Math 170: Brief notes

Svetlana Makarova

Truong-Son Van

Contents

Introduction

You may still be thinking about your major and trying this class as a part of exploration. Or this may be the only math class that you take in your four years of undergraduate studies, and you may be wondering why the university imposed such a requirement on you.

Instead of trying to find my own words for a motivational speech, let me cite Abraham Lincoln when he answered in 1864 how he had aquired his persuasive rhetorical skill:

> "In the course of my law-reading I constantly came upon the word *demonstrate*. I thought, at first, that I understood its meaning, but soon became satisfied that I did not. ... I consulted Webster's dictionary. That told of "certain proof", "proof beyond the possibility of doubt"; but I could form no idea what sort of proof that was. I thought a great many things were proved beyond a possibility of doubt, without recourse to any such extraordinary process of reasoning as I understood "demonstration" to be. I consulted all the dictionaries and books of reference I could find, but with no better results. You might as well have defined *blue* to a blind man. At last I said, "Lincoln, you can never make a lawyer if you do not understand what *demonstrate* means"; and I left my situation in Springfield, went home to my father's house, and staid there till I could give any propositions in the six books of Euclid at sight. I then found out what "demostrate" means, and went back to my law studies."

We see that the 16th president of the US highly regarded Euclid's "Elements" for its teaching of rigor and reasoning, and not as much for its content. The textbook itself is 2300 years old and you may think that it may have outdated material (arguably, this is a correct guess), but it has survived more than a thousand of editions, and mathematicians only came

up with other logically consistent geometries in the nineteenth century, thus rendering Euclid's work as one of the many possibilities. For more than two thousand years, this book was considered something all educated people had read, and it only came down this pedestal in the 20th century, by which time its content was universally taught through other school textbooks.

But as much as this book was central to the western European civilization (second to Bible), not all people are fond of planar geometry. In this course, we will offer an alternative invitation to the land of reason by means of showing many possible facets of mathematics. If you wish, you may consider it a collection of trailers for higher-level math courses.

CHAPTER 1

Warm-up: pigeonhole and numbers

1. Pigeonhole principle

Let me start with a question to you.

EXERCISE 1. *Last time I checked, there were 79 students enrolled in this course. Can anyone tell me if there is at least one pair of students whose birthday happen on the same week? Any guesses?*

In fact, I guarantee you, without knowing any of your birthdays, that yes. Moreover, I can guarantee that for some seven people in our class, their birthdays fall on the same month. And I am so sure of it because I can prove it using the "pigeonhole principle".

THEOREM 1.1 (Pigeonhole principle). *If $k > 0$ is a number of pigeonholes, and n pigeons try to occupy them, with $n > k$, then there will necessarily be a pigeonhole with at least two pigeons in it.*

Here is a brief example with $k = 9$ and $n = 10$:

The statement sure seems obvious, but let us prove it as a warm-up, and then we'll use it to prove our first claim about birthdays.

PROOF. We use a proof by contradiction. Assume that none of the boxes has more than one item. Then we would only have at most k items on our hands. But we assumed that the number of items is greater than k, so we

arrived at a contradiction, and our assumption was false. So there must be a box with at least two items. □

EXAMPLE 1.2. In a class of 79 students, there are at least two students whose birthdays fall on the same week.

PROOF. Here the weeks in a year – total of 52 – play the role of pigeonholes, and students – total of 79 – play the role of pigeons. □

EXAMPLE 1.3. There are two people in Pennsylvania with the same number of hairs on their body.

PROOF. Possible numbers of hairs on a human body play the role of pigeonholes and people play the role of pigeons. By googling, we can find that people usually have 5 million hairs on their body and the population of Pennsylvania is 13 million. Therefore, by pigeonhole principle, there should exist at least two people with the exact same number of hairs. □

Now you may think that that was easy. Let us take it up a notch and see what happens when you have many more pigeons than pigeonholes.

THEOREM 1.4 (Generalized pigeonhole principle). *If $k > 0$ is a number of pigeonholes, and n pigeons try to occupy them, with $n > mk$ for some positive integer m, then there will necessarily be a pigeonhole with at least $m + 1$ pigeons in it.*

In other words, we can say that if n pigeons occupy k pigeonholes, then there is at least one pigeonhole containing at least $\lceil \frac{n}{k} \rceil$ items. The number $\lceil \frac{n}{k} \rceil$ is defined as the smallest integer that is larger than $\frac{n}{k}$.

EXERCISE 2. *Prove Theorem 1.4.*

EXAMPLE 1.5. In a class of 79 students, there are at least seven students whose birthdays fall on the same month.

PROOF. Here the months in a year – total of $k = 12$ – play the role of pigeonholes, and students – total of $n = 79$ – play the role of pigeons. Then we can calculate that $n = 6 \cdot k + 7$, so by the generalized pigeonhole principle (Theorem 1.4) there are at least $6 + 1 = 7$ students whose birthdays occur in the same month. □

EXAMPLE 1.6. Pennsylvania needs to have at least two area codes for the phone numbers, while the US needs at least 42.

PROOF. Phone numbers in the US have the format $+1\,(AAA)\,N******$, where AAA is the area code. The six stars are digits from 0 to 9, while N can only be from 2 to 9. There are more subtle rules that you can find in Wikipedia on the page "North American numbering plan", but further restrictions do not affect the order of magnitude, so let us ignore them for now. With this, the total possible number of variants to fill the stars is $8 \cdot 10^6 = 8\,000\,000$, so $k = 8$ million. As we have found out before, there are $n = 13$ million people in Pennsylvania. So minimal number of area codes is $\lceil \frac{13}{8} \rceil = 2$.

The population of the US is $n = 328.2$ million, so you will need at least $\lceil \frac{328.2}{8} \rceil = 42$ area codes. □

In fact, if you google, you will find out that major cities in any state have their own area codes, sometimes a couple, and the total number of area codes is now around 320.

EXERCISE 3. *Can you think of reasons to have so many area codes? (Logistical, social, etc.) Do you think there is a restriction on applying mathematical ideas in real life?*

2. Proving things with the pigeonhole principle

Material for this section is take from https://www.math.uvic.ca/faculty/gmacgill/guide/pigeonhole.pdf.

As we saw in the above examples, there are four steps involved:

(1) Decide what pigeons are. They will be the things among which we want to find several of that have the same property.
(2) Set up pigeonholes. In order for the pigeonhole principle to work, it is necessary to have fewer pigeonholes than pigeons. Sometimes you need an astute observation to do this.
(3) Give a rule for assigning the pigeons to the pigeonholes. The pigeonhole principle works for any rule – you just need to choose the rule that works best for your situation.
(4) Apply the pigeonhole principle to your setup and get the desired conclusion.

EXERCISE 4. *Prove that if seven distinct numbers are selected from* $\{1, 2, \ldots, 11\}$ *(braces are used to denote a set of objects, e.g. numbers), then some two of these numbers sum to* 12*. Show that you can find six number so that no pair among those sums up to* 12*.*

(1) Let the pigeons be the numbers selected.
(2) Let the pigeonholes be labeled by the following sets of numbers: $\{1, 11\}$, $\{2, 10\}$, $\{3, 9\}$, $\{4, 8\}$, $\{5, 7\}$, $\{6\}$.
(3) The rule: when a number is selected, it is placed in the pigeonhole with the corresponding label.
(4) There are seven numbers and six pigeonholes, so two of the selected numbers will end up in the same pigeonhole. They cannot both end up in the pigeonhole labeled $\{6\}$ because we are choosing distinct numbers, so it's one of the first five. But then they sum up to 12.

EXERCISE 5. *A party is attended by $n \geqslant 2$ people. Prove that there will always be two people in attendance who have the same number of friends at the party. (Assume that the relation "is a friend of" is symmetric, that is, if X is a friend of Y then Y is a friend of X.)*

Each person either is, or is not, a friend of each of the the other $n - 1$ people in attendance. Thus, the possible values for the number of friends a person can have in attendance at the party are $0, 1, \cdots, n - 1$. However, it can not be the case that there is someone at the party with 0 friends and someone else with $n - 1$ friends simultaneously: if a person is friends with everyone, then everyone at the party has at least one friend there. Thus, the possible values for the number of friends a person can have in attendance at the party are $0, 1, \cdots, n - 2$ or $1, 2, \cdots, n - 1$. In either case, there are n numbers (of friends among the people in attendance) that can take on at most $n - 1$ different values. By the Pigeonhole Princple, two of the numbers are equal. Thus, some two people in attendance who have the same number of friends at the party.

