a and b are integers with either a or b nonzero, the nonzero ones have finite sets of divisors, say A and B, implying that $A \cap B$ is finite
- Hence, $A \cap B$ has a largest element.
- **Def:** This largest element is called the *greatest common divisor* of a and b and we denote it with $\gcd(a, b)$ or just as (a, b)
- Reason for the latter notation: it's referring to the ideal generated by a and b which is equal to the ideal generated by $\gcd(a, b)$ (for later)
- In the case of a and b being 0, we define $(0, 0) = 0$
- This lines up with the ideal idea or just makes our statements about gcds true
- **Ex:** $(24, 84) = 12$ because the divisors of 24 are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24$ and the divisors of 84 are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm7, \pm12, \pm14, \pm21, \pm28, \pm42, \pm84$
- **Ex:** $(n, 0) = n$ for all n
- **Ex:** $(n, 1) = 1$ for all n
- Of particular interest are numbers with $(a, b) = 1$.
- **Def:** If $(a, b) = 1$, we say that a and b are *relatively prime* or we say that a is *(relatively) prime to* b.
- We'll study these more in chapter 3 and we'll get a better algorithm for computing them than just "factor and decide"