Math 4030 Notes

Adam Boocher

Fall 2016

1 Week 1: The Natural Numbers

1.1 Monday: Natural Numbers and Induction

Today's Goals

- Talk about different number systems and their properties
- Give a definition of the natural numbers, including the Well-Ordered axiom
- Learn the principle of mathematical induction

We begin with a class discussion of:

What is a number?

Some different answers should emerge, and we see that there are different types of numbers: whole numbers, integers, rational numbers, real numbers, complex numbers, and maybe even some number systems like time, military time.

- These all have their uses
- There are many differences

Discuss the inclusions

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

what properties are shared by all of them? These number systems should feel very familiar. Indeed, we learn about them starting as children and by the time we are finished with high school, it's hard to imagine not knowing what a number is. But at the same time **defining** something so basic is often one of the hardest tasks. Imagine a small child asking "why" after each explanation and you'll start to see the difficulty in defining basic objects. For instance: Let's define a Utah resident to be "a person who lives in Utah." Well then we have to define what a person is, what it means to live, and what Utah is. You can imagine chasing through the dictionary and having a pretty long definition when you are done! However you should also quickly realize that you'll never get a perfect definition - how can you define the bare bones?

The same is true in math - we have to start somewhere. Mathematicians will use the word **set** without a definition. Second, when we give definitions we sometimes also state **Axioms** which are properties that we assert without proof. But enough talking - let's see the definition of the natural numbers!

Definition 1.1. The set of natural numbers is $\mathbb{N} = \{1, 2, 3, \dots, \}$. It comes with an ordering $1 < 2 < 3 < 4 < 5 < \cdots$. We say that 2 is the number after 1, and 3 is the number after 3, etc.

Note two things things we are saying here:

- If n is a natural number, then there is another natural number $n + 1$, that we call "the number after n."
- We can compare any two numbers, and 1 is the smallest number.[1][2]

A **subset** is a set that is contained inside of a (bigger) set.

[1] 1 is also the loneliest number.

[2] Strictly speaking we should define inequalities and their properties as well, but in favor of a lighter first lecture, we'll just remind that $<$ behaves as we're used to it.

Example 1.2. The following are all examples of subsets of $\mathbb{N}$

- $\{1, 2, 3\}$
- $\{175\}$
- $\{2, 4, 6, 8, 10, \ldots, 2n, \ldots\}$ - the set of even natural numbers
- $\{\}$ - the empty set
- $\mathbb{N}$ - a set is always a subset of itself
- $\{2, 3, 5, 7, 11, 13, \ldots\}$ - the set of prime numbers (We'll define the prime numbers soon)

Remark 1.3. You'll probably have no trouble noticing that $\mathbb{N}$ is an **infinite set** and that some of the subsets of $\mathbb{N}$ are **finite**. But how would you define these terms?

1.1.1 What can we do with the natural numbers

We have given a *definition* of the natural numbers, but so far we haven't really said anything about what we can do with the numbers. For instance, we'd like to be able to add and multiply numbers (can we expect to subtract?) We'd also like to maybe prove some statements like $m + n = n + m$.

Now, you probably think all of this is obvious, and to a large extent, that's true. If we just listed ten nice properties and had them as axioms, life would largely be the same. But wouldn't it be better if we could assume fewer axioms?

For example we could state as axioms: 1) Earth is a planet 2) All planets have atoms 3) Earth has atoms. But do we really need to assume axiom 3? Doesn't it follow from the first two?

We'll need a few axioms to get off the ground in this course, and we won't always dwell on the details, but it's important to see that math isn't just a large set of rules - it has very few basic principles which imply lots of beautiful results!

Axiom 1.4. (Well-ordered axiom) Every set of natural numbers except the empty set has a smallest element.

Does this seem reasonable? Even though this seems pretty obvious, we can actually use it to **prove** a pretty impressive statement:

Theorem 1.5. *(Principle of Mathematical Induction) Is S is a subset of $\mathbb{N}$ and*

1. $1 \in S$
2. *whenever n is in S, then the number after n is also an element of S*

then S is equal to $\mathbb{N}$.

Before we get to the proof, I want to emphasize how we'll use this principle. Induction is useful in two important ways:

- To make definitions inductively
- To prove statements

We'll see examples of both of these. A good piece of advice is that whenever you are tempted to write "..." then you can probably appeal to the Principle of Induction.

1.1.2 Definition of Addition

Let's try it! Let's let m be a fixed number, pretend it's like 157. Our goal is to say how to define $m + n$ when n is any number.

- Now $m + 1$ is easy to define. $m + 1 =$ the number after m.
- And then $m + 2 =$ the number after $(m + 1) =$ the number after (the number after m).
- And so $m + n =$ the number after (the number after(the number after (... after the number after m))) or something terrible like that.

Let's do better. Let's define $m+n$ to be the number after the number $m+(n-1)$. So let's think through...

$m+2 =$ the number after $m+1$ (and oh we have a definition for $m+1$, it's the number after n.)

$m+3 =$ the number after $m+2$ and I guess we already know how to define $m+2$.

etc! In fact, if you think about the set

$$S = \{\text{numbers } n \text{ such that } m+n \text{ is defined}\}$$

then what do we know about S. Well $1 \in S$ and whenever n is in S, so is $n+1$. So by the principle of mathematical induction, $S = \mathbb{N}$. In other words, we know how to define $m+n$ for every value of n.

The Upshot Defining things by induction is sometimes a delicate endeavor - it usually is a rigorous way to replace the use of "...".

1.1.3 On Definitions

Give the a definition of the nth Fibonacci numbers F_n, where they are $F_1 = 1$, $F_2 = 1$, and the full sequence is

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots.$$

You should have gotten that $F_1 = 1, F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ when $n \geq 3$. What's important isn't the formula, it's knowing that this gives a complete definition for F_n for all n. Now matter what n I gave you, you'd in theory be able to compute it.

Can you give something that's not a definition? By comparison, here's a definition $A(n) =$ the age of the nth oldest person in the world alive today. What's the problem? How could we fix this? With domain and range?

We could define

$$A : \{1, 2, 3, \ldots, \text{world population}\} \to \mathbb{N}$$

and then this would be ok.

1.1.4 Using Induction to Prove Statements

We will use induction to prove that for all natural numbers n,

$$1 + 3^1 + 3^2 + 3^3 + 3^4 + 3^5 + \cdots + 3^n = \frac{3^{n+1}-1}{2} \tag{1.1}$$

Notice that this is giving us an infinite number of statements - one for each value of n. For instance, if $n = 1$, it says that

$$1 + 3^1 = \frac{3^2 - 1}{2}.$$

If $n = 2$ then it says that

$$1 + 3^1 + 3^2 = \frac{3^3 - 1}{2}$$

and so on. We can check these by hand. Let's use mathematical induction to prove that Equation 1.1 is true for all natural numbers n.

Step 1: Let S be the set of natural numbers n such that Equation 1.1 is true.

Step 2: Show that $1 \in S$ - We did that above, when we checked that $1 + 3^1 = \frac{3^2-1}{2}$.

Step 3: Show that if $k \in S$ then $k+1 \in S$. Ok, let's do it. We know that $k \in S$, so we already know that

$$1 + 3^1 + 3^2 + 3^3 + 3^4 + 3^5 + \cdots + 3^k = \frac{3^{k+1}-1}{2}$$

then let's add 3^{k+1} to both sides:

$$1 + 3^1 + 3^2 + 3^3 + 3^4 + 3^5 + \cdots + 3^k + 3^{k+1} = \frac{3^{k+1}-1}{2} + 3^{k+1}$$

and now do some arithmetic to see that

$$\frac{3^{k+1}-1}{2} + 3^{k+1} = \frac{3^{k+1} - 1 + 2 \cdot 3^{k+1}}{2} = \frac{3 \cdot 3^{k+1} - 1}{2} = \frac{3^{k+2}-1}{2}.$$

but this shows that $k+1$ satisfies Equation 1.1 and hence $k+1 \in S$.

Since we've finished steps 1,2,3 we can conclude by the principle of mathematical induction that $S = \mathbb{N}$ and thus Equation 1.1 is true for all natural numbers n.