3. Divisibility

Let us now make things a little more abstract with numbers. We will not concern ourselves with where numbers come from (although this is a worthy subject in itself) but will learn how to do things with them. In particular, we will spend some time thinking about something that is very closely related to the pigeonhole principle: divisibility.

Let us first equip ourselves with a vocabulary.

- Natural numbers are numbers that are used for counting, starting from 0. We denote $\mathbb{N}$ to be the set of all natural numbers. Thus,

using set notation[1],

$$\mathbb{N} = \{0, 1, 2, \ldots\}\,.$$

- Integer numbers are numbers that are used to measure the difference between two instances of counting. We denote $\mathbb{Z}$ to be the set of all integers. Thus, using set notation,

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}\,.$$

The shorthand of saying "a belongs to a set S " is by using the notation

$$a \in S\,.$$

For example, the shorthand of "a is an integer" is "$a \in \mathbb{Z}$".

For what to come, we need the notion of the absolute value of a number.

DEFINITION 3.1. The absolute value of a number a is a non-negative quantity that represents the size of that number. In mathematical terms,

$$|a| = \begin{cases} a & \text{if } a \geqslant 0\,, \\ -a & \text{if } a < 0\,. \end{cases}$$

Our strategy for uncovering the structure of the natural numbers is to break down complex objects and ideas into their fundamental components, think about this quote by Desmond Tutu, a South African Anglican cleric and theologian, and a human rights activist[2]:

> There is only one way to eat an elephant: a bite at a time.

For example, when you prepare for an exam, you make a list of topics and learn one topic at a time; when I prepare lectures, I make a list of topics and write about one topic at a time; in both situations we achieve a complex result by taking many small bites. And when we study natural number, we break them down into their simplest building blocks – *prime numbers* – and then study their properties and observe how they interact. One way of breaking the numbers down is to try to divide by a smaller number and observe if there is a remainder. This leads us to the following sequence of definitions.

[1] We will discuss sets later.

[2] See also https://www.psychologytoday.com/us/blog/mindfully-present-fully-alive/201804/the-only-way-eat-elephant.

DEFINITION 3.2. A number $a \in \mathbb{Z}$ is said to be divisible by $b \in \mathbb{Z}$ if there exists a number $q \in \mathbb{Z}$ such that

$$a = bq\,.$$

b is called to be a divisor (or a factor) of a and we can also say that b divides a (notation: $b \mid a$).

The number a is not divisble by b if a can be written in the form

$$a = bq + r\,,$$

where $q, r \in \mathbb{Z}$ and $0 < r < |a|$. The number r is then called the remainder.

Just because I can define something, it doesn't mean that my definition is something that makes sense. For example, I can define a cat to be a mammal that lays eggs (what's wrong?). A good principle in life: question yourself often. Just because there are things you can imagine/define, it doesn't mean that those things exist or even make sense.

QUESTION. *Does Definition 3.2 make sense? Can there be a number that is both divisible and not divisible by another number?*

There is a theorem that guarantees that the situation described in the previous question cannot happen. In other words, Definition 3.2 does make sense.

THEOREM 3.3 (Division theorem). *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist a pair of integers $q, r \in \mathbb{Z}$ such that*

$$a = qb + r \quad \text{and} \quad 0 \leqslant r < |b|\,,$$

and moreover this pair is unique. q is called the quotient of a when divided by b; and r is called the remainder of a when divided by b.

EXAMPLE 3.4. Let $a = 101$ and $b = 3$. Then

$$101 = 33 \cdot 3 + 2\,.$$

Here, $q = 33$ and $r = 2$. As said in the division theorem, $2 < 3$.

EXAMPLE 3.5. A slightly interesting example is when a is positive and b is negative. Say, $a = 23$ and $b = -4$. Then

$$23 = (-5) \cdot (-4) + 3\,.$$

In this case $q = -6$ and $r = 3 < 4$.

We will not prove this theorem for now as it uses the technique of mathematical induction (CS majors would say "recursion").

EXERCISE 6. *Read the proof of this theorem in Newstead's book [New] (Theorem 6.1.1).*

4. Criteria of divisibility

Numbers that are divisible by two are called even, and they have a special name because in many cultures the distinction between odd and even numbers is quite prominent. For example, ancient Greek and Chinese seem to favor odd numbers like 3 and 5. Russian culture traditionally favors 3 and 7: there is a saying that "God loves groups of three", and seven commonly occurs in folk tales. Conversely, Eastern cultures have negative connotations with even numbers, and number 4 in Chinese is associated with death, because quite ominously, we can write it in two ways as an operation on two twos:

$$4 = 2 \cdot 2 = 2 + 2.$$

Some buildings in China skip the fourth floor, just like the thirteenth floor is skipped in some places in the US.

On the other hand, Western cultures seem to "prefer" even numbers. According to a historian of mathematics (Dr. Nishiyama), ancient preference for odd numbers probably faded in the West with the arrival of modern mathematics as represented by Newton. When counting numbers, odd numbers were incomplete, in-between numbers, whereas even numbers were certainly more "rational". This is even reflected in an English proverb that says that two heads are better than one.

So how do we tell even numbers from odd?

PROPOSITION 4.1. *An integer number n is divisible by 2 if and only if its last digit is even (i.e. 0, 2, 4, 6, 8).*

LEMMA 4.2. *Observe that if a number a is divisible by b, then $a + b$, $a + 2b$, etc. are also divisible by b.*

PROPOSITION 4.3. *An integer number n is divisible by 5 if and only if its last digit is 0 or 5.*

PROPOSITION 4.4. *An integer number n is divisible by 4 if and only if its last two digits comprise a number divisible by 4. An integer number n is*

divisible by 8 *if and only if its last three digits comprise a number divisible by* 8.

PROPOSITION 4.5. *An integer number* n *is divisible by* 3 *if and only if the sum of all its digits is divisible by* 3.

PROOF. Prove the criterion of divisibility by 3 by writing the decimal expansion:

$$a = a_k \cdot 10^k + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0 \cdot 1.$$

Notice that $10^k = 9 \ldots 9 + 1$, and the first summand is divisible by 3. So we can write

$$a - 9 \ldots 9 = a_k + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0 \cdot 1.$$

Repeat this process and we can see that the right handside would eventually be

$$a_k + \cdots + a_1 + a_0 \,.$$

Note that a and each of the $9 \ldots 9$ is divisible by 3. Therefore, $a_k + \cdots + a_0$ is divisible by 3. □

PROPOSITION 4.6. *An integer number* n *is divisible by* 9 *if and only if the sum of all its digits is divisible by* 9.

THEOREM 4.7. *Let* $n > 70$ *be a natural number that you want to test for being divisible by* 7.
Step 1: Separate the last digit of the number, call it d.
Step 2: Double the last digit and subtract from the remaining number, call the result n_1*:*

$$n_1 = \frac{(n-d)}{10} - 2 \cdot d.$$

Then n *is divisible by* 7 *if and only if* n_1 *is divisible by* 7.

If after using this test once, you still get a number $n_1 > 70$, you can repeat the test and get some number n_2.

EXERCISE 7. *In 2019, a 12-year old Nigerian boy, Chika Ofili, suggested an alternative test for being divisible by* 7. *Read the news article about Chika's test:* https://www.scilynk.in/divisibility-of-7/. *In this test, instead of subtracting* $2d$*, Chika suggests to add* $5d$*. What do you think about these two conclusions of the article?*

- *"Multiplying by* 5 *helps to reach a number within* 0–70 *at a faster rate compared to multiplication by* 2*."*

- *"Adding two numbers is psychologically simpler than subtraction."*

Test these conclusions on some numbers, e.g. 2021, 1234567: count the number of times you apply each test, and try to observe what is easier for you psychologically.

5. Prime numbers

When we factor numbers into smaller numbers, at some point we will have to stop, because there are some natural numbers that cannot be factored as the product of two smaller natural numbers. Trivially, zero and one are among them, but also there are 2, 3, 5, 7, 2017 and 2027.

I would like to argue that zero and one are so special that we don't even call them "prime". Most early Greeks did not even consider 1 to be a number, so they could not consider its primality. In modern mathematics, we actually have a formal definition that excludes 0 and 1 as prime numbers.

DEFINITION 5.1. A natural number p is called prime if it has exactly two positive distinct divisors.

