MAS114: Numbers and Groups
Semester 1 notes (up to week 11)

Dr James Cranch*

March 19, 2018

Lecture 1

Introduction

Practical arrangements

- There are two lectures a week, at

  Monday 1pm (Dainton LT1)

  and

  Tuesday 1pm (Dainton LT1).

- Notes will be placed online on the course webpage several days before each lecture:

  `http://cranch.staff.shef.ac.uk/mas114/`

- The course webpage also has some practical advice, including on what to do if you miss a lecture.

- Each week you will have a *problem class* (on Thursday or Friday).

- You should find the *homework* online soon after your problem class. You should do these exercises in your own time and hand them in at the next problem class. We will mark them, and return them to you at the beginning of the next problem class. If you'd like more feedback (on any of the solutions), please ask at the problem class.

*J.D.Cranch@sheffield.ac.uk

- The solutions to the *challenge problem* will make their way to me. I'll write up what you've managed.
- I offer *surgery hours* each week. During that time you can come to my office if you need extra help with the lecture material or exercises. These are at:

  Thursday 1pm–2pm

- At the end of this year there will be an exam, covering both semesters' material. This will count for

  80% of the module.

- There will be an *online test* each week, released immediately after Tuesday's lecture and at 2am on Monday (or, if you prefer, very late Sunday night). These will count for

  20% of the module.

- For this course you have *three hours* of contact time per week (two hours of lectures, one hour of problem classes). You're supposed to spend approximately as much time again (three more hours each week) in private study for this course, reading the notes and working on problems.

> If you do not do this, you *will not* be able to catch up in the run-up to the exams.

Things to do if you get stuck:

- Read the notes online.
- Ask your friends.
- Look in books.
- Search the web.
- Ask me.

Things not to do:

- Hope it will sort itself out.
- Leave it until the time of the exam.

What is mathematics?

It's hard to say what maths is. It is rather easier to say a few things about *what mathematics is not*.

> Contrary to popular belief, mathematics is not the study of numbers.

Of course, the study of numbers is:

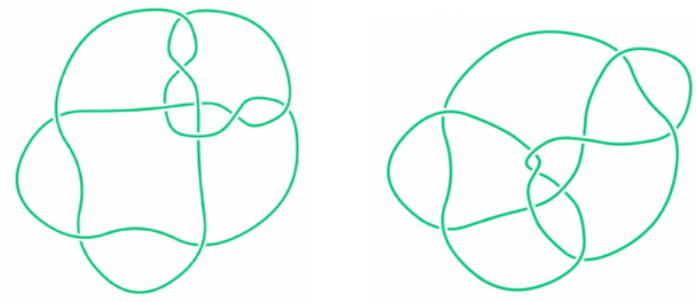
- *part* of mathematics,
- *very useful* in other parts of mathematics, and
- *particularly useful* in applications outside mathematics.

So we'll see lots of stuff about numbers in this course, and in other courses. But what else is there, if it's not all about numbers?

Here are a few pointers. These are just supposed to be a handful of examples rather than a big list of everything!

Ideas of space

Here are two knotted loops of string:



Are they the same? That is, if I had one, could I manipulate it so as to look like the other?

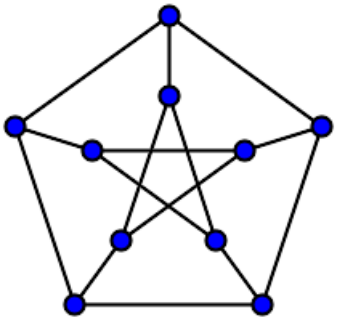
Knot theory — the study of problems just like this — is nowadays a thriving corner of mathematics. But knots are not numbers, and this question is not a question about numbers. Numbers might be useful in solving it, though!

This is just one of many examples of ideas of *space* in modern mathematics.

Ideas to do with space are nowadays of core importance in physics, just as numbers have. The world is made of space with interesting things in, after all.

Ideas of configuration

Is it possible to have a party of ten people, where everyone is a friend or a friend-of-a-friend of everyone else, and where everyone has exactly three friends present?



It's true that the numbers three and ten appear in this problem. But it's not really a problem about numbers: it's a problem about social networks and how they can be configured.

The study of networks (social and otherwise) has become known as *graph theory*. The subject of *combinatorics* encompasses this and many other kinds of configuration problem.

This has great application in computer science: after all, computer networks are examples of networks.

So what is mathematics?

It's hard to say! Perhaps you'll form an opinion yourselves over the next three or four years.

My working definition will be:

> Mathematics is the rigorous study of abstract systems.

Let's look at what that means.

Mathematics deals with simplifications, which are sometimes absurdly unrealistic. Mathematicians talk about a line of length 1, even if there's no ruler able to tell the difference between 0.999 and 1.001. They talk about perfect circles and lines with zero width.

Perhaps paradoxically, it's *because* of the unrealistic simplification that mathematics is able to describe the real world so well.

When mathematics models the behaviour of a spacerocket, treating the rocket as perfectly round and ignoring the dust and the small lumps of bird mess is the the right way to get an answer that's *good enough*.

One has to be very careful, but the abstraction of mathematics has been an amazing tool. For example, it *may be* true that nothing is perfectly round, but many things are so nearly round as to make their real shape irrelevant.

The purpose of choosing an abstraction is to give us something we can be completely certain about.

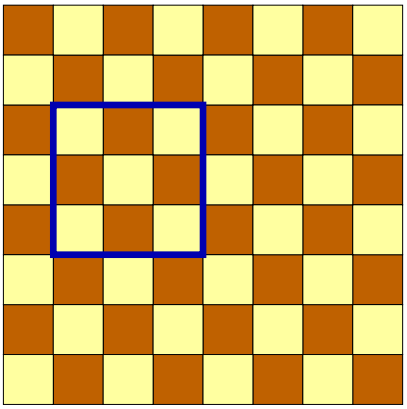
Every move must be fully justifiable (and fully justified, if you're trying to persuade people). There must be no risk of confusion or mistakes.

If we want to take liberties in our arguments then there's not much point in making an abstraction in the first place.

Rigour

Everyone knows that there are 64 squares on a chessboard. After all, chessboards are 8×8 grids, and $8 \times 8 = 64$.