The Upshot: We've seen instances of using induction to define operations (you'll get more practice on the homework) and to prove equalities for all natural numbers. These two ideas are two of the most important ideas in mathematics!

Finally for more practice, let's give a proof of the principle of math induction using only the well-ordered axiom.

Proof of Principle of Mathematical Induction. Let S be a subset of $\mathbb{N}$ such that $1 \in S$ and whenever $n \in S$ so is $n+1$. We want to show that $S = \mathbb{N}$. We argue by contradiction. Suppose that $S \neq \mathbb{N}$. Then that means that $W = \mathbb{N} \setminus S$ is non-empty. In other words there is something in $\mathbb{N}$ that is not in S. But then this means that W has a least element by the well-ordered property. Call this element k.

Let's think about k. Remember

$$k \text{ is the smallest number that's not in } S. \qquad \text{(dagger)}^{3}$$

So k can't be 1, because $1 \in S$. So we know $k > 1$. But now consider the number $k-1$. Since it is smaller than k, it can't be in W, but that means it is in S. But if $k-1$ is in S then by assumption, k should be in S. But this contradicts dagger! □

Remark 1.6. This proof is a good one to know. When I say things like this, it usually means a couple of things. First, it means that it's a theorem that I think is important and might show up on an exam some day. But also it means that the theorem contains some interesting mathematics that will help you in math and life if you understand it well. For instance, I think this theorem is important, because it is one that has very few ingredients (just the well-ordered principle, the idea of thinking of W as a set and studying W versus S, and using hypotheses carefully.)

[3] usually we use † to denote the dagger symbol. We haven't this time.

1.2 Wednesday: Division with Remainder

Main Points from Lecture 2:

- Review the notion of induction and do an example
- State what long division of natural numbers means
- Define **prime**, **composite**
- Describe the Euclidean Algorithm

A Review of What we did last time

Last time we defined the natural numbers and talked about the principle of mathematical induction. Although it's entirely believable and in one sense obvious, it allows us to do many impressive things, like defining operations as well as proving theorems.

We defined addition in class, and then on the worksheet learned how to define multiplication:

Definition 1.7. Multiplication of m by a number:

Let m be a natural number. I will define how to multiply m by any other number n. I declare

$$1 \cdot m = m$$

and then I declare that if $n > 1$ then

$$n \cdot m \cdot = m + (n-1) \cdot m.$$

Notice that this could be called a "recursive" definition if we were in a computer class. Indeed, you imagine the computer saying "how do I compute $10m$? Well the formula says that $10m = m + 9m$ and I know how to add, so I guess I just have to figure out what $9m$ is, and oh! $9m = m + 8m$ etc.

Warmup 1.8. Another common way that we see induction in action is to use it to prove mathematical expressions are true. As a warmup, prove that

$$2^n \leq 2n!$$

for all natural numbers n.

Proof. To solve this, remember that we need to first show that the statement is true when $n = 1$. Ok this is just $2^1 \leq 2(1!)$, which is true.

Now suppose that $2^k \leq 2(k!)$ for some k. Then we hope to show that $2^{k+1} \leq 2(k+1)!$. It's always good to start with what we know and end with what we want. (Especially with inequalities!)

$$2^k \leq 2(k!)$$

$$2 \cdot 2^k \leq 2(2)(k!)$$
$$2 \cdot 2^{k+1} \leq 2(2 \cdot k!)$$

hmm, this right hand side is definitely not what we had hoped it would be. There's no $(k+1)!$. But isn't it true that $2 \leq (k+1)$ always? So we can do

$$2^{k+1} \leq 2(2 \cdot k!) \leq 2(k+1)k! = 2(k+1)!.$$

Woohoo! □

1.2.1 Division and Factors

So far, we have seen that the natural numbers have two important operations: addition and multiplication. There is in general no way to divide two natural numbers without introducing fractions. However, sometimes we **can** divide one number by another. After all, what sort of world would it be if we couldn't divide 4 by 2 evenly. We'll need some information to do this though.

Definition 1.9. Let n and a be natural numbers. We say that a divides n (denoted $a|n$) if there is a natural number b such that $ab = n$.

Example 1.10. We say that 3 divides 18 and 6 divides 600. But 5 does not divide 13, nor does 18 divide 3.

Even though 5 does not divide 13, we can still divide 13 by 5 is we allow remainders. Indeed, we can say that

$$12 = 5 \cdot 2 + 3.$$

This suggests the following

Theorem 1.11. *Let $m < n$ be two natural numbers. Then there is a number $q \in \mathbb{N}$ called the* quotient *such that either*

(a) $n = mq$ (in which case, m divides n)

otherwise the is a remainder, some natural number $r < m$ such that:

(b) $k = mq + r$.

Remark 1.12. What's important? Notice that we require that $r < m$. In other words, our remainder is smaller than the quantity we are dividing by. Why does this seem reasonable? Well if you're dividing 100 apples among 9 people, you could certainly just give everyone 10 apples, and have 10 left over. But why not give everyone 11 and have 1 left over? The point is that you want to divide out as much as possible. Remember, both of these equations are true,

$$100 = 9 \cdot 10 + 10$$

$$100 = 9 \cdot 11 + 1,$$

but only the second is what we call division with remainder.

Proof. Suppose that $m < n$. If m divides n, then we have case (a) and we're done. So let's suppose that m does not divide n.

Ok, what does that mean? Well it means that if I multiply m by another natural number, I will NEVER get n. So let's look at the set

$$T = \{b \in N \ |mb > n\}.$$

This is some set, right? It is nonempty (why?) so by the well-ordered axiom, this means that T has a least element, which I will call p. Now let's see what this means:

I know that $mp > n$. And that $m(p-1) \leq n$, (since $p-1$ is not in T.)

Now it's true that $p > 1$, and I claim that if I pick $q = p - 1$ then I win. Let's see why: I know that $mq \leq n$, but since m does not divide n, we must have that

$$mq < n.$$

But this means that $mq + r = n$ for some number r. Now I just need to prove that $r < m$. But this is true because if $r \geq m$ then $r = m + r'$ and then we would have

$$mq + r = mq + m + r' = m(q+1) + r' = mp + r' > n,$$

a contradiction! □

There is a different proof of this fact in Aaron's notes, and you are encouraged to think of your own as well! The division algorithm is a formal statement of the long division with remainder that we teach in school. However, we'll see that it comes into play in addition, when we discuss the division of polynomials with remainder.

Definition 1.13. We say that a natural number p (other than 1) is prime if the only factors of p are itself and 1. Numbers other than 1 that are not prime are called composite numbers. The number 1 is neither prime nor composite.

Question 1.14. Why is 1 not a prime? We'll come back to this question when we discuss the uniqueness of prime factorizations.

Example 1.15. The following are all primes numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$.

Primes are the building blocks of all numbers as we see in the following

Theorem 1.16 (Fundamental Theorem Of Arithmetic)**.** *Let $n > 1$ be a natural number. Then n can be factored as a product of prime numbers.*

Proof. See Aaron's notes. □

Theorem 1.17. *There are Infinitely Many Primes*

Proof. There are dozens of proofs of this fact, but we present Euclid's proof because it is the most famous. Suppose that there are finitely many primes $p_1, p_2, \dots, p_k$. Then consider the number

$$N = p_1 \cdot p_2 \cdots p_k + 1.$$

This number is clearly not divisible by any prime since it leaves a remainder of 1 upon division by any number, but this contradicts the Fundamental Theorem of Arithmetic. □

1.2.2 The gcd of two numbers and the Euclidean Algorithm

It's very useful to understand the prime factorization of a number - for small numbers we can do this by hand. For instance, to factor 96 we can just peel off factors to see that

$$96 = 2(48) = 2(2)(24) = (2)(2)(2)(12) = (2)(2)(2)(2)(6) = (2^5)(3).$$

Similarly we could factor $168 = (2^3)(3)(7)$. From this factorization it is clear that $(2^3)(3)$, (24, that is) divides both of these numbers, and that that's the biggest such factor. This factor is called the greatest common factor or gcd. We would write

$$gcd(96, 168) = 24$$

Example 1.18. Compute $gcd(a, b)$ where

$$a = 2^3 \cdot 3 \cdot 17^3 \cdot 23^8, \quad b = 2^7 \cdot 3 \cdot 5^{17} \cdot 17^2 \cdot 101^3 \cdot$$

Answer: $2^3 \cdot 3 \cdot 17^2$.