With this definition, we can observe that 0 and 1 are not prime, because 0 is divisible by any number, while 1 is divisible by only one number – 1 itself.

THEOREM 5.2 (Fundamental theorem of arithmetic). *Every natural number $n > 1$ is either a prime or it can be expressed as a product of prime numbers in a unique way.*

SKETCH OF PROOF. We will not prove this theorem because it requires a technique called induction, which we have not yet covered.

However, you should be able to see that the existence of such expression is simply a matter of definition. If a number cannot be factored into products of smaller number, by definition, it is a prime number. Keep factoring the smaller number in the products until you get all primes.

The uniqueness part is the tricky part! □

REMARK 5.3. An important idea here is that in mathematics, a proof of unique existence of something is often done by two separate steps that are not in any order. Existence step is to establish that there is at least one object that satisfies the definition. Uniqueness step is to establish that if two objects with the same definition exist, they must be the same.

EXAMPLE 5.4. We can first try and factor 2021. Let's see which prime numbers, starting from the smallest, can divide it: not 2, 3, 5, 7... Eventually, we see that

$$2021 = 43 \cdot 47.$$

Now let us do the same with 2020. It is divisible by 2, because its last digit is divisible by 2:

$$2020 = 2 \cdot 1010 = 2^2 \cdot 505 = 2^2 \cdot 5 \cdot 101.$$

While doing prime decomposition and testing which numbers are prime, you can observe that if n is a natural number that is not divisible by any number up to $\sqrt{n}$, then n is prime.

Sieve method for finding prime numbers.

THEOREM 5.5. *There are infinitely many prime numbers.*

PROOF. We prove this statement by proof by contradiction.

Suppose that there are only finitely many primes, listing them as[3]

$$p_1 < p_2 < \cdots < p_n \,.$$

Then we claim that the number

$$a = p_1 p_2 \dots p_n + 1$$

is a prime number, which is larger than the largest prime number p_n, a contradiction. To see that a is a prime number, we suppose that it is not a prime number, then it must be uniquely factorizable by the primes from $\{p_1, \dots, p_n\}$. In particular

$$a = p_{l_1}^{m_1} \cdot \dots \cdot p_{l_k}^{m_k} \,.$$

But then we have

$$1 = p_{l_1} \cdot \dots \cdot p_{l_k} (p_{l_1}^{m_1 - 1} \cdot \dots \cdot p_{l_k - 1}^{m_k - 1} - q) \,,$$

where q is some natural number. This is a contradiction because that means both

$$p_{l_1} \cdot \dots \cdot p_{l_k}$$

and

$$(p_{l_1}^{m_1 - 1} \cdot \dots \cdot p_{l_k - 1}^{m_k - 1} - q)$$

must be 1 or (-1). This is impossible as at least $p_{l_1} \cdot \dots \cdot p_{l_k} > 1$ by definition of primes. □

[3]Note that it is necessary for a finite list of number to have a largest number and a smallest number. In this case, the largest number in our prime list is p_n.

REMARK 5.6. The proof above is by Euclid in 300 B.C.. A remarkable feat!

EXERCISE 8. *Infinity is lurking behind us already. You should start asking yourself what infinity really is and try to come up with a definition on your own.*

6. Greatest common divisor

One of the most fundamental concepts about numbers is the greatest common divisor.

DEFINITION 6.1. Let $a, b \in \mathbb{Z}$. An integer d is a greatest common divisor of a and b if:

(1) $d \mid a$ and $d \mid b$,
(2) if q is another integer such that $q \mid a$ and $q \mid b$ then $q \mid d$.

We denote the (unique) non-negative greatest common divisor of a and b as $\gcd(a, b)$.

EXERCISE 9. *Why is it that in our definition, we have "a" greatest commond divisor, but not "the" greatest common divisor?*

THEOREM 6.2. *Let $a, b, q, r \in \mathbb{Z}$ and suppose that $a = qb + r$. Then*

$$\gcd(a, b) = \gcd(b, r)\,.$$

PROOF. First, note that any number c that divides both a and b also divides r. To see this, we can write $a = m_1 c$ and $b = m_2 c$. Therefore,

$$m_1 c = q m_2 c + r\,,$$

which is equivalent to

$$r = c(m_1 - q m_2)\,.$$

By definition, c is a divisor of r.

Second, if d divides both b and r then d divides a. To see this, we write $b = m_3 d$ and $r = m_4 d$. Therefore,

$$a = q m_3 d + m_4 d = (q m_3 + m_4 m) d\,.$$

By those two observations, and definition of greatest common divisor,

$$\gcd(a, b) \leqslant \gcd(b, r) \quad \text{and} \quad \gcd(a, b) \geqslant \gcd(b, r)\,.$$

This means that

$$\gcd(a, b) = \gcd(b, r)\,,$$

as desired. □

One question arise, how can we find the greatest common divisor of any two numbers? For example, how on earth are we supposed to know $\gcd(199888, 4987774)$? Luckily, ancient people were pretty smart and there is a method that was invented at least 2300 years ago as it first appeared in Euclid's Elements (300 BC). We, as modern people, still benefit from this method as it has a lot of practical applications [4].

THEOREM 6.3 (Euclid's algorithm). *Let $a, b \in \mathbb{Z}$. The $\gcd(a, b)$ is computed as follows.*

- *Set r_1 to be the remainder of a divided by b .*
- *Set r_2 to be the remainder of b divided by r_2.*
- *Given r_{n-2} and r_{n-1}, define r_n to be the remainder of r_{n-2} divided by r_{n-1}.*
- *Stop when $r_{n+1} = 0$; then $r_n = gcd(a, b)$.*

Writing everything explicitly, we have

$$\begin{aligned} a &= bq_1 + r_1 \qquad (0 < r_1 < b) \\ b &= r_1 q_2 + r_2 \qquad (0 < r_2 < r_1) \\ r_1 &= r_2 q_3 + r_3 \qquad (0 < r_3 < r_2) \\ &\dots \\ r_{n-2} &= r_{n-1} q_n + r_n \qquad (0 < r_n < r_{n-1}) \\ r_{n-1} &= r_n q_{n+1} + 0\,. \end{aligned}$$

Then $\gcd(a, b) = r_n$.

EXERCISE 10. *Why must there is a 0 remainder at the end of Euclid's algorithm? This is an important question because it answer the following question, "why should the algorithm stop?" Is there a scenario when you have to do this forever?*

EXAMPLE 6.4. Use Euclid's algorithm to find

$$\gcd(242, 66)\,.$$

Let's compute!

$$\begin{aligned} 242 &= 66 \cdot 3 + 44 \\ 66 &= 44 \cdot 1 + 22 \end{aligned}$$

[4] For a curious mind, you can read more about it here: https://en.wikipedia.org/wiki/Euclidean_algorithm

$$44 = 22 \cdot 1 + 0\,.$$

So $\gcd(242, 66) = 22$.

Let's have some fun with greatest common divisors using Euclid's algorithm.

COROLLARY 6.5. *Let $l = \gcd(a, b)$. Then there exist two integers m, n such that*

$$l = am + bn\,.$$

PROOF. We apply Euclid's algorithm to prove this statement. Writing everything explicitly, we have

$$\begin{aligned}
a &= bq_1 + r_1 && (0 < r_1 < b)\\
b &= r_1 q_2 + r_2 && (0 < r_2 < r_1)\\
r_1 &= r_2 q_3 + r_3 && (0 < r_3 < r_2)\\
&\dots\\
r_{n-2} &= r_{n-1} q_n + r_n && (0 < r_n < r_{n-1})\\
r_{n-1} &= r_n q_{n+1} + 0\,.
\end{aligned}$$

We know that, $l = r_n$ because that is the content of Euclid's algorithm.

Now, to show what we want to show, we reverse engineer what's happening. Rewriting

$$r_1 = a - bq_1\,.$$

Then,

$$r_2 = b - r_1 q_2 = b - (a + bq_1)q_2 = (1 - q_1 q_2)b - q_2 a\,.$$

Keep doing this until r_n and we will arrive at our conclusion. □

CHAPTER 2

Logic

At its core, mathematics is a way of reasoning and is very similar to philosphy. The first part of this chapter wil reflect this basic observation. However, what sets apart mathematics from general philosophy is that the language of mathematics requires precision. There should be no ambiguity in a mathematical statement. The main goal of this chapter is to give the students a taste of what it is like to be mathematically precise.

1. What can logic be about?

We follow [Sai] for this part.