That said, here's a square on a chessboard:



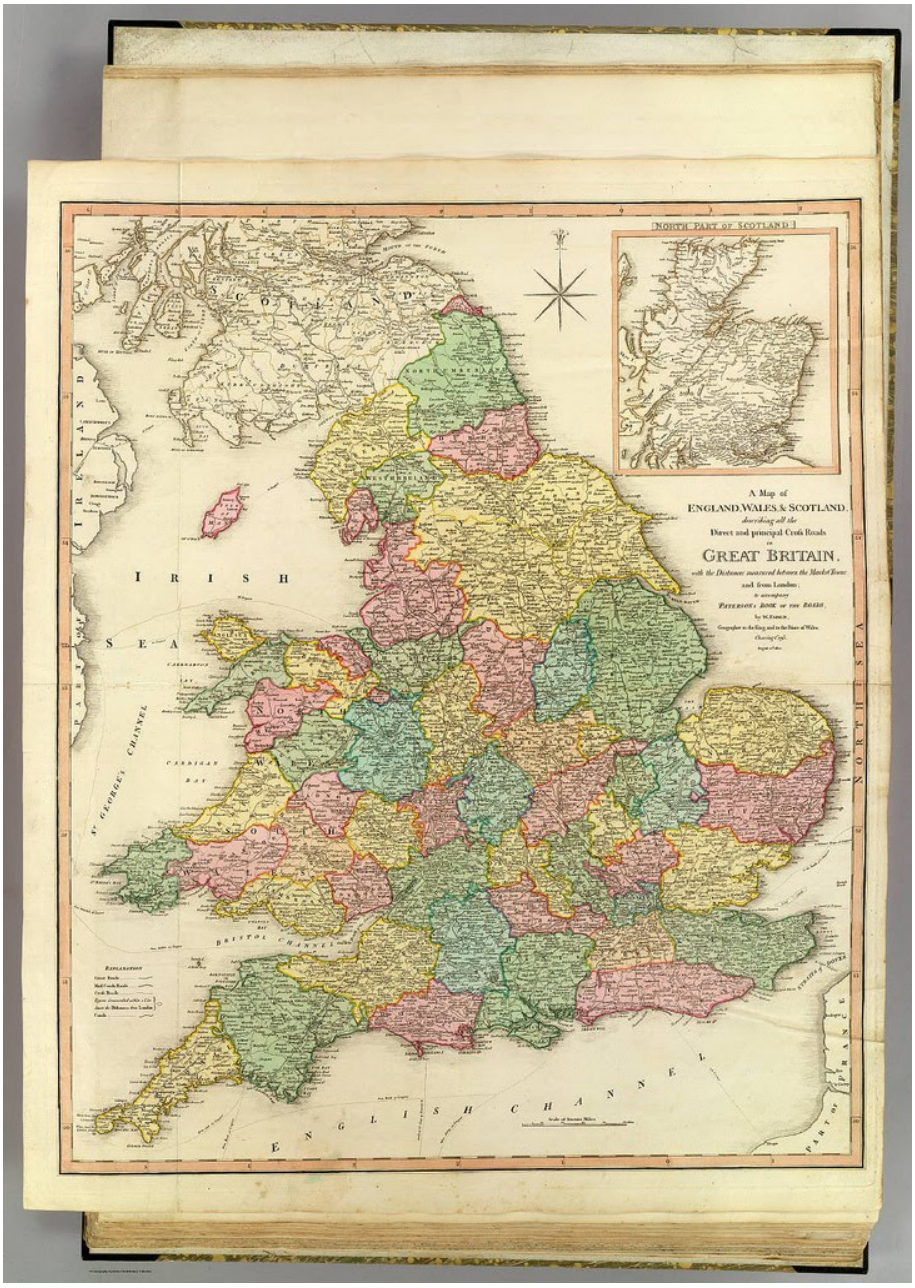
Obviously I've tricked you: I'm using the phrase "square on a chessboard" to mean two different things. But it's a good example of where mathematicians might be careful to be precise, to ensure that no mistakes are made. Things will get more complicated, and the need for care will be greater in future!

Here is a cautionary tale:

- In **1852**, Francis Guthrie asked:

  > Can every map be coloured with *only four colours* so that any two neighbouring regions have different colours?

Here's a vintage map of England and Wales (and, bizarrely, the Isle of Man) coloured in this way:



That's *not a proof*, but it is some evidence that it might be possible.

- In **1879**, Alfred Kempe offered a proof that the answer is *yes*.

- In **1880**, Peter Tait offered another, different, proof that the answer was *yes*. Mathematicians were satisfied, and stopped trying to prove it!
- In **1890**, Percy Heawood pointed out that Kempe's proof contained a big mistake.
- In **1891**, Julius Petersen pointed out that Tait's proof also contained a big mistake. Now, after twelve years spent believing the problem had been solved, and the answer was *yes*, mathematicians realised that in fact, they still had no idea.
- In **1976**, Kenneth Appel and Wolfgang Haken offered a new proof that the answer was indeed *yes*!
- As of **2017**, the argument of Appel and Haken has been checked many times, and is accepted as a complete solution.

The mistakes of Kempe and Tait are not particularly complicated. What caused this 12-year period of confusion was a *lack of sufficient rigour*.

In this course we will learn the basics of correct, logical argument. If you get the right final answer but your justification is incorrect or incomprehensible, you will deserve (and you will probably get) *very few marks*. Kempe and Tait had the right final answer too, but they had no way of knowing that.

At times this may seem like an unnecessary burden: especially when you feel that the right answer is "obvious". However, if you don't spend time in shallow water learning how to swim, you'll never be comfortably able to swim in deep water.

Sets and functions

Having spent the best part of an hour trying to persuade you that mathematics is not about numbers, most of this semester will now be about numbers.

But in order to study them properly, we'll need to start at the beginning, by talking about *sets*.

Sets of numbers

One problem with numbers is that there are several different sorts of them.

We're probably used to several sorts already:

natural numbers

integers

rational numbers

real numbers

complex numbers

We'll go into more detail later in the course.

We often need to say which we mean, in order to avoid confusion and error. For example, it's certainly possible that I might invite 3 friends over for dinner, but it's hard to invite -5 friends or $3/4$ friends or $\sqrt{2}$ friends over.

The natural numbers

The natural numbers are all the numbers you might find by counting.

The set of natural numbers is written $\mathbb{N}$ (that's just a letter N, written in a style called "blackboard bold"); in set notation, we might write

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}\,.$$

That "..." is often pronounced "dot-dot-dot", but it has the meaning of "and so on". When we use this symbol, we must be sure that the reader will be sure *how to go on* from here. Here I hope it really is clear: we go on with 4, 5, 6, adding one each time as we go, and we are to go on without end.

We'll see many more of those curly brackets later! Lecture 2

Actually, some mathematicians use the phrase "natural numbers" slightly differently, to denote the set

$$\{1, 2, 3, \ldots\}\,.$$

In other words, they leave out 0.

Our convention in this module will be that $0 \in \mathbb{N}$: that zero is a natural number.

If we're trying to work inside the natural numbers, we can add and multiply all we want, but subtraction and division are a pain: for example we can't do

$$3 - 5, \qquad \text{or} \qquad 2/7.$$

Working with a bigger system of numbers can cure this.

The integers

The *integers* are all the whole numbers, positive, negative and zero. The set of integers is denoted by $\mathbb{Z}$ (why Z? The German word for "number" is "Zahl"). So we might write

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

Here we have to go on in *both* directions without end.

Every natural number is an integer. This means that

$$\mathbb{N} \subset \mathbb{Z},$$

or, in words, "the set of naturals is contained in the set of integers".

We often use the handy words *non-negative*, meaning "not negative" (in other words, positive or zero) and *non-positive*, meaning "not positive" (in other words, negative or zero).

So the natural numbers are the same thing as the nonnegative integers.