In principle this tells us how we can find the gcd of any two numbers, but it requires us to know the prime factorizations of the numbers. This is actually a **really** difficult question if the numbers are very large. For instance, RSA Laboratories offered significant cash prizes for factoring numbers. For example, they offered \$30,000 to factor the following 212 digit number:

7403756347956171282804679609742957314259318888923128908493623263897276503402826627689199641962511784399589
...4330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359.

It was finally factored in 2012 after years of effort! It's the product of exactly two prime numbers.

We end today's lecture with a discussion of something called the Euclidean algorithm which allows us to compute the greatest common divisor of two numbers. What is cool about this is that this algorithm is often very quick even with large numbers.

Proposition 1.19 (The Euclidean Algorithm)**.** *Start with natural numbers $m < n$. Perform long division according to the following algorithm whenever there is a remainder:*

$$n = mq_1 + r_1$$

$$m = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$r_2 = r_3 q_4 + r_4$$

etc. Eventually the algorithm terminates with no remainder. That is we have a line

$$r_k = r_{k+1} q_{k+2}.$$

This last nonzero remainder r_{k+1} is the greatest common divisor *(gcd) of m and n, i.e. the largest natural number that divides both. This is proven later in the course.*

The greatest common divisor of two numbers is simply the biggest number that divides evenly into both of them. If we have a prime factorization of two numbers, it is easy to compute these

Here is an example of the Euclidean algorithm in action.

Example 1.20. Find the gcd of 105 and 385:

$$385 = 105 \cdot 3 + 70$$

$$105 = 70 \cdot 1 + 35$$

$$70 = 35 \cdot 2.$$

So the gcd is 35. Indeed, we could check that $105 = (2)(35)$ and $385 = (11)(35)$.

For next week's class, take a look at Section 1.2 of Aaron's notes.

2 Week 2: The Integers and Rational Numbers

2.1 Monday: Meet the Integers

We're going to define the integers this week as well as the rational numbers. We will see that the integers have some properties that the natural numbers do not. This is due mainly to the fact that the integers possess the operation of subtraction. Although subtraction seems very common to us nowadays, it was something that took a few thousand years to properly develop. Subtraction, along with the notion of zero, both lead to the notion of something called an Abelian group - a theme that we will return to very often in our course.

The integers are very much like the natural numbers - no real frills:

2.1.1 The definition

Definition 2.1. The set of integers is $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ which consists of three types of numbers:

- (I). The natural numbers, which we call positive integers $\{1, 2, 3, \ldots\}$
- (II). The negative integers $\{\ldots, -3, -2, -1\}$.
- (III). Zero

There is an operation that goes from an integer x to the "next lowest" integer $x - 1$. Remember we didn't have such a thing for the natural numbers, since $1 - 1$ wasn't defined (yet).

These numbers are ordered in the usual way: But! There is no well-ordered principle that we can speak of: Indeed, there are lots of subsets of $\mathbb{Z}$ that have no smallest element. For instance, the set of negative numbers does not. Nor does the set $\mathbb{Z}$ itself.

2.1.2 How to add and subtract

Suppose we wanted to add two integers x and y. How could we do that? Remember - we can think of the positive integers as natural numbers, and in that case we have already defined what addition (and multiplication) mean. For instance, we know how to define $4 + 3$.

Thus to define addition, we have to just consider the different cases when y is positive, negative or zero. We'll work through these cases on the board. (Or see Aaron's notes for more information)

Question 2.2. Why is it ok to just consider the cases of y? Don't we also have to think about x?

Notice that we can always talk about the **negation** of an integer x, which we denote by $-x$. It is defined exactly as you think. For example, the negative of 5 is -5. Shocking.... But useful! How so?

Proposition 2.3. *If x is an integer, then*

$$x + (-x) = 0.$$

Proof. What the heck is the content of this statement? Well it's all about the definition of negation and addition. Remember that both of these have three cases. If $x = 0$ then $-x = 0$ so this says that $0 + 0 = 0$. If $x > 0$ then this is saying that going x steps to the left of x gets you to zero. If $x < 0$ then this says that going x steps to the right of $-x$ gets you to zero. Does this make sense? □

So you might not be very impressed that $x + (-x) = 0$. Indeed, this isn't so impressive since we kind defined $-x$ to be exactly the number that cancels x down to zero. Maybe that's why I called the above result a Proposition and not a Theorem... But here's a Theorem!

Theorem 2.4. *The only integer we can add to x to get 0 is the number $-x$. Said differently, the only solution to $x + y = 0$ is $y = -x$.*

Proof. This proof requires a bit more. It's saying that the only solution to "$x+$ something = 0" is when that something is the exact number $-x$. How can we prove something like this? Well we can say: Suppose that

$$x + y = 0$$

and then try to figure out what y is. Let's add $-x$ to both sides. Then we get

$$(-x) + (x + y) = 0 + (-x)$$

$$(-x + x) + y = -x$$

$$0 + y = -x$$

$$y = -x.$$

□

Remark 2.5. Notice that in the proof we had to use the associative property of addition, which says that $(a + b) + c = a + (b + c)$. All this is setting you up for the notion of an Abelian group!

Definition 2.6 (Subtraction)**.** If x and y are integers then $x - y$ is defined to be $x + (-y)$.

Exercise 2.7 (Cancellation Law)**.** Show that if $a, b, cin\mathbb{Z}$ and $a + b = c + b$ then $a = c$.

2.1.3 Multiplication

Let's get something straight - I know that we all know how to multiply numbers, yet here we are, about to define them one more time. What gives? Well sometimes I forget how a definition goes (not about how to multiply numbers, but maybe like how Cramer's rule goes or something like that. Or maybe how the epsilon and delta work in analysis) What's a mathematician to do? One method would be say

> "Alas, it's a **definition**, so it could be ANYTHING - I can't possibly figure it out."

Yes, you could say that.. but what's better is to think about the definition and say

> "Hmm, well how would X work in this super simple case. Was it rows or columns?
> Was it $\leq$ or $\geq$? etc ..."

Many a time, you will discover that often knowing what happens in a simple case will be enough to tell you the whole story. For real.

Let's see what I mean. Suppose that we want to define multiplication of integers. Naturally we want to do this in a way that extends the multiplication we already have for natural numbers. So if we want to define how to multiply $x \cdot y$ when $x, y \in \mathbb{Z}$ then we already know how to do this when $x, y > 0$. If, say $x = 0$, then we have to figure out what $0 \cdot y$ is, and then we have to figure out what happens when, say, $x > 0$ and $y < 0$, or when both $x, y < 0$. This seems like a lot of cases, and surely we all know the rules governing these sorts of things. But:

Prize Problem 2.8. A common question for a youngster is "Why is a negative times a negative equal to a positive?" Indeed, this is an excellent question, and it's actually a little subtle to answer. Why exactly is $(-3)(-5) = 15$? For a prize, whoever comes up with the most compelling answer (aimed at a middle school students, say) to this question will win a prize and I'll include it in this copy of the notes.[4]

While you are encouraged to think about this prize problem at home, in class I'm going to give the mathematician's answer to this problem. Note: while I hope this convinces you as mathematicians, this doesn't mean it's at all what you should tell a young student. My hope in this course is that you think about how all these different ideas interact and how this can help you in your future teaching.

Multiplication by 0: If you think multiplication by zero is easy - you're right, but then again it took people a long time to even come up with the notion of zero. I think it's not all as obvious as you'd think. Here's an idea that will be useful a bit later. Let's recall that we want our number system to satisfy the distributive property: $n(x + y) = nx + ny$. Now what happens if we play different games with n, x, and y?

For instance, if we let $x = y = 0$, then we get

$$n(0 + 0) = n \cdot 0 + n \cdot 0.$$

$$n \cdot 0 = n \cdot 0 + n \cdot 0.$$

Now by the cancelation rule, we see that $0 = n \cdot 0$.