Most broadly, logic is about reasons and reasoning. There are reasons for *acting*: you may avoid sugary desserts for the reason of wanting to keep thin or lose weight. There are reasons for *believing*: you may think that the potatoes are ready to eat for the reason that they have been boiling for twenty minutes. Historically, logic has concerned itself with reasons for believing. But even this question can be answered in various ways. For example, I asked an Indian friend of mine why she believes that she should not eat meat. Her answer was that this belief was instilled in her by her family at an early age. This explains the origin of this belief, but does not give a reason for it. But then she continued her answer and said that now she doesn't like the smell of meat, and eating food that smells bad is usually a bad idea. This also justifies her belief. Some other people may say that killing anything is wrong, and eating meat requires killing, thus reasoning why they shouldn't eat meat.

The way it works is that one deduces the reasons for a certain belief by making it a consequence of a "higher", more abstract, belief. Logic as a discipline of "good reasoning" was first considered as early as the 6th century B.C. and independently in India, Greek and China.

Example 1.1. Consider the following chain of sentences.

"I believe that humans breath oxygen to live. I believe that I am a human. Therefore, I believe that I breath oxygen to live."

"All humans breath oxygen" is a higher, more abstract, fact than " I breath oxygen", as I am just a particular member of the human race.

WARNING 1.2. *Not every belief has its reasons. Every logical system has its core "beliefs" (called axioms) that are taken for granted, and they have no further explanation. These are the most abstract beliefs that are used to deduce every other belief in the same logical system. To have reasons, one needs to take a leap of faith at some point.*

Logic is a normative discipline. It sets out standard for good and bad arguments. These are technical terms and should not be confused by subjective opinions. However, the these technical terms are somewhat inspired by daily commonsense distinction between good and bad reasons. In our daily conversation, to make good reasons for something is to create premises so that the something follows.

EXAMPLE 1.3. "James is a banker and all bankers are rich" is a good reason for "James is rich."

QUESTION. *If James is not a banker, can we conclude that he is not rich?*

EXAMPLE 1.4. "James likes expensive cars" is not a good reason for "James is rich."

It is important to note that one can discern good and bad reasons without having to believe in the reasons themselves. In fact, Einstein himself did not believe in (even reject) quantum physics while being one of the founding fathers of the theory. A lot of modern mathematics revolves around physics and biology but a lot of mathematicians barely know any physics or biology (confession time).

1.1. Inductive and deductive logic. The result of assembling premises and conclusions together is called an argument. An argument is valid, or true, or good, if the conclusions follow from the premises. The two most common forms of logic are inductive logic and deductive logic.

An example of inductive logic is the following.

EXAMPLE 1.5. The sun has risen every morning so far; therefore it (probably) will rise tomorrow.

EXERCISE 11. *Contrast the previous example with the following sentence:*

" The sun has risen every morning so far; therefore it (probably) will NOT rise tomorrow."

Is one of these sentences more true than the other? How do you know?

An example of deductive logic is the following.

EXAMPLE 1.6. All men are mortal. Socrates is a man. Therefore, Socrates is mortal.

Thus, a way to distinguish between inductive and deductive logic is: for deductive logic, it is impossible for the conclusion to be false if the premises are true. For inductive logic, this is not the case as the conclusion in this case may be false despite the premises being true. We can see that it is only in deductive logic, one can talk about the validity of an argument. In inductive logic, there are degrees in strength of an argument but inductive reasoning can never be valid by our definition of validity[1]. However, an inductive argument can be stronger than another inductive argument (just make sure one is talking about the same thing – comparing apples to apples and not to pears).

Mathematics is all about deductive logic whereas science must involve both inductive and deductive logic. The combination of inductive and deductive logic in science gives birth to the need of probability and statistics (whose theories are all mathematical and deductive), and in modern day data science and machine learning that are based on statistics.

WARNING 1.7. *Do not confuse inductive logic with the method of induction, which is a method in deductive logic. Although, there are resemblance between the two. The difference is that in the method of induction, one is given the super power in theory to transcend time to "go off to infinity" whereas inductive logic is limited by physical evidence, where time is a major road block...*

EXERCISE 12. *Make a table of comparison between inductive and deductive logic.*

Watch this lecture about inductive logic: https://youtu.be/DRx-3jvC918.

EXERCISE 13. *What's wrong with the following?*
Statement: You have horns.

[1]Be careful here that validity is a technical term and should not be confused with the daily use of the word

"Proof": What you haven't lost, you have. You haven't lost your horns. Therefore you have horns.

EXERCISE 14. *What's wrong with the following?*
Statement: You don't know your father.
"Proof": I show you a photo of someone, the photo is covered by a cloth. Do you know who's in the photo? You can't see, so you don't. But it's a photo of your father. Therefore you don't know your father.

2. Mathematical logic

We follow [New] for this part.

Mathematical logic is the study of logic restricted to mathematics. Its existence is to address the biggest problem in the foundation of mathematics: are theories of mathematics consistent with each others? That said, many working mathematicians do not pay attention to the question of foundations, which might be a worrisome fact. I can only have my fingers crossed that mathematics will not fall apart one day (which, it did for a period of time, when Georg Cantor discovered different infinities in the 19th century)...

A **mathematical statement** is a statement that at least the statement maker has to be able to assign a **truth value** ('true' or 'false') to it. The truth assignment could be the result of an immediate observation or a long chain of difficult reasoning. To make the truth assignment valid, every single argument in the chain of reasoning must be valid. A **proof** of a mathematical statement is a chain of valid arguments that make the mathematical statement true.

There are many names for a true mathematical statement, depending on the use:

- **Theorem:** a particularly important mathematical statement given the context.
- **Proposition:** general term that can be used anytime.
- **Lemma:** a mathematical statement that will be used as a stepping stone to prove a theorem.
- **Corollary:** a mathematical statement whose truth value could be deduced from a theorem without much effort.

A statement that are believed to be verifiable but no human has seen or discovered its proof yet is called a **conjecture**.

2.1. Structure. Every mathematical statement has the following structure:

Assumptions + Goals

EXAMPLE 2.1. Suppose Philadelphia is in Massachusetts and Penn is in Philadelphia, then Penn is in Massachusetts.

WARNING 2.2. *Assumptions themselves need not to be true. We will talk more about this later when we talk about truth table.*

EXERCISE 15. *Find an example of a famous mathematical statement that its assumptions are not yet verified.*

EXAMPLE 2.3. For example, abc conjecture implies Fermat's last theorem. But as of now, the status of the abc conjecture is subject to debate. A Fields medalist Peter Scholze and Jakob Stix found a gap in Mochizuki's proof.

Now a quote from Wikipedia: "Scholze and Stix wrote a report asserting and explaining an error in the logic of the proof and claiming that the resulting gap was "so severe that ... small modifications will not rescue the proof strategy"; Mochizuki claimed that they misunderstood vital aspects of the theory and made invalid simplifications.

On April 3, 2020, two Japanese mathematicians announced that Mochizuki's claimed proof would be published in Publications of the Research Institute for Mathematical Sciences (RIMS), a journal of which Mochizuki is chief editor. In March 2021, Mochizuki's proof was published in RIMS."

We will end this section by discussing a few logical axioms that look obvious but people use all the time in mathematics without realizing it.

3. Symbolic logic

One of the main goals of mathematics is to reduce complicated statements/observations to simple abstract structures that are more tractable to human minds and still keep the essential features of the things one would like to study. This is as much of an art as anything else because too much abstraction would lead to triviality, which may not be very interesting.

Symbolic logic is a system of logic that can be used to reduce a mathematical statement into "agreed" formulas that are easier to determine its truth value.[2]

[2]Gottfried Leibniz (another inventor of Calculus) was among the first people to realize the importance of having a system of logic that is universal and calculatable but couldn't

Let us consider a simple example from [New]:

EXAMPLE 3.1. If c divides b and b divides a, then c divides a.

We see that each of the statements "c divides b", "b divides a", and "c divides a" is a proposition if they stand alone by themselves. Thus, abstractly, each of them could be assigned a symbol

- $P = c$ divides b
- $Q = b$ divides a
- $R = c$ divides a

Then you can write

$$\text{If } P \text{ and } Q, \text{ then } R.$$

The above form of the statement looks easier to follow (at least to the mind of a non-English speaker) since at least we don't need to know what "divides" means. While it is not too useful in terms of conveying knowledge, it is extremely useful when it comes to determining the validity of the statement itself. This leads us to the next question: What makes a statement true?