If we're working in the integers, we can add, subtract and multiply all we want. Division is still a problem: for example, we can't do

$$-4/9.$$

The rational numbers

The *rational numbers* (sometimes just called the *rationals*), are the numbers that can be written as fractions $\frac{a}{b}$, where a and b are integers and $b \neq 0$.

Fractions can be written in many different ways: for example, we have

$$\frac{1}{2} = \frac{2}{4} = \frac{5}{10} = \frac{-3}{-6}.$$

In general, fractions $\frac{a}{b} = \frac{c}{d}$ are equal if

$$ad = bc.$$

We write $\mathbb{Q}$ for the set of rational numbers (Q stands for "quotient", which is a name for what you get when you do division).

Of course, any integer n can be regarded as a rational (we can take $\frac{n}{1}$), so

$$\mathbb{Z} \subset \mathbb{Q}.$$

If we're working in the rationals, we can add, subtract, multiply *and* divide all we want. (Well, we can't divide by zero, but who wants to divide by zero?).

There are still many things we might want to do but can't do in the rationals though: square roots, logarithms, trigonometry, and suchlike.

The real numbers

The *real numbers* $\mathbb{R}$ are perhaps the most general sort of numbers you'll have used by now (or perhaps not). They contain lots of the numbers you care about, for example:

$$\pi \in \mathbb{R}, \qquad \log 1729 \in \mathbb{R}, \qquad \sqrt{5} \in \mathbb{R}, \qquad \sin(37^\circ) \in \mathbb{R}.$$

One could define $\mathbb{R}$ as the set of all possible decimal expansions, but there are problems with this:

- It requires some adjustment, because

$$0.999999\cdots = 1.000000\cdots.$$

- Proving things about decimal expansions — even simple things like arithmetic — is a big pain.
- The idea of digits is, mathematically, an unnatural one. It is okay for the way we *write* mathematics to depend on the fact that we have ten fingers, but our *understanding* of fundamental mathematical constructions shouldn't depend on how many fingers we have.

Producing a good and useful definition of $\mathbb{R}$ is quite tricky, and there wasn't one until about 1870. We'll see one later in the course.

Sets in general

Now we have all these collections of numbers, it's good to have a language to discuss them with.

A *set* is a collection of objects. The objects in a set are often called its *elements*.

Given a set S, we write:

- $a \in S$ to mean "a is in S".
- $a \notin S$ to mean "a is not in S".
- $|S|$ to denote the *size* of S: the number of elements in it. (Of course, some sets are infinite, but this works well for finite ones, at least.)

Listing elements

If we have a small set, it might be practical to define it by listing its elements; we do so in curly brackets. Here's an example set:

$$T = \{\text{Tinky Winky}, \text{Dipsy}, \text{Laa-Laa}, \text{Po}\}\,.$$

Let's write some examples of facts about T using our notation:

$$\text{Po} \in T, \qquad \text{Noo-noo} \notin T, \qquad |T| = 4$$

Note that sets don't have any ordering on them. If we find it more convenient to list Teletubbies according to alphabetic order, we can write

$$T = \{\text{Dipsy}, \text{Laa-Laa}, \text{Po}, \text{Tinky Winky}\}\,,$$

and in doing so we are defining exactly the same set T.

Also note that an element is either in a set, or not in it. So we could, if we wanted, define exactly the same set again by writing

$$T = \{\text{Dipsy}, \text{Laa-Laa}, \text{Po}, \text{Po}, \text{Po}, \text{Po}, \text{Po}, \text{Tinky Winky}, \text{Dipsy}\}\,.$$

However, there are few good reasons to write something like that.

Empty sets

The empty set, which could be written $\{\}$, is more commonly written $\varnothing$. It has size given by $|\varnothing| = 0$.

Note that $\varnothing$ is very different to $\{\varnothing\}$. The former, as I mentioned, has no elements; the latter has exactly one element.

That shouldn't confuse you. They're different for pretty much the same reason that "an empty bag" is not the same thing as "a bag which contains an empty bag and nothing else".

Containment

If A and B are sets, we write $A \subset B$ to mean "if x is a member of A then x is also a member of B". We say that A is a *subset* of B, or that A is *contained* in B.

The symbols "$\in$" and "$\subset$" are different, and using the wrong one tends to result in nonsense.

For example, we might write

$$\text{Mathematicians} \subset \text{People},$$

which says "all mathematicians are people". If we used the symbol "$\in$" instead, that would mean that "mathematicians is a person". It's not a mistake you'd make speaking English, and if you're using symbols you should aim to be no less precise.

Notice that, for every set A we have

$$A \subset A \qquad \text{and} \qquad \varnothing \subset A.$$

Set operations

Let A and B be sets. We define their *union* $A \cup B$ to contain exactly the things that are in one set or the other (or both):

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

That notation is called a *set comprehension*: the thing on the left of the vertical bar are the things we want to put in the set, and the things on the right of the vertical bar are the conditions under which we put them in. We'll use them a lot.

Similarly, we define the *intersection* $A \cap B$ to contain exactly the things that are in both sets:

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

Lastly, we define the *difference* $A \backslash B$ to be the things which are in A but not in B:

$$A \backslash B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Equality

Two sets A and B are equal if they have the same members.

A straightforward way of proving this is often to show that $A \subset B$ and $B \subset A$. That is, in words, two sets A and B are equal if every element of A is an element of B and every element of B is an element of A.

Here's an example of this proof strategy:

Proposition 3.1. [1]

[1] In this course, we'll be numbering results by lecture, so that Theorem 15.3 will be the third result in the 15th lecture.

Let A, B and C be three sets. We have

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof. Let's show firstly that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Suppose that $x \in A \cap (B \cup C)$; we must prove that $x \in (A \cap B) \cup (A \cup C)$.

Since $x \in A \cap (B \cup C)$, we have both $x \in A$ and $x \in B \cup C$ by the definition of intersection. But that means that $x \in B$ or $x \in C$, by the definition of union. In either case, the desired result holds:

- If $x \in B$, then since $x \in A$ also, then $x \in A \cap B$, and so $x \in (A \cap B) \cup (A \cap C)$ by the definition of intersections and unions respectively.
- If $x \in C$, then, similarly, since $x \in A$, we have $x \in A \cap C$, and hence $x \in (A \cap B) \cup (A \cap C)$.

So we've proved that containment.

Now let's prove the other containment: namely, that $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Let's suppose accordingly that $x \in (A \cap B) \cup (A \cap C)$; we must prove that $x \in A \cap (B \cup C)$.

Since $x \in (A \cap B) \cup (A \cap C)$, we have either $x \in A \cap B$ or $x \in A \cap C$ by the definition of union. In either case, we get what we want:

- If $x \in A \cap B$, then $x \in A$ and $x \in B$ by the definition of intersection. From the latter, we get that $x \in B \cup C$, by the definition of the union, and hence $x \in A \cap (B \cup C)$ by the definition of intersection.
- If $x \in A \cap C$, then, as before, $x \in A$ but now $x \in C$. However, it's still true that $x \in B \cup C$, and so $x \in A \cap (B \cup C)$. □

That was the first example of a formal proof in this course. You'll have to write many proofs like this yourself, in assessed homework and in the exam. Though we'll discuss it in depth later, it may be worth observing the style from the beginning. One big mistake that many beginner mathematicians make is *not using words to explain the flow of the argument.*

A warning

What we are practising here is called *naïve set theory.* What's so naïve about it?