Multiplication by -1: Whoa, we're on a roll! We **figured out** what $n \cdot 0$ was just by using the distributive property. Let's see if we can do that for other multiplications. Let x be an integer.

$$x(1 + (-1)) = x(-1) + x(1)$$

$$x(0) = x(-1) + x(1)$$

[4] Warning: my prizes are often rather silly.

$$0 = x(-1) + x$$

Well look - this means that $n(-1)$ must be the negation of n. In other words:

$$n(-1) = -n.$$

For instance, this shows that $(-1)(-1) = 1$.

Finally, we can figure out what $(-3)(-5)$ should be, by the same reasoning. Pay careful attention to this and see how each step uses something we've done before:

$$(-3)(-5) = ((-1)(3))(-5) = (-1)((3)(-5)) = (-1)(3)(5)(-1) = (15)(-1)(-1) = 15.$$

As mentioned before, this isn't the explanation we would give to the non-mathematician. But today's lecture is really a lesson in how so many of the "rules" that we have in mathematics can actually be gotten from a very small set of principles. In the worksheet today (and on the next homework) you'll see a few abstract examples where you get a chance to prove similar rules in slightly more abstract settings.

Read or re-read Aaron's notes about the Rational Numbers for the next class

2.2 Wednesday: Equivalence Relations and Rational Numbers

In this lecture we are going to define rational numbers. Aaron's treatment in his notes is very thorough and I think quite pleasing to read. We'll start by talking about what is subtle about the rational numbers.

Somehow we talk about the number 1/2 by many different names. Sometimes we call it 1/2 and other times 2/4 and yet other times as $(-3)/(-6)$. What is that slash? What do we mean when we say they are the "same"? Well that's what we're going to do today.

First off I'm going to give the definition that Aaron gives in his notes. He says that the set of rational numbers $\mathbb{Q}$ is defined to be the set

$$\mathbb{Q} = \{\text{slopes of lines that pass through } (0,0) \text{ and a point } (b,a)\}$$

where we require that $a, b \in \mathbb{Z}$ and $b \neq 0$. (So the line isn't vertical)

Let's do an example. According to this definition we can look at the line through $(0,0)$ and $(2,1)$. (Draw it on the board). But isn't this the same as the line through $(0,0)$ and $(4,2)$? Why yes - this is related to the fact that $1/2 = 2/4$. In fact, as long as we pick any point on this line with integer coordinates, those could very well be the a and b in our definition. Is this a problem?

No! Our definition of $\mathbb{Q}$ says that we are interested in the set of slopes of lines, not in these points. So in other words, even though $(2,1)$ and $(4,2)$ are totally different points, the lines through those points are the same, and so they give the same element of $\mathbb{Q}$.

Exercise: When do two points (b,a) and (b',a') determine the same point in $\mathbb{Q}$. (Answer: see Aaron's notes)

What we want to do next is to assign a symbol to each line. i.e. the fraction symbol. But we have a problem, that there are gonna be many ways to represent a given rational numbers as a fraction. Well let's try

Definition 2.9. An integer fraction is a symbol of the form: $\frac{a}{b}$. Where $a, b \in \mathbb{Z}$ and $b \neq 0$. Two integer fractions are called **equivalent**, written

$$\frac{a}{b} \sim \frac{a'}{b'}$$

if (b,a) and (b',a') are on the same line through the origin.

Notice that the symbol "$\sim$" is called a **relation** and it is easy to see that (talk through why these are true. Remember that $\sim$ just means "is on the same line as".)

1. $\sim$ is reflexive, meaning that $a/b \sim a/b$
2. $\sim$ is symmetric meaning that if $\frac{a}{b} \sim \frac{a'}{b'}$ then $\frac{a'}{b'} \sim \frac{a}{b}$
3. $\sim$ is transitive meaning that if $\frac{a}{b} \sim \frac{a'}{b'}$ and $\frac{a'}{b'} \sim \frac{a''}{b''}$ then $\frac{a}{b} \sim \frac{a''}{b''}$.

A relation satisfying these three properties is called an equivalence relation.

Remark 2.10. Let's pause for a minute and recap what we have so far. We have fractions. We have a way of saying they are equivalent. What we are about to do is define something called an equivalent class - which we can think of as a box that contains all elements that equivalent. For instance, we'll have a box labeled 1/2 that contains all fractions like $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}$ etc. Then we will declare that the set of rational numbers is $\mathbb{Q} = \{\text{boxes of equivalent fractions}\}$.

Definition 2.11. The equivalence class

$$\left[\frac{a}{b}\right]$$

is the set of all fractions that are equivalent to $\frac{a}{b}$.

Let's be careful here: $\left[\frac{1}{2}\right]$ is the box that contains all fractions equivalent to $\frac{1}{2}$. And $\left[\frac{2}{4}\right]$ is the box that contains all fractions equivalent to $\frac{2}{4}$. THESE ARE THE SAME BOX!

$$\left[\frac{1}{2}\right] = \left[\frac{2}{4}\right]$$

Notice that if we want to visualize the rational number a/b as appearing on a line, we can look at where the corresponding line intersects the vertical line $x = 1$. This helps us see, for instance when to say that $[\frac{a}{b}] < [\frac{c}{d}]$. (Aaron's notes go into this in more detail)

We are now ready to declare (fanfare!) that

$$\mathbb{Q} = \{\text{equivalence classes of fractions}\}.$$

Notice that $\mathbb{Q}$ is ordered, but has no well-ordered axiom, nor does it have a "next smallest element" operation. We can't talk about the "next smallest number" so induction isn't really around for rational numbers.

Remark 2.12. We've got some work to do. Let's make a long list: we want to :

- Define addition of rational numbers
- Define multiplication
- Maybe we can finally divide?
- See what any of this is good for?

Since we don't have induction, we have to define the addition of two rational numbers in a more direct way:

Definition 2.13. If $\left[\frac{a}{b}\right]$ and $\left[\frac{c}{d}\right]$ are two rational numbers then we define their sum to be

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right].$$

What do we have to check? We need to check that this is well-defined! (For this proof, see Aaron's notes - we'll do it in class)

We can also similarly define multiplication -

Definition 2.14. If $\left[\frac{a}{b}\right]$ and $\left[\frac{c}{d}\right]$ are two rational numbers then we define their product to be

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

Again, we should check that this is well-defined, and maybe also that addition is associative, and so is multiplication, and that we have the distributive law, etc.

Exercise 2.15. Show that if a and b have a common factor, say m then we can "cancel" m in the fraction. That is, say that $a = ma'$ and $b = mb'$ then show that $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$

3 Week 3: Labor Day and The Rational Numbers Concluded

3.1 Monday: Labor Day

3.2 Wednesday: Finish the Rational Numbers

- Homework is due! And Homework 1 is being returned. The homework was very good for the most part. There were a few concerns about induction, so I'll continue to put some induction problems on each homework until we iron out those difficulties. Remember that your induction hypothesis should be a mathematical sentence. Examples of sentences are "The sum of the first n even numbers is given by formula $*$." "A set with n elements has 2^n subsets." "$1 + 2 + 3 + \cdot + n = n(n + 1)/2$". Note that the equals sign in the last statement is the verb in that final sentence.

- For the last homework problem, very few people got full points - if you didn't, you can re-write your solution and turn it in to me on Monday and I can give you up to 3 points back.

- Also - please come talk to me if you have questions! My office hours are a bit lonely at present.

Today our goal is to finalize our work with the rational numbers and make a preparation for the existence of numbers that are not rational. We'll start with a review of our definition of the rational numbers. We'll go over the proof in Aaron's notes that the addition of rational numbers is well-defined. Then you'll get a chance to work on some problems about well-defined operations.

Also today, I want to prove that there are numbers that are not rational. For instance, imagine the square with side length 1. The diagonal of this square obviously has a length, and it would be nice to have a number system that includes this length. Geometry tells us that this length is equal to $\sqrt{2}$, i.e. if we made a square with this as its sidelength, that square would have area 2.

