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 The textbook itself is 2300 years old and you may think that it may have outdated material (arguably, this is a correct guess), but it has survived more than a thousand of editions, and mathematicians only came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.

[1]We will discuss sets later.

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.

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.

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

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 $10^k = 9\ldots9 + 1$, and the first summand is divisible by 3. So we can write

$$a - 9\ldots9 = a_k + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0 \cdot 1.$$

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 $9\ldots9$ 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 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 thoorem 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 establis 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. □

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 $d \mid b$,

[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.

(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 .*

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

- *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!

$$\begin{aligned} 242 &= 66 \cdot 3 + 44 \\ 66 &= 44 \cdot 1 + 22 \\ 44 &= 22 \cdot 1 + 0\,. \end{aligned}$$

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

$$a = bq_1 + r_1 \qquad (0 < r_1 < b)$$

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

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. □

Bibliography

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