The Welsh mathematician Bertrand Russell realised in 1901 that there are serious problems with being allowed to form sets carelessly:

Paradox 3.2. *Suppose there is a set S of all sets which are not elements of themselves:*

$$S = \{A \mid A \notin A\}.$$

This creates a contradiction.

Proof. Is S a member of itself? If $S \in S$, then by the definition of S, we have $S \notin S$. On the other hand, if $S \notin S$, then again by the definition of S we have $S \in S$.

□

As a result of this paradox, modern set theorists impose strict rules on what sets can be formed, with the aim of banning this particular beast and everything like it.

However, you probably won't need to worry about this, unless you take a course in set theory later in your mathematical careers.

Functions

A function is to be thought of as a machine that takes an element of one set and gives you an element of another. Here's a formal definition:

Definition 3.3. Given sets A and B, a *function* (sometimes called a *map*) $f : A \to B$ gives for each element $a \in A$ a unique element $f(a) \in B$.

Examples include:

- the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2 - 7$.
- the function $g : \mathbb{Q} \to \{4, 6\}$ defined by

$$g(x) = \begin{cases} 4, & \text{if } x = 3/7 \text{ or } x = -14/17; \\ 6, & \text{otherwise.} \end{cases}$$

The set A is called the *domain* of f, and B is called the *codomain* of f. We call $f(a)$ the *value* of f at a, or the *image* of a under f.

Consider the "age in years" function from the set of people in this room to the natural numbers.

The *domain* of this function is the set of values you're permitted to apply it to. This is the set of people in this room, because I said so.

The *codomain* of this function is the set of values it is *permitted* to take. This is the set $\mathbb{N}$ of natural numbers, because I said so.

Some people like to talk about the *image* of this function, being the set of values it actually takes in practice. This might (perhaps) be the set

$$\{18, 19, 20, 34\}\,.$$

The *range* is not a phrase that's used consistently:

- some people use it to mean the codomain;
- some people use it to mean the image;
- some (confused) people, who don't know the difference, use it inconsistently to mean both.

Lecture 4

When you're trying to work out whether something's a function, there are three bits of the definition where things can go wrong:

"each $a \in A$" A function must be defined for every single element of the domain. Why does $\alpha(x) = 1/x$ not define a function $\alpha : \mathbb{Q} \to \mathbb{Q}$?

α is not defined at zero

"unique element" A function must have only one value at any given element of the domain. If we set $\beta(n)$ to be the real number x whose square is n, why does that not define a function $\beta : \mathbb{N} \to \mathbb{R}$?

$\beta(3)$ could be $+\sqrt{3}$ or $-\sqrt{3}$.

"$f(a) \in B$" A function must return values within its codomain. Why does $\gamma(n) = n - 7$ not define a function $\gamma : \mathbb{N} \to \mathbb{N}$?

$\gamma(4) = -3$ does not lie inside $\mathbb{N}$.

Two functions are equal if:

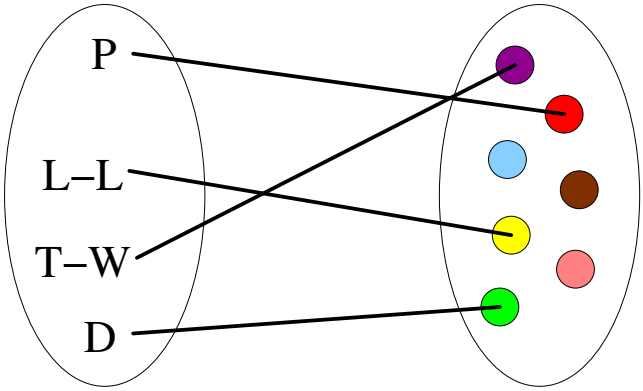
- they have the same domain and codomain, as $f, g : A \to B$; and
- their values are equal, for every point in the domain: in other words, for all $a \in A$, we have $f(a) = g(a)$.

Given two functions $f : A \to B$ and $g : B \to C$, we can define their *composite* $g \circ f : A \to C$ by the rule:

$$g \circ f(x) = g(f(x)).$$

Functions don't have to be described by formulae (as they are in the examples, and non-examples, above).

For example, if the domain is finite we can define them pictorially. Accordingly, here is a function from the set T of Teletubbies, as considered earlier, to the set of colours:



Now we're well-equipped to describe functions, we can start describing their properties.

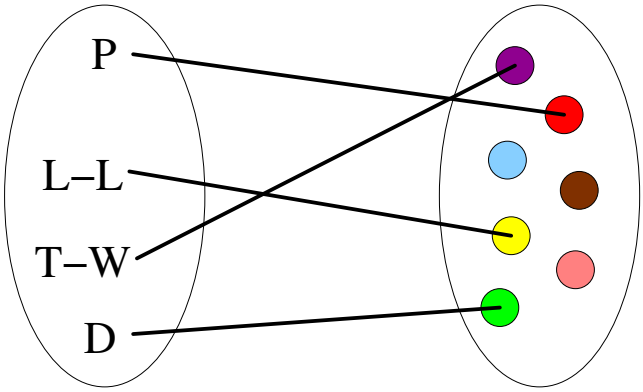
Here are some useful words.

Definition 4.4. A function $f : A \to B$ is said to be *injective* if, for any two elements $a_1, a_2 \in A$ with $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$. I think of this as saying that "nothing is hit twice", or equivalently that "no two elements of the domain have the same image".

Definition 4.5. A function $f : A \to B$ is said to be *surjective* if, for every element $b \in B$, there is some element $a \in A$ with $f(a) = b$. I think of this as saying that "every element of the codomain is hit at least once".

Definition 4.6. A function $f : A \to B$ is said to be *bijective* if it is both injective and surjective. I think of this as saying that "every element of the codomain is hit exactly once".

For example, let's consider our function assigning colours to Teletubbies.



It is is injective, because each one of the Teletubbies has a different colour.

However, it is not surjective, because there are no pink Teletubbies in all of Teletubbyland. Hence it is also not bijective.

Note that these properties (injective, surjective, bijective) don't just depend on the rule that defines it: they depend on the domain and codomain.

For example, consider the rule $f(n) = n^2$. Is this injective, considered as a function $f : \mathbb{N} \to \mathbb{N}$?

Yes! Every natural number has a different square

Is it injective as a function $f : \mathbb{Z} \to \mathbb{Z}$?

No; $f(3) = f(-3)$.

Similarly, consider the rule $g(n) = n + 100$. Is this surjective, considered as a function $g : \mathbb{N} \to \mathbb{N}$?

No; there is no $a \in \mathbb{N}$ with $g(a) = 50$.

Is it surjective as a function $g : \mathbb{Z} \to \mathbb{Z}$?

Yes it is! For any n we have $g(n - 100) = n$.