Theorem 3.1. *There is no rational number a/b whose square is* 2*.*

Proof. If this were true, then we would have that $(a/b)(a/b) = 2$ for some integers a and b. Let's assume this fraction is in lowest terms. In particular, maybe a is even, or maybe b is even. But they can't BOTH be - since it's in lowest terms.

So this means that $a^2/b^2 = 2/1$. Since these fractions are the same, this must mean that $a^2 = 2b^2$ (cross-multiplying). But now look at the right hand side of this equation. It is even. So that must mean that the left hand side is even.

$$\text{So we know } a^2 \text{ is even.}$$

But this means that a must be even. So that means $a = 2k$ and now our equation says

$$a^2 = 2b^2$$

$$4k^2 = 2b^2$$

$$2k^2 = b^2$$

Uh oh, this says that the left hand side is even, so the right hand side must be as well. Hence b^2 is even, and thus b is even. But this is impossible, since we assumed that a and b can't both be even. □

So we have some number (a length) that is not a rational number. We'll want to make sense of these numbers in the coming week when we learn about the real numbers. To do that, we'll have to talk about expanding rational numbers, and decimals and the like!

3.2.1 Finding Pythagorean Triples

Depending on whether or not there is time at the end of class, we might explore the following problem:

Problem 3.2. Given a rectangle with side lengths $a, b \in \mathbb{Z}$ when is it true that the diagonal is also in $\mathbb{Z}$?

We can see that the square with sides $1, 1$ does not give a positive answer to this problem. Indeed, we showed that the diagonal was $\sqrt{2}$ which does not even live in $\mathbb{Q}$, let alone $\mathbb{Z}$. In symbols, we are asking for triples a, b, c of integers that satisfy an equation

$$a^2 + b^2 = c^2.$$

Question 3.3. What are the natural number solutions (a, b, c) to the equation $a^2 + b^2 = c^2$? Such a solution is called a Pythagorean triple.

Corollary. Some easy-to-remember Pythagorean triples are e.g. $(3, 4, 5), (5, 12, 13), (8, 15, 17)$.

A first question we might ask if there are infinitely many such triples. However, we see that as soon as we have a single solution, we have found infinitely many:

Remark 3.4. If (a, b, c) is a Pythagorean triple, and d is any positive integer then so is (da, db, dc).

Proof. We just check that

$$(da)^2 + (db)^2 = d^2(a^2 + b^2) = d^2(c^2) = (dc)^2.$$

□

Given this fact, we define a **primitive Pythagorean triple (PPT)** to be a Pythagorean triple such that a, b, c have no common factor. This means that there is no number d that divides all of a, b, c. We can now rephrase Question 3.3 as: What is the set of PPTs?

A Geometric Idea: Notice that if (a, b, c) is a PPT then $(a/c, b/c)$ is a point with rational coordinates on the unit circle $x^2 + y^2 = 1$. We notice that $N = (0, 1)$ is a point on the circle. Never matter that one of the coordinates is zero, we can worry about that later. The key insight is to now notice that if (x, y) is another point on the circle with rational coordinates then the slope of the line between these two points will have rational slope. The converse is also true, which we prove now:

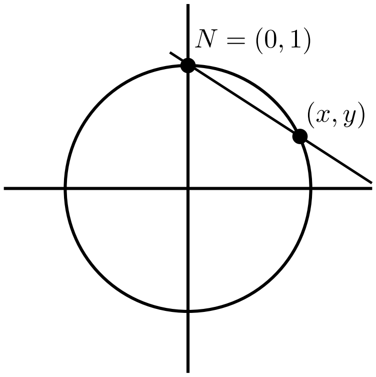

Figure 1: Geometric Method of Finding Pythagorean Triples

Suppose that $P = (x, y)$ is a point on the unit circle such that the line between N and P has a rational slope m. Then $m = (y - 1)/x$ or equivalently $y = mx + 1$. Since P lies on the unit circle, we can conclude that

$$\begin{aligned} x^2 + (mx + 1)^2 &= 1 \\ (1 + m^2)x^2 + 2mx + 1 &= 1 \\ x((1 + m^2)x + 2m) &= 0 \end{aligned}$$

This equation describes the set of points that lie on the intersection of the circle and the line. The solution $x = 0$ is the point N, and the solution $x = (-2m)/(1 + m^2)$ describes the point P. Using $y = mx + 1$ we have proven

Theorem 3.5. *Every point on the circle $x^2 + y^2 = 1$ with rational coordinates is of the form*

$$(x, y) = \left(\frac{-2m}{1 + m^2}, \frac{1 - m^2}{1 + m^2} \right)$$

where m is a rational number. (Except for the point $(0, -1)$ which is the limiting value as $m \to \infty$.)

If we write $m = u/v$ and clear denominators, then we see that this formula becomes:

$$(x, y) = \left(\frac{-2uv}{u^2 + v^2}, \frac{v^2 - u^2}{v^2 + u^2} \right)$$

which if we plug into the equation for the unit circle and simplify we get

$$\begin{aligned} x^2 + y^2 &= 1 \\ (-2uv)^2 + (v^2 - u^2)^2 &= (v^2 + u^2)^2 \\ (uv)^2 + \left(\frac{v^2 - u^2}{2}\right)^2 &= \left(\frac{v^2 + u^2}{2}\right)^2. \end{aligned}$$

There are lots of other questions we might want to answer. For example, if c is given, do there exist a and b so that $a^2 + b^2 = c$? If so, how many such a and b are there? For example

$$33^2 + 56^2 = 65^2 \text{ and } 16^2 + 63^2 = 65^2.$$

It turns out that the a highbrow way to view this question (and others) involves passing to the so-called ring of Gaussian integers - which involves imaginary numbers. We might return to this topic at the end of the course once we have a larger toolkit.

4 Week 4: The Real Numbers

This week I mostly followed Aaron's notes about the Real Numbers. What's important?

- We learned that they are defined by their decimal expansions.
- We learned that rational numbers are precisely those real numbers who decimal expansion repeats
- We learned how to convert between repeating decimals and rational numbers.
- We also discussed some modular arithmetic vis a vis the homework, and learned about continued fractions.

On Wednesday we went through how one might define addition and multiplication of real numbers. We did so by approximation. The idea is that if we have a sequence of rational numbers that converges to x, then we can think of this number as being approximated by rationals. Then we can use the constructions we have already built for rational numbers.

5 Week 5: The Complex Numbers

5.1 Monday: Introduction to the Complex Numbers

Let's look at the equation $x^2 - 2 = 0$. When does it have a solution?

- Integers? No
- Rational numbers? No
- Real numbers? Yes
- Mod 4? No
- Mod 7? Yes

Key Point: There are sometimes solutions to equations and sometimes not. What matters is the number system that we're working with.

Let's prove the following

Proposition 5.1. *Let $b \in \mathbb{R}^+$. The equation $x^2 - b = 0$ always has a positive real solution. We call this number $\sqrt{b}$.*

Proof. This proof of this fact requires something (here we'll use some calculus) of the analysis sort. Notice that if we define the function $f(x) = x^2$ (a continuous function) then we see that $f(0) = 0$ and $f(big) = big$ so that by the intermediate value theorem there must be a point where the graph crosses the line $y = b$. Hence this crossing happens at some point (a, b) with $a > 0$ where we must have that $a^2 = b$. This number a is our solution. □

In other number systems it's often hard to predict whether a number will have a square root. For instancce

Question 5.2. When does 2 have a square root in $\mathbb{Z}/n\mathbb{Z}$?

It turns out that the answer to this question is the set when n is one of $1, 2, 7, 14, 17, 23, 31, 34, 41, 46, 47, 49, 62, \ldots$. This is the list of numbers that are not multiples of 4 and for which all odd prime factors are congruent to ± 1 mod 8.