We will need a few new words.

DEFINITION 3.2. A **propositional variable** is a symbol that represents a proposition.

As we said earlier, propositions are just mathematical statements, which are required to have truth values ('true' or 'false').

DEFINITION 3.3. A **logical operator** is a symbol (or collection of words) that turn one or more propositional variables to a single new statement.

Basic logical operators are:

- Conjuction ('and', $\wedge$)
- Disjunction ('or', $\vee$)
- Implication ('if...then...', $\implies$)
- Negation ('not', $\neg$)

As simple as they look, these four operators build most of mathematics and anything that require reasoning (philosophy, law, computer science, etc.).

actualize this dream. The goal was to reduce confusions and disputes among philosophers and arguers. (Just turn on the Presidential debates and you will understand why we need such a system...) The first well-known work that successfully made symbolic logic a mathematical field was by George Boole in 1854 [Boo]. One of the earliest work that started the modern account of logic and foundation of mathematics was by Russel and Whitehead [WR] (there is a comic book about it [DP]!).

DEFINITION 3.4. A **propositional formula** is an expression that is either a propositional variable, or is built up from simpler propositional formulae using logical operators.

REMARK 3.5. When I ask, "What is the variable for the proposition?", I am more interested in what the symbol you give to the mathematical statement, not so much the content of it. Similarly, when I ask, "What is the formula for the proposition?" I am more interested in the way the proposition is written up, not so much what the proposition conveys.

The simplest kind of propositions is one that only contains one single propositional variable that already explicitly has the truth value ('true' or 'false') known (whether it is a proven statement, ~~a common knowledge~~ or an assumption). From these atomic propositions, we could build more complicated kinds of propositions with more complicated propositional formula by obeying certain logical rules of the logical operators[3]. This process is entirely "calculatable". Here are the rules for the basic logical operators listed above.

Conjunction ('and', $\wedge$). The propositional formula for a proposition made by a conjuction has the following form

$$P \wedge Q\,.$$

RULE. *The proposition $P \wedge Q$ (we say "P and Q") is true if* **both** *P and Q are true. Otherwise, if either (or both) P or Q is false, $P \wedge Q$ is false.*

Disjunction ('or', $\vee$). The propositional formula for a proposition made by a disjunction has the following form

$$P \vee Q\,.$$

RULE. *The proposition $P \vee Q$ (we say "P or Q") is true if* **either one** *(or both) of P or Q is true. $P \vee Q$ is flase if* **both** *P and Q are false.*

Implication ('if...then...', $\implies$). The propositional formula for a proposition made by a disjunction has the following form

$$P \implies Q\,.$$

RULE. *The proposition $P \implies Q$ (we say "P implies Q") is true if one of the following cases holds:*

[3]Even though we call them rules, they follow an intuitive model of our daily reasoning. The advantage of defining explicit rules is to make the reasoning more consistent by the abstraction.

- *P is true and Q is true.*
- *P is false.*

EXERCISE 16. *This is one of the most confusing rules in logic. Meditate on the rule of implication.*

Negation ('not', $\neg$). The propositional formula for a proposition made by a disjunction has the following form

$$\neg P\,.$$

RULE. *The proposition $\neg P$ (we say "not P") is true if P is false.*

EXERCISE 17. *Mess with your friends/parents/siblings with 'and', 'or', 'if not ... then...'*

AXIOM 1 (Law of excluded middle). Let P be a propositional formula. Then $P \vee (\neg P)$ is true. In plain English, this says that every proposition is either true or false.

AXIOM 2 (Principle of explosion). If a contradiction is assumed, any consequence may be derived.

4. Variables and quantifiers

4.1. Variables. It is nice to know basic rules of logic and how propositions work in sequences in order to produce proofs (arguments). It is unfortunate, however, that if we only work with propositions, our reasoning would be fairly limited. Consider the following sentence:

"x is divisible by 7."

QUESTION. *Is this a proposition?*

ANSWER. This is not a proposition as one cannot assign a truth value to it– we don't know what x is. □

If we know a specific value of x, we would be able to determine the truth value of the sentence above and it would become a proper proposition. For example, if $x = 49$, the sentence would be true and if $x = 42$, it would be false. If we suppose that x should belong the set of natural number, $\mathbb{N}$, then The symbol x is called a free variable the set $\mathbb{N}$.

DEFINITION 4.1. Let x be a variable that is understood to refer to an element of a set X. In a statement involving x, we say it is free if it makes

sense to substitute particular elements of X in the sentence; otherwise we say x is bound.

So if the sentence in the above question is not a proposition, what do we call it? Glad you ask– statements like those, which depend on free variables (hence abstract the notion of proposition) are called predicate. More formally, we have the following definition.

DEFINITION 4.2. A predicate is a symbol P with a specified list of free variables $x_1, x_2, \ldots, x_n$ and, for each variable x_i, a specification of a set X_i (called the domain of disclosure of x_i).

Notation: we will typically write $P(x_1, \ldots, x_n)$ in order to make the variable explicit.

EXAMPLE 4.3. We can represent the sentence 'x is divisible by 7' by $P(x)$, where $x \in \mathbb{N}$. $P(49)$ is true and $P(10)$ is false.

EXAMPLE 4.4. The sentence "there exist integers a, b such that $x = a^2+b^2$" has free variable x and bound variables $a^2 + b^2$, and can be represented by a predicate $R(x)$, where the domain of disclosure can be chosen to be $\mathbb{Z}$.

REMARK 4.5. A predicate with no free variables is precisely a propositional variable.

EXERCISE 18. *How would you represent the sentence "$x - y$ is rational" as a predicate.*

EXERCISE 19. *How would you represent the sentence "every even natural number $n \geqslant 2$ is divisible by k"?*

4.2. Quantifiers. Looking back to Example 4.4 and Exercise 19, we notice that the bound variables come with either "there exist" or "every". Without those terms, those variables will be come free variables.

Expressions that refer to how many elements of a set make a statement true, such as "there exists" and "every" turn free variables into bound variables. We represent such expression using symbols called quantifiers.

In mathematics, there are two universal quantifiers, $\forall$ (every) and $\exists$ (there exists).

EXAMPLE 4.6. intuitively speaking,

- The expression "$\exists x \in X$" denotes "there exists $x \in X$".
- The expression "$\forall x \in X$" denotes "for every $x \in X$".

Just like we can build propositional formulae from propositions and logical operators, we can build something out of predicates and logical operators.

DEFINITION 4.7 (**Logical formula**). A logical formula is an expression that is built from predicates using logical operators and quantifiers; it may have both free and boundary variables. The truth value of a logical formula depends on the free variables according to the rules for logical operators and quantifiers.

It is an important skill to translate from human languages into purely symbolic logical formulae and vice versa.

Formally, we have the following definitions of quantifiers.

DEFINITION 4.8 (**The universal quantifier $\forall$**). If $p(x)$ is a logical formula with free variable with free variable x with domain X, then $\forall x \in X, p(x)$ is the logical formula defined according to the following rules:

- If $p(x)$ can be derrived from the assumption that x is an arbitrary element of X, then $\forall x \in X, p(x)$;
- If $a \in X$ and $\forall x \in X, p(x)$ is true, then $p(a)$ is true.

DEFINITION 4.9 (**The universal quantifier $\exists$**). If $p(x)$ is a logical formula with free variable x with domain X, then $\exists x \in X, p(x)$ is the logical formula defined according to the following rules:

- If $a \in X$ and $p(a)$ is true, then $\exists x \in X, p(x)$;
- If $\exists x \in X, p(x)$ is true, and q can be derived from the assumption that $p(a)$ is true for some fixed $a \in X$, then q is true.

There are more quantifiers out there in the wild world of mathematics but they depend on specific fields of study. The above two quantifiers are used in every field of mathemtics, however.

One can combine quantifiers in a logical formula and the order of the quantifiers matter.

EXERCISE 20. *Translate the following expressions and convince yourself that they are different.*

(1) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, \exists z \in \mathbb{Z}, x = y^2 + z^2$.
(2) $\exists y \in \mathbb{Z}, \exists z \in \mathbb{Z}, \forall x \in \mathbb{Z}, x = y^2 + z^2$.
(3) $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, \exists z \in \mathbb{Z}, x = y^2 + z^2$.

Are those propositions?

Are the following statements different?