Remark 4.7. Note that that function also has an *inverse*, a function which undoes g. Namely, we can take the inverse $g^{-1} : \mathbb{Z} \to \mathbb{Z}$ to be $g^{-1}(n) = n - 100$.

You'll see a lot more about inverses next semester.

Logic

Now we'll briefly move on to another building block of mathematics: logic. Logic studies the properties of statements, which can be either *true* or *false*.

Implication

Much of logic involves deductive reasoning. Here's the definition that encapsulates that:

Definition 4.8. Let A and B be statements. We say that A *implies* B, written $A \Rightarrow B$, to mean "if A is true, then B also has to be true".

There are many common ways of saying the same thing, used by mathematicians. These include:

- A implies B;
- $A \Rightarrow B$;
- If A, then B;
- A only if B;
- A is sufficient for B;
- B is necessary for A.

Remark 4.9. Notice that $A \Rightarrow B$ cannot be used to mean "A is true, and so B is also true".

For example, let A be the statement "I visited Cardiff last week", and B be the statement "I've been to Wales this year". We can all agree that $A \Rightarrow B$ is true, which says

> "If I visited Cardiff last week, then I must have been to Wales in the last year."

However, as it happens, neither of these is true: in fact, I haven't been in Wales for more than a year.

As such, it is quite different to saying "A is true, and therefore B is also true". Beginning students often get these confused.

Lecture 5

Remark 5.10. The implication $A \Rightarrow B$ only says something interesting about B if A happens to be true! If A is false, then we have $A \Rightarrow B$ no matter whether B is true or false.

For example, it's correct to say

> "If $2 + 2 = 337$, then this course is lectured by Dr Cranch".

This may be a surprise if you're basing your intuition on ordinary English, where people use the words "if... then" in several different ways, sometimes slightly ambiguously.

Remark 5.11. Another important point is that if $A \Rightarrow B$ does not say that B is true *only* if A is true (that would be $B \Rightarrow A$, in fact).

So it's correct to say

> If it rains next Wednesday, then $2 + 2 = 4$.

In fact, it's true that $2 + 2 = 4$ no matter whether it rains next Wednesday, but that's not a problem. Whether or not it's *helpful* to say that is another question!

We can sum up the comments above by giving a *truth table* for implication. We write 0 for false and 1 for true.

First off, note that if Q is true, then $P \Rightarrow Q$ is definitely true no matter whether P is true.

Also, if P is false, then $P \Rightarrow Q$ is true no matter whether Q is true.

In fact, it's only if P is true and Q is false that $P \Rightarrow Q$ is false.

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

We've seen in the above, that $A \Rightarrow B$ and $B \Rightarrow A$ are different statements. It's helpful to have a word relating them:

Definition 5.12. Consider a statement of the form $A \Rightarrow B$. Then the *converse* of that statement is the statement $B \Rightarrow A$.

The truth of an implication has very little to do with the truth of its converse, as we'll see.

Example 1. Let P be the statement "X lives in England" and Q be the statement "X lives in Sheffield".

Is the statement $P \Rightarrow Q$ always true?

> No. (X could live in Newcastle.)

Is its converse always true?

> Yes, it is.

Example 2. Let C be the statement "Y is English", and let D be the statement "Y lives in Sheffield".

Is the statement $C \Rightarrow D$ always true?

No. (Y could live in New York.)

Is the converse always true?

No. (Y could be German.)

Equivalence

Equivalence is the relationship between two statements of being both true, or both false.

Definition 5.13. Let P and Q be statements. We write $P \Leftrightarrow Q$, pronounced "P is equivalent to Q" for the statement that P is true if and only if Q is true.

Sometimes people shorten "if and only if" to "iff".

Negation

Negation is a type of opposite:

Definition 5.14. Let P be a statement. The *negation* of P, written $\neg P$ and often pronounced "not P", is the statement "P is false".

Remark 5.15. We must be careful in thinking of negation as an opposite. For example, the negation of "Richard is happy" is "Richard is not happy".

Most people would say that the "opposite" is "Richard is sad". That's not quite the same thing!

Similarly, the negation of "Alice is in front of Bob" is not "Alice is behind Bob", but:

"Alice is not in front of Bob".

Note that double negation doesn't do anything: the statement $\neg(\neg P)$ is equivalent to P. Since statements are either true or false, if it's not "not true", it's true.

The negation allows us to make sense of something very important about implication:

Definition 5.16. Consider a statement of the form $P \Rightarrow Q$. Its *contrapositive* is the statement $(\neg Q) \Rightarrow (\neg P)$.

The main useful fact about the contrapositive is that it's equivalent to the original implication. This is something very familiar from everyday life. If my friend Mel says

"If I can come visit you this evening, then I'll text you at lunchtime,"

then I might rephrase it to myself as:

"I don't get a text at lunchtime, then Mel won't visit this evening."

But here's a formal statement and proof, anyway:

Proposition 5.17. *Let P and Q be statements. The statement $P \Rightarrow Q$ is equivalent to its contrapositive $(\neg Q) \Rightarrow (\neg P)$.*

Proof. I'll prove this using a truth table, showing what happens in all possibilities.

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

We now provide a table for $(\neg Q) \Rightarrow (\neg P)$ (using the table above to fill in the implications):

P	Q	$\neg Q$	$\neg P$	$(\neg Q) \Rightarrow (\neg P)$
0	0	1	1	1
0	1	0	1	1
1	0	1	0	0
1	1	0	0	1

The reader can see from this that $(\neg Q) \Rightarrow (\neg P)$ is true exactly when $P \Rightarrow Q$ is, and this proves that they're equivalent.

□

"And" and "Or"

There are other ways to combine statements, other than implication:

Definition 5.18. Let P and Q be statements. The statement $P \wedge Q$, pronounced "P and Q", is the statement that both P and Q is true.

The statement $P \vee Q$, pronounced "P or Q", is the statement that at least one of P or Q (and possibly both) is true.

We can make truth tables for both of them:

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

Remark 5.19. While you're all used to these words from everyday life, there can be vagueness about how "or" is used in English.

For example,

I'll have my pie with chips or I'll have it with mashed potatoes.

is probably intended to mean "but not both". In mathematical argument when we use "or" and mean "but not both", we have to say so explicitly.

It is sometimes worth knowing that implication can be defined in terms of "or":

Proposition 5.20. *The statement $P \Rightarrow Q$ is equivalent to $(\neg P) \vee Q$.*

Proof. The only way that the first statement can be false is if P is true and Q is false. But that's also the only way that the second statement can be false, so they're equivalent. □

Note that that shows another style of proof of logical statements: by analysis rather than the "case bash" used in truth tables.

Quantifiers

Lastly, we need to discuss how to make statements about *general* situations and *particular* examples. The phrases we use again and again are "for all" and "there exists": these are called *quantifiers*.

The following symbols are in common use:

$\forall$	for "for all";
$\exists$	for "there exists";
s.t.	for "such that".

So, for example,

$$\forall n \in \mathbb{N}, \quad n^2 - 1 = (n+1)(n-1)$$

is to be read as

"For all natural numbers n, we have $n^2 - 1 = (n+1)(n-1)$."