5.1.1 Introduction of i:

Now let's talk through the reason why $x^2 + 1 = 0$ has no solutions in $\mathbb{R}$. (Both terms on the left are ≥ 0.) We can now add a symbol i to our number system and just declare that $i^2 = -1$. This allows us to define

$$\mathbb{C} = \{a + bi \mid a, b, \in \mathbb{R}\}.$$

We will define addition and multiplication so that these numbers (see Aaron's notes). Here are some salient features:

- The complex numbers are no longer ordered (we can't make sense of whether $1 + 2i$ is bigger or smaller than $2 + 1i$ for instance.
- Addition and multiplication are commutative and satisfy the distributive and associate laws etc.
- There is a conjugation operation: $c : \mathbb{C} \to \mathbb{C}$ that sends $a + bi$ to $\overline{a + bi} := a - bi$. This is just reflection across the x-axis. (The Real axis).

This conjugation function is very useful. First of all it satisfies some nice properties that

$$\overline{(a + bi) + (c + di)} = \overline{a + bi} + \overline{c + di}.$$

$$\overline{(a + bi) \cdot (c + di)} = \overline{a + bi} \cdot \overline{c + di}.$$

(We will prove this in class).

It is maybe a bit surprising that conjugation is multiplicative. After all - negation is not. $-(rs)$ is not the same as $(-r)(-s)$.

Second of all, the conjugate allows us to compute inverses. We start with the notion of "absolute value" or length. We define the absolute value of a complex numbers $a + bi$ to be $|a + bi| = \sqrt{a^2 + b^2}$. (Draw a picture to see that this is the length from the origin to the point $a+bi$. What does this have to do with conjugates? Well notice that

$$|a+bi|^2 = (a+bi)\overline{a+bi}.$$

In other words, if z is a complex number then $|z|^2 = z\overline{z}$. Let's emphasize that again:

$$|z|^2 = z\overline{z}$$

Why is this so cool? Well we know that the number on the left is **real**. Indeed, it's just a^2+b^2. And this is nonzero unless $a=b=0$. And we know how to divide by real numbers (we just multiply by the multiplicative inverse). So we can see that

$$1 = z\overline{z}/(|z|^2).$$

$$1 = z(\overline{z}/|z|^2).$$

This means that if z is not zero, then $1/z = (\overline{z}/|z|^2)$, another complex number.

Problem 5.3. Find the multiplicative inverse of $z = 3+4i$. Well the answer should be $1/(3+4i)$. We can then multiply top and bottom by the conjugate $3-4i$ and we obtain

$$\frac{1}{3+4i} = \frac{3-4i}{3^2+4^2} = 3/25 - (4/25)i.$$

6 Week 6

6.1 Monday - Review of Exam plus the rest of Complex Numbers

It's been a week since the last class, and we've had an exam. The exam was mostly good, I just want to emphasize a few things:

- Negative numbers in modular arithmetic - rewrite $[-5]$ in $\mathbb{Z}/9\mathbb{Z}$ as $[a]$ with $a > 0$.
- Class discussion about whether
$$k^2|ab \implies k|a \text{ or } k|b.$$
- Class discussion about induction this went really well and we had presentations at the board. Well done!

6.2 Wednesday

I talked about complex multiplication and how it is rotation in the complex plane. We went over how to use this intuition to get information about inverses, and how to extract nth root.

7 Week 7

7.1 Monday

Warmup 7.1. We write a number $z = r(\cos\theta + i\sin\theta)$ as (r, θ) following Aaron's notes. Let
$z = (5, 240^o)$,
$w = (2, 60^o)$
Compute (in polar coordinates is fine):

$$zw, \quad z^2, \quad \text{the 4 fourth roots of } z.$$

7.1.1 Exponentials

If we multiply two complex numbers, their angles add together. And their lengths multiply. Hmm, this sounds a lot like another property that we've seen before. Exponentials! Recall that for example, $(a^s)(a^t) = a^{s+t}$. And $(r_1a^s)(r_2a^t) = r_1r_2a^{s+t}$. Perhaps we could write our polar coordinates (r, t) in such a way? After all, we know that $(r_1, s) \cdot (r_2, t)$ should be $(r_1r_2, s + t)$. So why not just write

$$(r_1, s) = r_1a^s?$$

Well there are a couple of questions. First, why should this mean anything, like why should there be a connection between complex numbers and exponentials? And secondly, even if there were a connection, we'd have to figure out what a is. Luckily there is a beautiful answer to both questions. The answer is that

$$(r, t) = re^t$$

where $e = 2.71828\ldots$ is the base of the natural logarithm. To understand why this equation is true we need to address a question we haven't really talked about before

Question 7.2. How do we define exponentiation? In other words, what does 2^i mean? Or what about i^{-3i}?

The answer to this question is maybe not what you'd expect. A bit of digression is perhaps warranted. Let's split into teams and try to talk about how we define exponentiation. Be careful, if we want to define b^x then there have to consider what sort of beast b and x are. The difficulty arises with the exponent, rather than with the base, though. Let's assume $b \neq 0$.

x **is a natural number**: Then b^x is just $b \cdot b \cdots b$ the product x number of times.

x **is a natural number**: Well if $x = 0$ then $b^0 = 1$ and if $x < 0$ then $b^x = 1/(b^{-x})$.

x **is a rational number**: Well if $x = a/b$ then we can intrepret $x^{a/b}$ as the b, bth roots of (x^a). These might be complex, so we have to just clarify which ones we are talking about.

x **is a real or complex number**: There are different ways to look at this - all of them are going to involve some sort of limit. Here's what we'll do though:

Recall that

$$e^x = 1 + x + x^2/2! + x^3/3! + x^4/4! + \ldots + x^n/n! + \ldots$$

is a convergent series for any choice of x. So now let's think about it:

Say we wanted to compute $e^{(x+yi)}$. Well however we define this, we probably want it to equal e^xe^{yi}. And we already know what e^x means, since x is real. Ok, what about e^{yi}? Well we could try the power series:

$$e^{yi} = 1 + (yi) + (yi)^2/2! + (yi)^3/3! + \ldots + (yi)^n/n! + \ldots$$

$$= 1 + yi - y^2/2! - (y^3/3!)i + \ldots$$

Let's keep track of the real and complex parts:

$$(1 - y^2/2! + y^4/4! - y^6/6! + / - \ldots) + (y - y^3/3! + y^5/5! - y^7/7! + / - \ldots) \cdot i$$

Which is none other than

$$\cos y + i\sin y.$$

So we have shown that

$$e^{iy} = \cos y + i\sin y.$$

So we can proclaim happily now that the number (r, t) in polar coordinates is none other that $r(\cos t + i\sin t)$ which we just saw is re^{it}. Many times it will be easier to think of polar coordinates as exponentials.

Let's say it again: $e^{it} = \cos t + i \sin t$. It's important here that the angle t be in radians, otherwise the series won't converge like it should. So for instance we get an equation $e^{i\pi} = -1$. I think that's really satisfying.

Finally, I should finish up our discussion of exponents. If we want to define b^x when b is not e, then we have to do it in a slightly roundabout way. We should note $b^x = e^{\ln(b^x)} = e^{x \ln b}$, so if we can define $\ln b$, then we have that $b^x = e^{\text{something we can compute}}$. Defining $\ln b$ is not so hard - we can just say that ln is the "inverse" of the exponential function, but that actually gets us into lots of technical details. So maybe I'll just give an advertisement for a course in complex analysis - truly a beautiful course!

7.1.2 Some terms

It's probably a good time to review some mathematical nomenclature. I'll be a bit informal here, because what's important is that you remember the distinctions between these notions, not that you know all the details.

- A **field** is a number system where we can add, subtract, multiply and (divide by nonzero numbers)
- A **ring** is a number system where we can add, subtract, multiply but maybe not divide
- An **abelian group** is a number system where we can add and subtract.

Notice that this means that every field is also a ring, and every ring is also an abelian group. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are all examples of fields, $\mathbb{Z}$ is an example of a ring. $\mathbb{Z}/6\mathbb{Z}$ is an example of a ring that is not a field. $\mathbb{Z}/p\mathbb{Z}$ is a field when p is prime. All these examples are also abelian groups. We haven't really seen examples of abelian groups that aren't rings (and that's ok!). In math sometimes we want to zoom in on one structure - say the $+$ and $-$ structure, and that is why we give a name to this structure.

7.1.3 Polynomials

We'll start Aaron's notes - Chapter 2.