(1) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, \exists z \in \mathbb{Z}, x = y^2 + z^2$.
(2) $\forall x \in \mathbb{Z}, \exists z \in \mathbb{Z}, \exists y \in \mathbb{Z}, x = y^2 + z^2$.

4.3. Logical equivalence. We start out with a question

QUESTION. *Let P be the set of all prime numbers. Are these two logical formulae the same?*

(1) $\forall n \in P, (n > 2 \implies (\exists k \in \mathbb{Z}, n = 2k + 1))$.
(2) $\neg \exists n \in P, (n > 2 \wedge (\exists k \in \mathbb{Z}, n = 2k))$.

In plain English, the two logical formulae read as follows.

(1) Every prime number greater than two is odd.
(2) There does not exists an even prime number greater than two.

Because of the way they are framed, one would go on to prove these statements by using two completely different techniques.

(1) Fix a prime number n, assume that $n > 2$, and then prove that $n = 2k + 1$ for some $k \in \mathbb{Z}$.
(2) Assume that there is some prime number n such that $n > 2$ and $n = 2k$ for some $k \in \mathbb{Z}$ and derive a contradiction.

QUESTION. *Which strategy is easier to follow/prove?*

One can see that knowing more ways to rephrase a statement gives us more ways to prove/disprove it. The notion of logical equivalence tells us exactly when two statements have the same logical meaning, hence gives us confidence to think about one statement in the form of a different statement without worrying about being led astray by irrelevant thoughts and discover later that all the work we have done was in vain (even though this happens all the time).

DEFINITION 4.10. Let P and Q be logical formulae. We say that P and Q are logically equivalent and write $P \equiv Q$ if Q can be derived from P and P can be derived from Q.

EXAMPLE 4.11. We claim that

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R),$$

where P, Q, R are propositional variables.

PROOF. First, assume that $P \wedge (Q \vee R)$ is true. Then P is true and $Q \vee R$ is true by definition of conjunction. By definition of disjunction, either Q is true or R is true. So, we divide our reasoning into two cases:

- If Q is true, then $P \wedge Q$ is true by definition of conjunction.
- If R is true, then $P \wedge R$ is true by definition of conjunction.

In both cases, we have that $(P \wedge Q) \vee (P \wedge R)$ is true by definition of disjunction.

Second, assume that $(P \wedge Q) \vee (P \wedge R)$ is true. Then, either $P \wedge Q$ is true or $P \wedge R$ is true by definition of disjunction. Again, we divide our reasoning into two cases:

- If $P \wedge Q$ is true, then P is true and Q is true by definition of conjunction.
- If $P \wedge R$ is true, then P is true and R is true by definition of conjunction.

In both cases, we have P is true and $Q \vee R$ is true by definition of disjunction. Therefore, $P \wedge (Q \vee R)$ is true.

Thus, we have derived that $(P \wedge Q) \vee (P \wedge R)$ is true from $P \wedge (Q \vee R)$ being true and vice versa. This proves our claim by definition of logical equivalence. □

Now we turn to everyone's favorite tool, the truth table.

4.4. Truth table.

Definition 4.12. The truth table of a propositional formula is the table with one row for each possible assignment of truth values to its constituent propositional variables, and one column for each sub-formula (incluidng the propositional variables and the propositional formula itself). The entries of the truth table are the truth values of the sub-formulae.

There are many ways that one could employ to prove the logical equivalences of propositional formulae. The most fundamental way is to use the definition. Another way that is one of the all-time favorites is to use the truth table: in order to prove that propositional formulae are logically equivalent, it suffices to show that they have identical columns in a truth table.

Example 4.13. We will prove the what's claimed in Example 4.11 using the truth table.

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$Q \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

EXAMPLE 4.14. Use the truth table to show that

$$P \implies Q \equiv (\neg P) \vee Q\,.$$

THEOREM 4.15 (De Morgan's laws for logical operators). *Let P, Q be propositional variables. Then,*

(1) $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$,
(2) $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$.

THEOREM 4.16 (De Morgan's laws for quantifiers). *Let $P(x)$ be a logical predicate and X be a set. Then,*

(1) $\neg(\forall x \in X, P(x)) \equiv \exists x \in X, \neg P(x)$,
(2) $\neg(\exists x \in X, P(x)) \equiv \forall x \in X, \neg P(x)$.

CHAPTER 3

Sets and functions

1. Sets

The notion of a set is extremely fundamental (as we already used it in previous discussions) yet, if not defined carefully, could lead to paradoxes and break mathematics from its core. Perhaps the most infamous paradox in naive set theory is the so-call Russell's paradox. However, for the sake of sanity in this course, let's stick with the naive notion and trust that mathematicians already fixed this issue and unbroke mathematics...

DEFINITION 1.1. A set is a collection of objects. The objects in the sets are called elements of the set. If x is an element in the set X then we write $x \in X$. We write $x \notin X$ to mean $\neg(x \in X)$.

The way that Bertrand Russell broke naive set theory is via the following chain of reasoning, taken directly from Wikipedia:

> Let R be the set of all sets that are not members of themselves. If R is not a member of itself, then its definition entails that it is a member of itself; if it is a member of itself, then it is not a member of itself, since it is the set of all sets that are not members of themselves.

We will need to use the so-called set-builder notation to describe sets in general. Given a set X, set set of elements of X satisfying some property $P(x)$ is denoted by

$$\{x \in X \mid P(x)\}.$$

From now on, we define the set of all rationals to be

$$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{Z} \text{ and } q \neq 0\},$$

and the set of real numbers to be

$$\mathbb{R} = \{\text{rationals and irrational numbers}\}.$$

We are cheating in the definition of real numbers above but that is too technical for the moment. Let's just go with what you imagine it to be from

high school. We will also use the usual open and closed set notations.

$$[a,b] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\},$$
$$[a,b) = \{x \in \mathbb{R} \mid a \leqslant x < b\},$$
$$(a,b] = \{x \in \mathbb{R} \mid a < x \leqslant b\},$$
$$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}.$$

See Newstead [New] (Chapter 2) for representations of intervals on the number line.

DEFINITION 1.2. Let X be a set. A subset of X is a set U such that

$$\forall a, (a \in U \implies a \in X).$$

We write $U \subseteq X$ for the assertion that U is a subset of X. The notation $\subsetneq$ means that U is a proper subset of X, that is a subset of X that is not equal to X.

In order to prove that U is a subset of X, it is sufficient to take an arbitrary element $a \in U$ and prove that $a \in X$.

EXAMPLE 1.3. Prove that $\mathbb{Z} \subset \mathbb{Q}$.

We want to be able to say when two sets are the same (equal) with each other. There are different ways to go about this. One can say that two sets are equal if they have the exact same definition or there definition are somehow logically equivalent to each other. In real practice, these are not very useful. However, there are those who believe that "we are what we are made of." This sounds like a reasonable description and is a criteria to distinguish two different people. Surely, even though our bodies might be made of atoms but my atoms are different than your atoms. This inspires the following axiom about set equality.

AXIOM 3 (Axiom of extentionality). Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.

EXAMPLE 1.4. Prove that,

$$\{x \in \mathbb{R} \mid x^2 \leqslant 1\} = [-1,1].$$

One question may arise when we define intevals. Consider, (a,b), for example. Some people might object this definition because if $a > b$ we have a contradiction

$$b < a < x < b.$$

How can this be? A careful look at this definition, we realized that it says, if $x \in \mathbb{R}$ and $a < x < b$, then we admit x into the set. If the description itself does not make sense, we can't even start to consider anything, let alone the admission. When this situation, the set (a, b) simply does not contain any element, and we call that an empty set.

DEFINITION 1.5. A set is non-empty if it contains at least one element. Otherwise, it is empty.

QUESTION. *How many empty sets are there?*

ANSWER. There is only one empty set. That is if E' and E are both empty set, then

$$E' = E\,.$$

To see this, we want to show $E \subseteq E'$ and $E' \subseteq E$ (axiom of extentionality). By definition, Let a be an element in the universe that E belongs to. $a \in E$ is always false because E is empty. Therefore, the statement

$$a \in E \implies a \in E'$$

is always true. By definition of subsets, $E \subseteq E'$. Likewise, $E' \subseteq E$, showing our claim. □

1.1. Set operations. We will introduce some basic operations on sets. There are many more but the interested reader could find them in fuller details in Newstead's book.