And

$$\exists x \in \mathbb{R} \quad \text{s.t.} \quad x^2 - 3x - 12 = 0$$

is to be read as

"There exists a real number x such that $x^2 - 3x - 12 = 0$."

It's important that you get used to this notation. This is not because there is anything amazing about it, but because mathematics involves lots of general rules and particular examples: much of the mathematics you do for the next few years will require you to be able to deal with these things.

One thing you'll have to get used to is situations with two or three quantifiers. These happen very frequently: "in general, there is always a particular example of such-and-such", or "there is a particular amazing example which has the general property of such-and-such".

For example, the statement

$$\forall n \in \mathbb{N}, \quad \exists x \in \mathbb{R} \quad \text{s.t.} \quad x^2 = n$$

says that every natural number n has a square root x. Lecture 6

Remark 6.21. The order of quantifiers is very important. If we swap over the two quantifiers in the last example, we get

$$\exists x \in \mathbb{R} \quad \text{s.t.} \quad \forall n \in \mathbb{N}, \quad x^2 = n.$$

This says that there's a particular number x which has the property that x is the square root of *every natural number*. And that's nonsense.

Another thing that mathematicians have to do every day is understanding how negation interacts with quantifiers.

The negation of "all Teletubbies are red"is "not all Teletubbies are red", which is equivalent to "there exists a Teletubby which is not red".

Similarly, the negation of "there exists a dolphin who likes Beethoven"is "there does not exist a dolphin who likes Beethoven",and that's equivalent to "all dolphins do not like Beethoven".

In symbols,

$$\begin{array}{rcl} \neg\,(\forall x \in X, \quad P(x)) & \text{is equivalent to} & \exists x \in X \quad \text{s.t.} \quad \neg P(x). \\ \neg\,(\exists x \in X \quad \text{s.t.} \quad P(x)) & \text{is equivalent to} & \forall x \in X, \quad \neg P(x). \end{array}$$

Perhaps you may want to remember that "negation swaps $\forall$ and $\exists$." But being able to *do it correctly by remembering what's going on* is much more

important than remembering a slogan. After a while it should come to seem natural.

Suppose I am wondering whether all fish are slippery. If it's true, I need to find some general reason why *every single* fish is slippery. If it's false, I only need to find *one single* fish which isn't slippery, and then I've proved it.

In general, if you have a general statement and you don't know if whether it's true or false, then it could either be:

- *true*, in which case you need to prove it in general (that's a statement with a "$\forall$" in);
- *false*, in which case you need to find a counterexample (that's a statement with a "$\exists$" in).

Induction

The basics of induction

The most obvious interesting thing about the natural numbers is that it's natural to start listing them, one after the other:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

This, of course, is how *counting* works.

It turns out that this way of thinking about the integers gives us a very powerful tool for proving things one integer at a time: the *principle of mathematical induction*, usually known to mathematicians simply as *induction*.

Informally, I like to think of the following example:

> *If* I can reach the bottom (rung number zero?) of a ladder, *and* if I'm on any rung I can reach the next rung up, *then* I can reach any rung on the ladder.

Why, for example, can I reach the fourth rung? One can imagine a detailed proof of this, as follows:

- I can reach rung zero;
- Because I can reach rung zero, I can reach rung one;
- Because I can reach rung one, I can reach rung two;
- Because I can reach rung two, I can reach rung three;

- Because I can reach rung three, I can reach rung four.

The connection with counting is obvious: our proof visibly counts up to four.

Writing that out was okay, but you are probably glad I didn't write out a proof that we could reach the hundred and seventy-eighth rung. I suppose that we could do so, writing "and so on" at some point: but that's a little vague (what about situations where it isn't obvious what "and so on" means)?

It's helpful to have a way which isn't vague.

So here's a formal version:

Definition 6.22 (Induction)**.** Let $P(n)$ be a statement that depends on a natural number n. Then, if

(i) the statement $P(0)$ is true, and

(ii) for all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true,

then the statement $P(n)$ is true for all $n \in \mathbb{N}$.

Here are some useful words:

Remark 6.23. We call part (i) the *base case*, and part (ii) the *induction step*. These words agree quite well with our mental picture of a ladder!

When we are trying to prove the induction step $P(k) \Rightarrow P(k+1)$ we refer to $P(k)$ as the *induction hypothesis*.

Example of induction

We'll prove many things by induction in this course, but this is one:

Proposition 6.24. *For any natural number n, we have the following formula for the sum of the first n positive integers:*

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

Let $P(n)$ be the statement above for some particular n.

So $P(3)$ is the statement that says $1 + 2 + 3 = 3 \times 4/2$, and $P(10)$ is the statement that

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = (10 \times 11)/2.$$

Notice that $P(n)$ is *not a number*, it's a *statement*.

Proof. We will prove $P(n)$, which says that

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

for all n by induction.

For our base case, $P(0)$ says that the sum of *no integers at all* is $0 \times 1/2$, which is true, as the sum of no integers is zero.

Now we will do our induction step, proving $P(k) \Rightarrow P(k+1)$ for all k. Suppose $P(k)$ is true: we need to show that $P(k+1)$ is true.

The statement $P(k)$ tells us that

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

We need to prove $P(k+1)$, which would say that

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

Now note that

$$\begin{aligned}
& 1 + 2 + \cdots + (k-1) + k + (k+1) \\
= \; & (1 + 2 + \cdots + (k-1) + k) + (k+1) \\
= \; & \tfrac{k(k+1)}{2} + (k+1) \quad \text{(by the induction hypothesis)} \\
= \; & \tfrac{k(k+1)+2(k+1)}{2} \\
= \; & \tfrac{(k+1)(k+2)}{2}.
\end{aligned}$$

This is exactly the statement $P(k+1)$, which is what we needed for the induction step, and that completes the proof.

□

Remark 6.25. You may know other ways of proving that. (I can think of a few.) But I hope you're impressed with this as a strong potential method for proving identities.

Nonexamples of induction

Let's now try proving some *completely false* statements using induction. The plan is (of course) not to succeed, but to understand where we need to be careful.

Example 3. We'll try proving using induction that for all n, we have

$$n = n + 83.$$

Clearly this statement is complete and utter rubbish.

> If you believe that induction is a reliable method of proof (and I do, and I hope you do too), then it had better be the case that we're not using induction correctly.

Anyway, here's an induction "proof". Suppose that $k = k + 83$ for some k. We'll prove that $(k + 1) = (k + 1) + 83$. But we have

$$\begin{aligned} k + 1 &= (k + 83) + 1 && \text{(by assumption)} \\ &= (k + 1) + 83 && \text{(by rearrangement).} \end{aligned}$$

This completes the proof.

What's the problem with the argument above?

There's no base case.

If you don't have a base case, such as $P(0)$, then it's of no use to prove that $P(k) \Rightarrow P(k + 1)$ for all k. It's no use to be able to climb a ladder if the bottom of the ladder is unreachable.

Lecture 7

Here's another, more subtle example:

Example 4. We'll try proving using induction that all horses are the same colour.