7.2 Wednesday

Today is the last day before fall break. We are going to learn a lot of mechanical things about polynomials and get practice with them. The goals today include learning:

- Review the definition of polynomials and give worksheet about adding and multiplying.
- Emphasize the difference between when the coefficient ring is a field or not.
- List the theorems at the bottom of the worksheet and see which are true when.
- Come together and go over the proofs.

8 Week 8

8.1 Monday

Today we will mostly finish up following Aaron's notes. After today, however, we'll deviate a bit from his notes. In particular, we will skip most of section 2-2.

We'll start today's class by asking a volunteer to go to the board and write down the statement of long division (with remainder) for the natural numbers. Then we'll write the corresponding statement for $\mathbb{Q}[x]$ and do the example in Aaron's notes. **Make sure you are proficient at dividing polynomials**. We'll do another example in class in doing the Euclidean algorithm on the polynomials $x^{10}+1$ and x^6+1 to find their gcd. We'll discuss what this means.

Let's now think about what a prime polynomial should mean? Discuss with your neighbor the definition of what it means to be a prime natural number. We'll get a definition on the board.

Definition 8.1. We say that a polynomial $f(x)$ is a factor of a polynomial $g(x)$ if there is a third polynomial $q(x)$ such that $g(x) = f(x)q(x)$. In other words, there is no remainder in the division algorithm.

We say that $f(x)$ is a prime polynomial if 1) it has degree $d > 0$. 2) It has no factors except for itself and constants. In other words, all of its factors are either of degree d or degree 0.

Now that we've got a definition, let's see which of the following are prime polynomials in $\mathbb{Q}[x]$:

$$6, 5, x+2, 2x+4, 3x-1, x^2-1, x^2-2, x^2+1, 2x^2+6, x^{300}+1, x^{21}-17x^{16}+9x^8-184.$$

Can we come up with any statements about what prime polynomials look like?

- Degree 1 polynomials are always prime (why? we'll talk through a proof)
- Sometimes it matters what the field is (x^2-2 factors over $\mathbb{R}$ but not over $\mathbb{Q}$, and similarly for x^2+1 over $\mathbb{R}$ or $\mathbb{C}$.)
- In general it's probably pretty hard to tell if something factors. (More on this later!)

Remember: For integers, remember it was an interesting question to consider what prime factors they had. In general, we knew that every number has a prime factorization. Do we think the same will be true for polynomials? Let's have a discussion about this - and see if we can come up with a statement.

8.2 Wednesday: Finishing up 2-1

We'll warm up with a discussion on any homework problems and then we'll discuss the following:

Theorem 8.2. *Let F be a field. Then every non-constant polynomial in $F[x]$ factors as a product of finitely many prime polynomials.*

Proof. In class we shall develop an informal proof - hopefully something involving factor trees. Here let's give a formal proof.

We will proceed by induction to show that if $f(x)$ is a polynomial of degree d then it factors as a product of finitely many prime polynomials.

Base case: $d = 1$: If $f(x)$ has degree 1 then it is prime by our discussion above. Thus every degree 1 polynomial is the product of 1 prime factor!

Inductive Step: Let's assume that if $f(x)$ is a polynomial of degree $\leq d$ then the statement is true. I.e. that if $f(x)$ has degree at most d, then it must factor into a product of finitely many prime polynomial.

Final Step: Ok, let's take a polynomial of degree $d + 1$ and show that we can factor it into a product of primes. Well there are a couple of options - $f(x)$ might be prime and then we're done. If not, then it must have two factors, say

$$f(x) = a(x)b(x)$$

and those have to have degree less than d (and greater than 0). Hmm but that means that the degrees of $a(x)$ and $b(x)$ must be $\leq d$. So by the induction hypothesis, we have that a and b factor as a product of prime polynomials. But then f as a product of a and b is itself a product of prime polynomials. □

8.2.1 Anything else?

I hope at this point you should be seeing a pretty tight connection between polynomials in $F[x]$ and the natural numbers $\mathbb{N}$. We have a division algorithm, we have a euclidean algorithm, we have primes, factorization. What's another theorem?

Theorem 8.3. *There are infinitely primes in $F[x]$ when F is a field.*

Proof. We'll do this in class but you can do this one yourself! It's almost word for word the same as the proof for the infinitude of prime natural numbers. □

Remark 8.4. Now this is a little silly, for example if we are working with say $\mathbb{Q}[x]$ because if our goal was to come up with infinitely many primes, that would be easy. Here - $x + 1$ is prime, and so is $x + 2$ and so is $x + 3$, etc etc. However, what's great about our setup is that we only used that F was a field. In general, there are lots of weirdo fields - including fields that have only a finite number of elements.

8.2.2 On Fields

Our goal in this section is going to be to crowd-source a definition of a field. We remember that $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, and we remember that our "rough" definition is that a field is a number system where we can add, subtract, multiply and divide (by non-zero numbers). Let's try to make this formal - we want a list of axioms:

I'll start by writing "A set F is called a field if ...":

We'll try to come up with a complete list of the axioms and talk about which ones are more interesting than others.

8.2.3 The Field with 2 Elements

You're probably not too surprised by this, but $\mathbb{Z}/2\mathbb{Z}$ is a field. Indeed, let's check that it satisfies the properties we just agreed upon. (Check). Now let's think about what polynomials look like over this field. Let's write down the constants:

$$0, 1$$

and the linear ones

$$x, x + 1$$

and the quadratic ones

$$x^2, x^2 + 1, x^2 + x, x^2 + x + 1.$$

and so on... We'll do a class exercise to discuss which ones are primes. And we might even true Euclid's algorithm to generate some more primes!

Do a worksheet on finite fields.

What's coming up next? In the next few lectures there are a few things I'd like to develop

1) I'd like us to think about what "unique factorization" should mean? In the next few lectures I'll want us to be able to come up with the right definition of what this should mean - and whether it might be true for $\mathbb{N}$ or $\mathbb{Z}$ or $F[x]$.

2) What are roots of polynomials? What do they have to do with factoring? Are there ways to test if a polynomial factors? Are there ways to tell if it has a root?

3$**$) Homework for Next Class: Explain why $\mathbb{Z}/4\mathbb{Z}$ is NOT a field. I will ask this exact question on the exam. Now it turns out that just because $\mathbb{Z}/4\mathbb{Z}$ isn't a field doesn't mean that there isn't some other field with 4 elements. Maybe there is! Can you come up with it? Hint: To describe a field, you'll just need to give a set and its operations of $+$ and $*$ and illustrate that it has the desired properties. Now you know that every field has to have a 0 and a 1, so those sound like good names for two elements. Now call the other two elements, α and β and see if you can fill in the tables.

9 Week 9

9.1 Monday

9.1.1 Moving forward - Revisiting the gcd

Let's throw out the following question - what is the gcd of 4 and -10? Is it 2 or is it -2? Similarly, what is the gcd of x^2 and $\frac{1}{2}x(x+1)$? Is it x or is it $\frac{1}{2}x$ or $-x$? The answer is that these could all reasonably be called gcds.

Remark 9.1. In the natural numbers, there was no choice of plus or minus, so we could just say "the biggest common factor" but with the integers, or with polynomials, there are more reasonable options. In our class we are mainly going to focus on $\mathbb{Z}$ and $F[x]$ when F is a field.

Definition 9.2. If a, b are in $\mathbb{Z}$ then we say that a is

9.2 Wednesday

10 Week 10

10.1 Monday

10.2 Wednesday

11 Week 11

11.1 Monday

11.2 Wednesday

12 Week 12

12.1 Monday

12.2 Wednesday

13 Week 13

13.1 Monday

Today we'll talk about field extensions and how to build finite fields.

Write on the board: Last time: We proved that if F is a field field, then $|F| = p^n$ for some prime p and a natural number n.

Question: Given such p and n - is there actually a field of order p^n? To answer this question we need to introduce the notice of slightly more generalized clock arithmetic. If F is a field and $f(x)$ is a polynomial then we write $F[x]_{f(x)}$ where we think of polynomials with the *new* relation that $f(x) = 0$. Formally speaking we say that $g(x) = h(x)$ in $F[x]_{f(x)}$ if the difference, $g(x) - h(x)$ is divisible by $f(x)$.