DEFINITION 1.6 (Pairwise intersection). Let X and Y be sets. The pairwise intersection of X and Y, denoted $X \cap Y$ is defined by

$$X \cap Y \stackrel{\text{def}}{=} \{a \mid a \in X \wedge a \in Y\}\,.$$

EXAMPLE 1.7. Let $X = \{1, 2, 3, 4\}$ and $Y = \{2, 4, 7\}$, then

$$X \cap Y = \{2, 4\}\,.$$

DEFINITION 1.8 (Pairwise union). Let X and Y be sets. The pairwise union of X and Y, denoted $X \cup Y$ is defined by

$$X \cup Y \stackrel{\text{def}}{=} \{a \mid a \in X \vee a \in Y\}\,.$$

EXAMPLE 1.9. Let $X = \{1, 2, 3, 4\}$ and $Y = \{2, 4, 7\}$, then

$$X \cup Y = \{1, 2, 3, 4, 7\}\,.$$

DEFINITION 1.10 (Relative complement). Let X and Y be sets. The relative complement of Y and X, denoted $Y \setminus X$ is defined by

$$Y \setminus X \stackrel{\text{def}}{=} \{a \mid a \in Y \wedge a \notin X\}.$$

EXAMPLE 1.11. Let $X = \{1, 2, 3, 4\}$ and $Y = \{2, 4, 7\}$, then

$$Y \setminus X = \{7\},$$
$$X \setminus Y = \{1, 3\}.$$

1.2. Venn diagram. For this part, please refer to in-class lecture.

You can prove the following using Venn diagram.

THEOREM 1.12 (de Morgan's laws for sets). *Let X, Y, Z be sets. We have*

(1) $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$,
(2) $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$.

DEFINITION 1.13 (Ordered pair). For any two objects, x and y, an ordered pair (x, y) is the notation for the two objects being arranged in that particular order.

Thus, $(x, y) \neq (y, x)$ unless $x = y$.

DEFINITION 1.14 (Cartesian product). Let X and Y be sets. The Cartesian product of X and Y, denoted by $X \times Y$ is the set of all ordered pairs (x, y) such that $x \in X$ and $y \in Y$. In set-builder notation

$$X \times Y \stackrel{\text{def}}{=} \{(x, y) \mid x \in X, y \in Y\}.$$

2. Functions

We all talk about functions. So much in math classes that we almost think they are synonyms. Believe it or not, they are not synonyms and a function has its own definition.

DEFINITION 2.1 (Function). A function f from a set X to a set Y is a specification of elements $f(x) \in Y$ for $x \in X$, such that

$$\forall x \in X, \exists! y \in Y, y = f(x).$$

The symbol $\exists!$ represents the phrase"there exists a unique". The unique element $f(x) \in Y$ is called the value of f at $x \in X$.

X is called the domain of f and Y is called the codomain of f.

We next discuss how to specify a function so that it satisfies the above definition.

(1) Totality. A value $f(x)$ should be specified for each $x \in X$ – this corresponds to the quantifier $\forall x$.
(2) Existence. For each X, the specified value $f(x)$ should exists, and should be an element in Y.
(3) Uniqueness. For each x the specified value $f(x)$ should refer to only one element in Y.

(2) and (3) correspond to the quantifier $\exists! y$.

Example 2.2. The following are functions:

(1) $f : X \to X$, where $f(x) = x$ for any set X. This function is called the identity function.
(2) $f : \emptyset \to X$ is called the empty function. It has no values since there is no element in its domain.
(3) $f : \{1, 2, 3\} \to \{\text{red, yellow, green, blue}\}$ where $f(1) = red$, $f(2) = blue$, $f(3) = blue$.
(4) $g : \mathbb{R} \to \mathbb{R}$, where $g(x) = 2x$.

The following are NOT functions:

(1) $f : \{1, 2, 3\} \to \{\text{red, yellow, green, blue}\}$ where $f(1) = red$, $f(3) = blue$.
(2) $g : \mathbb{R} \to \mathbb{R}$, where
$$g(x) = \frac{1}{x}\,.$$

Definition 2.3 (Graph of a function). Let $f : X \to Y$ be a functin. The graph of f is the subset $\mathrm{Gr}(f) \subseteq X \times Y$ defined by

$$\mathrm{Gr}(f) \stackrel{\text{def}}{=} \{(x, f(x)) \mid x \in X\} = \{(x, y) \in X \times Y \mid y = f(x)\}\,.$$

The graph of a function is perhaps the most important idea in modern mathematics as one can graphically draw functions on paper or turn graphs on papers into mathematical equations so that computations can be done. It is this idea that bridges geometry and calculus together. It is not an understatement to say science (and pseudo-science!) would not reach the its height today without this simple idea of Decartes.

Example 2.4. Graph of the function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x/2$ is

$$\mathrm{Gr}(f) = \left\{ \left(x, \frac{x}{2}\right) \,\middle|\, x \in \mathbb{R} \right\}.$$

Definition 2.5 (Composition of functions). Given two functions $f : X \to Y$ and $g : Y \to Z$. Their composite $g \circ f$ (read g composed with f) is

the function $g \circ f : X \to Z$, defined by

$$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X\,.$$

EXAMPLE 2.6. Let $f : [0,\infty) \to [0,\infty)$ be that $f(x) = x^3$ and $g : [0,\infty) \to [0,\infty)$ be that $g(x) = \frac{1}{1+x}$. Then, $f \circ g : [0,\infty) \to [0,1]$ is given by

$$(f \circ g)(x) = f(g(x)) = (g(x))^3 = \frac{1}{(1+x)^3}\,.$$

What happens if I keep the above formula and change $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \setminus \{-1\} \to [0,\infty)$?

EXAMPLE 2.7. We can write the function $M : \mathbb{Q} \to \mathbb{Q}$, $M(x) = \frac{(2x+5)^2}{6}$ as a composition as follows.

$$M = ((k \circ h) \circ g) \circ f\,,$$

where

- $f : \mathbb{Q} \to \mathbb{Q}$ is defined by $f(x) = 2x$,
- $g : \mathbb{Q} \to Q$ is defined by $g(x) = x + 5$,
- $h : \mathbb{Q} \to \mathbb{Q}$ is defined by $h(x) = x^2$,
- $k : \mathbb{Q} \to \mathbb{Q}$ is defined by $k(x) = \frac{x}{6}$.

2.1. Injections and surjections. The concepts of injections and surjections play very crucial roles in mathematics. Among other use, they are the tools for mathematicians to compare sizes of sets. It is with these concepts that one could talk about different sizes of infinities! We will just list definitions here, for a full reading, please read [New]. He does a fantastic job there discussing the concepts so there's no need to copy his text to here.

DEFINITION 2.8 (Injection). A function $f : X \to Y$ is injective (or one-to-one) if

$$\forall a \in X, \forall b \in X, f(a) = f(b) \Rightarrow a = b\,.$$

An injective function is said to be an injection.

EXAMPLE 2.9. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function that $f(n) = 2n + 1$. We will show that f is injective. Fix some $m, n \in \mathbb{Z}$ and suppose that $f(m) = f(n)$. By definition, we have

$$2m + 1 = 2n + 1 \iff m = n\,.$$

Therefore, f is injective.

EXAMPLE 2.10. Let $f : \mathbb{R} \to [0, \infty)$ be a function that $f(x) = x^2$. f is not injective since $f(-1) = f(1) = 1$, for example.

However, if we change the domain of f so that $f : [0, \infty) \to [0, \infty)$, it would be injective (why?).

PROPOSITION 2.11. *Let $f : X \to Y$ and $g : Y \to Z$ be functions. If f and g are injective, then $f \circ g$ is injective.*

PROOF. Let $a, b \in X$ and suppose that $(f \circ g)(a) = (f \circ g)(b)$. By definition of composition,

$$f(g(a)) = f(g(b)) .$$

Because f is injective, $g(a) = g(b)$; and because g is injective, $a = b$. Because a, b are arbitrary in X, $(f \circ g)$ is injective. □

DEFINITION 2.12 (Surjection). A function $f : X \to Y$ is surjective (or onto) if

$$\forall y \in Y, \exists x \in X, f(x) = y .$$

An surjective function is said to be an surjection.

EXAMPLE 2.13. Fix $n \in \mathbb{N}$ with $n > 0$ and define a function $r : \mathbb{Z} \to \{0, 1, \ldots, n-1\}$ by letting $r(a)$ be the remainder of a when divided by n. This function is surjective since for each $k \in \{0, 1, \ldots, n-1\}$, we have $r(k) = k$.

This function is not injective, however (why?).