> Again, we find ourselves hoping very strongly that there's a mistake in the use of induction in what follows. I'll write it out and we can see if we can spot it.

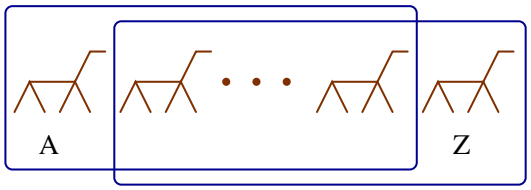
In order to do this, we'll let $P(n)$ be the statement "Given any n horses, all of them have the same colour". We'll prove $P(n)$ for all n by induction: that will give us what we want, because we can take n to be the number of horses in the world.

We'll take $P(1)$ as the base case of the induction. This is the statement "Given any one horse, all of them have the same colour": this is obviously true.

Now we'll prove the induction step. We will assume that $P(k)$ is true ("given any k horses, all of them have the same colour"): our job is to prove

that $P(k+1)$ is true ("given any $(k+1)$ horses, all of them have the same colour").

So suppose we have $(k+1)$ horses. Name two of them Alice and Zebedee.



Excluding Alice, there are k horses, which all have the same colour, by the induction hypothesis. So all the horses except Alice have the same colour as Zebedee.

Also, excluding Zebedee, there are k horses, which all have the same colour, again by the induction hypothesis. So all the horses except Zebedee have the same colour as Alice.

Hence all the horses except Alice and Zebedee have the same colour as both Alice and Zebedee, which says that all the horses have the same colour. That ends the proof.

What's wrong with this?

The particular case $P(1) \Rightarrow P(2)$ doesn't work.

I find this surprisingly subtle.

In fact, it's a parody of a *valid* style of argument. If it is the case that *any two things are the same*, then we could prove using exactly this method that they're *all the same*. In fact, this is something you already know, since "all are alike" and "no two differ" are synonymous phrases.

Variants

There are other techniques which use the same *idea* of induction, but not quite the same formal principle as I've written out above.

We can start with a base case which isn't $P(0)$. For example, if

(i) $P(15)$ is true, and

(ii) $P(k)$ implies $P(k+1)$ for all $k \geqslant 15$,

then $P(n)$ is true for all $n \geqslant 15$.

Perhaps you want to think of that as saying "if have a door which leads to the fifteenth rung of a ladder, and you know how to climb ladders, then you can get to every rung above the fifteenth".

Actually, this is really just ordinary induction in disguise.

Indeed, if we define $Q(n)$ to be $P(n+15)$, then proving $Q(n)$ for all $n \in \mathbb{N}$ by induction is the same as proving $P(n)$ for all integers $n \geqslant 15$.

Perhaps you want to think of that as "ignoring all the bits of the ladder below the fifteenth rung, imagining the ladder starts outside your door, and starting counting rungs from there". Or perhaps you're bored of the ladder analogy now.

Actually, you should have been prepared for this variant: my induction proof that "all horses have the same colour" started with 1, not 0. (Okay, that proof was wrong. But there was nothing wrong with *that bit* of the proof: there's nothing wrong with induction starting from 1. It was something else that was wrong).

Another common variant is known as *strong induction*. This allows you to assume all previous cases in your induction step, rather than just the last one.

It looks like the following:

Definition 7.26 (Strong induction)**.** Let $P(n)$ be a statement that depends on a natural number n. Then if

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

(ii) for all k, if $P(0), P(1), \ldots P(k)$ are all true, then $P(k+1)$ is also true,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Again, this can be viewed as a cleverly disguised version of ordinary induction: if we define the statement $Q(n)$ as follows:

$$\begin{aligned} Q(n) &= P(0) \wedge P(1) \wedge \cdots \wedge P(n-1) \wedge P(n) \\ &= \text{"all the statements } P(0), \ldots, P(n) \text{ are true"}, \end{aligned}$$

then proving $Q(n)$ by ordinary induction works out to be effectively the same thing as proving $P(n)$ by strong induction.

Indeed, the base case $Q(0)$ is the same thing as the base case $P(0)$. The induction step $Q(k) \Rightarrow Q(k+1)$ looks like

$$P(0) \wedge \cdots \wedge P(k) \Rightarrow P(0) \wedge \cdots \wedge P(k) \wedge P(k+1).$$

In order to prove this, we assume $P(0), \ldots, P(k)$ are all true and have to prove that $P(0), \ldots, P(k+1)$ are all true. But then all of these except the last

are assumptions: what is left is to prove $P(k+1)$ assuming $P(0), \ldots, P(k)$, and that's exactly the induction step of a strong induction.

Here's an example of strong induction in practice. First we'll need a definition:

Definition 7.27. The *Fibonacci numbers* $F_0, F_1, \ldots$ are defined by taking $F_0 = 0$ and $F_1 = 1$, and then for $n \geqslant 2$ by

$$F_n = F_{n-1} + F_{n-2}.$$

Now for the result in question:

Proposition 7.28. *For all $n \in \mathbb{N}$ we have $F_n < 2^n$.*

Proof. Let $P(n)$ be the statement $F_n < 2^n$. We know that $P(0)$ is true, since

$$F_0 = 0 < 1 = 2^0.$$

We also know that $P(1)$ is true, since

$$F_1 = 1 < 2 = 2^1.$$

Now we'll show that for all $k \geqslant 1$ we have that if $P(0), \ldots, P(k)$ are all true, then $P(k+1)$ is true. So suppose that $P(0), \ldots, P(k)$ are all true.

We now have that

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} \\ &< 2^k + 2^{k-1} \qquad \text{(using } P(k) \text{ and } P(k-1)\text{)} \\ &< 2^k + 2^k \\ &= 2^{k+1}, \end{aligned}$$

which is exactly $P(k+1)$. This completes the induction step, and so finishes the proof.

□

That strong induction argument really had *two base cases* before the induction step.

So we proved $P(0)$, and we proved $P(0) \Rightarrow P(1)$ by proving $P(1)$, and then we proved $P(0) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$ by proving $P(k-1) \wedge P(k) \Rightarrow P(k+1)$.

I like to think that the proof was arranged according to the shape of the definition of the Fibonacci numbers: that definition has two base cases $F_0 = 0$ and $F_1 = 1$, and a step $F_{n+2} = F_{n+1} + F_n$. This is not a rare coincidence.

Why induction works

In this section we make a few comments on why induction works. They may be helpful in thinking about when you can and when you can't generalise induction to other settings.

Let's introduce a definition:

Definition 7.29. A set (of numbers) is *well-ordered* if every nonempty subset has a least element.

For now, our main use of that is to say this:

Definition 7.30. The *well-ordering principle for* $\mathbb{N}$ says that $\mathbb{N}$ is well-ordered.

This is a very special property of $\mathbb{N}$. The integers $\mathbb{Z}$, for example, are not well-ordered. Indeed, the subset $\mathbb{Z} \subset \mathbb{Z}$ of all integers does not have a smallest element: there is no smallest integer.