Example 13.1. If we work with $\mathbb{Q}[x]_{x^2-2}$, then we see that the polynomial $x^3 = x(x^2 - 2) + 2x$ so that mod $x^2 - 2$ we have that

$$x^3 = 2x.$$

In fact, since we have the division algorithm it's easy to see that we can always divide any polynomial by $f(x)$ so that each element in $\mathbb{Q}[x]_{x^2-2}$ is equivalent to something of the form $ax + b$.

Example 13.2. Last time we worked with $\mathbb{F}_3[x]_{x^2+1}$. How many elements does this set have?

Example 13.3. What about $\mathbb{F}_7[x]_{x^4}$ how many elements does this have? Is it a field?

Theorem 13.4. *Suppose that $f(x)$ is a polynomial of degree n over a field F. Then the clock $F[x]_{f(x)}$ is a ring consisting of elements:*

$$b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0$$

where $b_i \in F$. If $f(x)$ is a prime polynomial, then $F[x]_{f(x)}$ is a field. is a field with p^n elements. If F is finite with p elements then $F[x]_{f(x)}$ has p^n elements.

Example 13.5. For example, over the field $\mathbb{F}_2$, the polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. Thus if we work with the set

$$\{b_1\alpha + b_0\}$$

where $b_0, b_1 \in \{0, 1\}$, with the rules

$$2 = 0$$

$$\alpha^2 + \alpha + 1 = 0$$

will be a field. Remember to work out multiplication and addition we just use the relation given by $f(\alpha)$ to determine multiplication. This has 4 ($= 2^2$) elements, namely the elements $\{0, 1, \alpha, \alpha + 1\}$.

Example 13.6. On the worksheet, we saw another example where we used the polynomial $f(x) = x^2 - 2$ over the field $\mathbb{F}_3$. This field had nine elements.

Proof. To prove this theorem, let's think about the steps we'd have to show. The associativity, commutativity, and distributive property will all hold because they hold for polynomials. The real work is to show that we have additive inverses, multiplicative and additive identities, that multiplication and addition are well-defined, and that inverses of nonzero elements exist. Talk through most of this.

Caim: Every polynomial has an inverse in this system. Suppose that we have a nonzero polynomial $g(\alpha)$. Well then the gcd of $g(x)$ and $f(x)$ must be 1 (since $f(x)$ is prime. Thus we have that we can write $1 = f(x)p(x) + g(x)q(x)$. So if we plug in α we see that

$$1 = f(\alpha)p(\alpha) + 0$$

in F. Thus we have inverses. □

Remark 13.7. If p is prime and n is any natural number, then there is a field with p^n elements. As we have seen above, to construct this, all we have to do is find an irreducible polynomial over $\mathbb{F}_p[x]$ that has degree n. If you play around, you can convince yourself that this is usually possible.

For example, over $\mathbb{F}_5$ the polynomials

$$x^2 + 2, x^2 + 3, x^2 + x + 1, x^2 + 2x + 4,$$

(and 6 others) are all irreducible polynomials of degree 2. If we used these relations, we would get a field with 25 elements.

It turns out that all of these different fields, are more or less the same. (What this means specifically is that there is a way to relabel all of the elements in such a way that the addition and multiplication tables of any two can be made the same) **Fact: All finite fields with q elements are isomorphic**

Here is a construction that will **always** work to construct a field with $q = p^n$ elements.

1. Work over $\mathbb{F}_p$
2. Factor the polynomial $x^q - x$
3. It is guaranteed to have a prime factor of degree n.
4. Use this factor as your polynomial $f(x)$ to build your finite field.

Example 13.8. Say we want a field with $81 = 3^4$ elements. We will just factor the polynomial

$$\begin{aligned} &x^{81} - x \\ &= x(x^{80} - 1) = x(x^{40} + 1)(x^{40} - 1) \\ &= x(x^{40} + 1)(x^{20} + 1)(x^{20} - 1) \\ &= x(x^{40} + 1)(x^{20} + 1)(x^{10} + 1)(x^{10} - 1) \\ &= x(x^{40} + 1)(x^{20} + 1)(x^{10} + 1)(x^5 + 1)(x^5 - 1) \\ &= x(x^{40} + 1)(x^{20} + 1)(x^{10} + 1)(x^5 + 1)(x^5 - 1) \\ &= x(x^{40} + 1)(x^{20} + 1)(x^{10} + 1)(x^5 + 1)(x - 1)(x^4 + x^3 + x^2 + x + 1) \end{aligned}$$

13.1.1 Adjoining elements to fields, aka field extensions

The main mantra of the previous section was as follows: Take a field, add a new element α to it, and then use a prime polynomial $f(\alpha)$ to allow you to do multiplication. This is an incredibly useful idea, and one that we will study now as our final goal in the course is to study field extensions of the rational numbers.

Recall that if $\alpha \in \mathbb{C}$, we say that α is algebraic if there is a prime polynomial (with leading coefficient 1) $f(x)$ such that $f(\alpha) = 0$. By the remarks above, if we look at the $\mathbb{Q}[x]_{f(x)}$ this will be a field. We call this field $\mathbb{Q}(\alpha)$. But since its elements are just polynomials in α they are complex numbers. So this field lives inside of $\mathbb{C}$. So we have

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{C}.$$

Example 13.9. Suppose that we adjoin $\sqrt[3]{2}$ to the rational numbers: Our goal is to understand

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]_{x^3-2} \subset \mathbb{C}$$

Well what we we have? We have $1, \alpha, \alpha^2$ but $\alpha^3 = 2$, everything in this system can be expressed in degree 2 or lower. For example, we have that $\alpha(\alpha^2 + 1) = 2 + \alpha$.

Or we could also just write that $\sqrt[3]{2}(\sqrt[3]{2}^2 + 1) = 2 + \sqrt[3]{2}$.

Draw the multiplication tables. Do the inverse of $x^2 + 1$.

13.1.2 The degree of a field extension

For the rest of the course we will be interested in field extension of various fields. Let's go back to that example of $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{2}$. This is a field, and every element in it looks like $a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Indeed, the three numbers 1, $\sqrt[3]{2}$ and $c\sqrt[3]{4}$ are all **linearly independent** over $\mathbb{Q}$. Go ahead - try to find a relation amongst them over $\mathbb{Q}$. Why can't you? Well if you did, say you had that $a + b\alpha + c\alpha^2 = 0$ well then α would satisfy a polynomial equation of degree smaller than three - but the characteristic polynomial is supposed to be the only such equation!

Proposition 13.10. *Let $\alpha \in \mathbb{C}$ be an algebraic number. The degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is equal to the degree of the characteristic polynomial of α.*

Example 13.11. Let α be the complex number $(1, 72^o)$. What is its characteristic polynomial? Well $x^5 = 1$ so its is a root of $x^5 - 1$. So we factor and get

$$(x - 1)(x^4 + x^3 + x^2 + 1)$$

The second factor is prime by our work last week.

Example 13.12. Let α be the complex number $(1, 72^o)$. What is its characteristic polynomial? Well $x^5 = 1$ so its is a root of $x^5 - 1$. So we factor and get

$$(x - 1)(x^4 + x^3 + x^2 + 1)$$

The second factor is prime by our work last week. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

Example 13.13. Let α be the complex number $(1, 60^o)$. What is its characteristic polynomial? Well $x^6 = 1$ so it is a root of $x^6 - 1$. In fact, it is a root of $x^3 + 1$ which factor as $x^2 - x + 1$. This is the minimal polynomial of $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

We can do this with other fields as well. For instance, we can look at what happens when we **adjoin** the complex number i to the field $\mathbb{R}$.

$$\mathbb{R} \subset \mathbb{R}(i) \subset \mathbb{C}$$

in this case $\mathbb{R}(i)$ is equal to all of $\mathbb{C}$. On Wednesday we'll see that this is part of a larger story.

13.2 Wednesday

14 Week 14

14.1 Monday

14.2 Wednesday

15 Week 15

15.1 Monday

15.2 Wednesday