DEFINITION 2.14 (Bijection). A function $f : X \to Y$ is bejective if it is both injective and surjective. A bijective function is called a bijection.

EXAMPLE 2.15. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function that $f(n) = n + 10$. Then f is a bijective.

When we change the domain of f so that $f : \mathbb{N} \to \mathbb{Z}$, it is no longer a bijective. Which fails – injectivity or surjectivity?

CHAPTER 4

Mathematical induction

Mathematical induction is a way to prove a sequence of statements by scaffolding. In a way, it can be compared to inductive logic, because in both cases we start by considering "small examples" and from those, we deduce that all of the examples have some property. However, there is an important distinction: mathematical induction is a part of deductive reasoning, because it provides a formal proof that yields correct statements, and does not just show that these statements are plausible. Here is the formal statement:

THEOREM 0.1 (The Induction Principle). *Suppose that we have a sequence of statements $P(n)$ labeled by the natural numbers $0, 1, 2, \ldots$ such that we know that*

(1) $P(0)$ is true, and

(2) $\big(P(0) \wedge P(1) \wedge \cdots \wedge P(n)\big) \Rightarrow P(n+1)$.

Then all the statements $P(0), P(1), P(2), \ldots$ are true.

1. All natural numbers are interesting

As a warm-up, let us prove that all natural numbers are interesting.

DEFINITION 1.1. A natural number n is called interesting if it has some special property that no other natural number has.

THEOREM 1.2. *All natural numbers are interesting.*

Let us first do a survey of the first few natural numbers:

- 0 is interesting because it is the only number that yields itself when you multiply it by another number.
- 1 is interesting because it is the only number that doesn't change the other number when multiplied.
- 2 is interesting because it is the first prime number, i.e. the number that has exactly two positive divisors (1 and itself).
- 3 is interesting because it is the first odd prime number.
- 4 is interesting because it is the first nontrivial square: $4 = 2^2$.

- 5...

We could say that 5 is a prime number, but it is not the first one of those. However, it is recognizable as a member of a certain sequence that is well-known to mathematicians and even in popular culture – Fibonacci sequence, which appears in Indian mathematics in connection with Sanskrit prosody (study of poetic metres and verse in Sanskrit).

EXERCISE 21. *Watch this really nice introduction to Fibonacci numbers in nature by Vi Hart (total duration of all combined is 18 minutes):*

Part 1: https://www.youtube.com/watch?v=ahXIMUkSXX0

Part 2: https://www.youtube.com/watch?v=lOIP_Z_-0Hs

Now create an angle 137.5°*, draw approximately* 30 *petals, each* 137.5° *from the previous one, and when you are done, mark the spirals and count the number of them.*

Part 3: https://www.youtube.com/watch?v=14-NdQwKz9w

After watching the third video, can you explain why we almost always get a Fibonacci number of spirals in plants?

And so we can continue finding interesting properties for numbers:

- 5 is the first Fibonacci number for which we didn't find another property.
- 6 is the first perfect number, which by definition means that it is the sum of its positive divisors excluding itself: $6 = 1+2+3$. Incidentally, 6 is also a triangular number, i.e. a sum of consecutive numbers starting from 1. The next perfect number is $28 = 1+2+4+7+14$.
- 7 is the first Mersenne prime number for which we didn't find another property. Mersenne prime numbers are prime numbers that can be written as $2^k - 1$, e.g. $7 = 2^3 - 1$, and the next one is $31 = 2^5 - 1$.

In fact, even perfect numbers and Mersenne prime numbers are connected by this beautiful theorem:

THEOREM 1.3 (Euclid-Euler theorem). *If* $2^k - 1$ *is a Mersenne prime number, then* $2^{k-1} \cdot (2^k - 1)$ *is a perfect number, and all even perfect numbers are of this form.*

We omit the proof, but the interested reader will be able to read and understand the proof here: https://primes.utm.edu/notes/proofs/EvenPerfect.html. Before you read, note that $\sigma(n)$ is defined as the sum

of divisors function, e.g. $\sigma(6) = 1+2+3+6 = 2\cdot 6$, so a number n is perfect exactly when $\sigma(n) = 2n$.

It is still an open question whether there are infinitely many Mersenne prime numbers or perfect numbers. Additionally, it is not even known if there are odd perfect numbers! It has been proved however that there are no odd perfect numbers that have 1500 digits or less, or in math terms, a lower bound for the odd perfect numbers is 10^{1500}.

So far, we have seen three sequences of natural numbers: Fibonacci, Mersenne primes, perfect number. For even more, visit this page: https://oeis.org.

EXERCISE 22. *Imagine the sequence that starts with* $1, 1, 1, 1$. *What would be the next term? Go to OEIS and see what the encyclopedia shows.*

2. Proof by induction

We can talk about numbers, their properties and sequences of numbers all day long, but since there are infinitely many of them, we will never stop the case by case analysis. So let us do all cases at once by induction!

PROOF. Recall the Induction Principle: we first need a list of statements labeled by natural numbers. We have a natural candidate for this:

$$P(n) = \text{“}n \text{ is interesting”}.$$

Then we need to prove that $P(0)$ is true, but we have already observed a unique property of 0.

Now, let us assume that $P(0) \wedge P(1) \wedge \cdots \wedge P(n)$ is true, or in plain English, that all natural numbers up to n are interesting. We prove that $n+1$ is interesting by contradiction: if it wasn't, then it will have the special property that it is the smallest natural number that is not interesting. Isn't that interesting?! So $P(n+1)$ is true.

Finally, we can apply the Principle of Induction and get that all $P(n)$ are true, i.e. that all natural numbers are interesting. □

3. Structure of proofs by induction

By analyzing the proof above, we can divide proofs by induction into several steps:

(1) Identify the statements $P(n)$.
(2) Step 2 is also called base of induction: prove $P(0)$ or $P(1)$ (sometimes it doesn't make sense to talk about $P(0)$).

(3) Assume that all $P(k)$ with $k \leqslant n$ are true – this is called the induction hypothesis. Now perform the step of induction: prove that $P(n+1)$ is true.
(4) Finally, conclude by the Principle of Induction that all $P(n)$ are true.

4. Exercises

EXAMPLE 4.1 (Triangular numbers). Prove that the sum of the first n positive integers is $\frac{n(n+1)}{2}$.

(1) Here $P(n)$ means "$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$", and we will avoid talking about $P(0)$. Although, strictly speaking, it makes sense, because $P(0)$ simply states that $0 = 0$.
(2) $P(1)$ states $1 = \frac{1\cdot 2}{2}$, which can be seen is true.
(3) Now assume that $P(n)$ is true, i.e. $1 + \cdots + n = \frac{n(n+1)}{2}$. Therefore, by induction hypothesis,

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

We can calculate the sum and get:

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

But now the equality that we get is exactly the statement $P(n+1)$.
(4) So by induction, the sum $1+\cdots+n$ is equal to $\frac{n(n+1)}{2}$ for all natural numbers n.

EXAMPLE 4.2. Prove that the sum of the first n odd positive integers is n^2.

We also have a picture proof.

Bibliography

[Boo] George Boole. An investigation of the laws of thought. Cambridge Library Collection. On which are founded the mathematical theories of logic and probabilities, Reprint of the 1854 original, Previously published by Dover Publications, Inc., New York, 1957 [MR0085180]; Prometheus Books, Amherst, NY, 2003 [MR1994936]. Cambridge University Press, Cambridge, pp. ii+viii+425. ISBN: 978-1-108-00153-3. DOI: 10.1017/CBO9780511693090.024.

[DP] Apostolos Doxiadis and Christos H. Papadimitriou. Logicomix. An epic search for truth, Character design and drawings by Alecos Papadatos, color by Annie Di Donna. Bloomsbury Press, New York, p. 347. ISBN: 978-1-59691-452-0; 1-59691-452-1.

[New] Clive Newstead. Infinite Descent. URL: https://infinitedescent.xyz/dl/infdesc.pdf.

[Sai] R. M. Sainsbury. Logical forms : an introduction to philosophical logic. Oxford, UK Cambridge, Mass: B. Blackwell. ISBN: 0631177787.

[WR] Alfred North Whitehead and Bertrand Russell. *Principia mathematica* to *56. Cambridge Mathematical Library. Reprint of the second (1927) edition. Cambridge University Press, Cambridge, pp. xlvi+410. ISBN: 0-521-62606-4. DOI: 10.1017/CBO9780511623585.