The main interest is this:

Theorem 7.31. *The well-ordering principle for* $\mathbb{N}$ *and the principle of strong induction(Definition 7.26) are equivalent.*

Proof. We'll show first that we can derive the principle of strong induction from the well-ordering principle.

So suppose we had a statement $P(n)$ for each $n \in \mathbb{N}$, and we had a base case (that $P(0)$ was true) and an induction step (that, for all $k \in \mathbb{N}$ if we have $P(i)$ for all $i < k$, we also have $P(k)$). We need to show that $P(n)$ is true for all n.

We might argue as follows. Let A be the set of natural numbers n for which $P(n)$ does not hold:

$$A = \{n \in \mathbb{N} \mid \neg P(n)\}\,.$$

So A is the set of "counterexamples".

If A has any elements at all, it has a smallest element a. But a can't be 0, because we have $P(0)$. But a can't be bigger than 0 either: because a is minimal, we have $P(i)$ for all $i < a$. Hence we have $P(a)$ also, by the induction step. But that's a contradiction: we assumed that $\neg P(a)$.

Hence A doesn't have any elements, which is the same as saying that $P(n)$ holds for all n.

Now we'll show the other half of the equivalence: that we can derive the well-ordering principle from the principle of strong induction.

Let $Q(n)$ be the statement, "any subset of $\mathbb{N}$ which contains n has a smallest element". We'll prove $Q(n)$ for all n by strong induction.

Firstly, for a base case, we must prove $Q(0)$ ("any subset of $\mathbb{N}$ which contains 0 has a smallest element"). This is clearly true, as 0 is the smallest natural number of all, so any such subset has 0 as its smallest element.

Now we must prove the induction step: we assume for some k that $Q(i)$ is true for all $i < k$, and we prove that $Q(k)$ is true. Consider a subset $S \subset \mathbb{N}$ which contains k. If it contains some element $i < k$, then by $Q(i)$ it has a least element. If, however, it contains no element $i < k$, then k is its least element: so in particular, it has a least element. This proves $Q(k)$.

Hence we have $Q(n)$ for all n by strong induction. So if S is a nonempty subset of $\mathbb{N}$, it has at least one element: call it n. But then by $Q(n)$, the set S has a least element: this proves the well-ordering principle.

□

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers. Whenever you find a well-ordering, you get a notion of induction for free.

For example, consider the set of pairs (m, n) of naturals, where we say that $(m, n) < (m', n')$ if $m < m'$, or if $m = m'$ and $n < n'$. (This is called the *lexicographic* ordering, because it's inspired by the way that words in dictionaries are ordered).

It is not too hard to prove that that is well-ordered: any set of pairs of natural numbers has a "least" element with respect to this ordering. Hence we can do (strong) induction on pairs of naturals! Lecture 8

Advice on writing proofs

In this section I simply give a few thoughts on how to write a good proof.

Think of it as a literary form

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

If you see a proof which you consider to be particularly well written, try to *learn from it* as an example of what's good to do. Similarly, if you see a proof which you consider to be particularly badly written, maybe you can learn something from the experience about what to avoid!

Also, *read it back* to yourself (or better yet, get a colleague to read it). You're writing it so others can read: it's good to test it to make sure this is possible. This goes particularly for proofs containing large amounts of symbols: these can be very hard to read, and reading it back to yourself is probably the best way of detecting this.

Use words and symbols

A common mistake that beginners make is to use very few words at all. Words are fantastic for *explaining* what you're doing.

In particular, too many people overuse the symbol "$\therefore$" (meaning "therefore"), and the symbol "$\because$" (meaning "because"). I won't use them at all in my proofs in these notes. There are so many good phrases which do its job, and choosing one helps you write what you're actually thinking. Also, it distracts the reader's eye from the symbols which matter — the actual maths you're doing — to things which don't.

Here are some phrases which do the job of "$\therefore$":

> so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, ...

Here are some which do the job of "$\because$":

> because, since, as a result of, as we have, as we know, as we have seen that, because we saw, ...

On the other hand, if you do write words, don't write them all in one paragraph. Try to write in a structured fashion, and if you are producing paragraph after paragraph after paragraph, ask yourself if you could use symbols to make your life easier in places.

The clearest pieces of mathematical writing I've read often make good use of words and symbols, working together.

When it's really important, I like to use both to make sure the point is clear. I might write,

> Let $A = \sum_{i=1}^{n} a(i)$ be the sum of the first n values of a, and let $p > A$ be a prime number greater than A.

Make the structure obvious

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:
  - use words which introduce a change of pace ("now we do this...");
  - name or number something earlier, and refer back to it by name or number;
  - leave a paragraph break;
  - leave a space;
  - have a descriptive section heading.

It is particularly important to avoid unstated assumptions.

For example, if a proof contains an assertion that some construction is a function, then the definition of a function gives you some things to check: that *every* element of the domain gives a *unique* element lying *inside* the codomain. Unless they're obviously true, it could be that these checks are the hardest and most interesting part of the proof. They could even be lies.

Explain beforehand and afterwards

Here is a classic account of a public speaking strategy:

> First I tell them what I'm going to tell them. Then I tell them. And then I tell them what I've told them.

This approach is even better in proofs than it is in public speaking.

Some explanation at the beginning is important. It may well be that your reader doesn't know even what you're aiming to do, and it's even more likely that your reader doesn't know how you're planning to do it.

Also, some explanation at the end is important. When you reach a conclusion, why do you think that what you have written actually means you have finished the proof?

If the proof is long, then regard it as being made of several parts. Give each part an explanation when you start and when you finish it.

I quite like proofs with the following kind of framework:

We'll prove this by induction on n.

The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.

Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$. So we're assuming that blah blah blah, and have to prove that blah blah blah.

But blah blah blah blah blah. Also, blah blah blah blah blah. So, in conclusion, blah blah blah, which is what we had to prove. That finishes off the induction step, and so completes the proof.

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so...

This was a very efficient process for working out what time to do everything (much better than trial and error, where you repeatedly guess times to leave your house, working out when you arrive). But the paragraph above is a terrible set of instructions for someone else who wants to get from Sheffield to Guernsey: it's *backwards*.

It's the same with proofs: when you write them down, you're supposed to *finish* with the result you're trying to prove, and on the way things are supposed to follow from your assumptions and the things you said earlier.

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal. In proofs later in this course I'll sometimes try to talk you through how you'd think about it.

A very common sign you're going the wrong way is when you finish up with something obvious (like $1 = 1$).

This is especially bad when you mix forwards and backwards reasoning, and what you're writing is likely to be *badly wrong* in this situation. For example, we could prove $9 = 11$ as follows: subtract 10 from both sides to get $-1 = 1$, and then square both sides to get $1 = 1$. This is true, so we're done.

Here's an example of weird backwards reasoning: earlier in the course we

had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\begin{aligned}
\frac{k(k+1)}{2} + k + 1 &= \tfrac{(k+1)(k+2)}{2} \\
k(k+1) + 2k + 2 &= (k+1)(k+2) \\
k^2 + k + 2k + 2 &= k^2 + k + 2k + 2 \\
k^2 + 3k + 2 &= k^2 + 3k + 2, \qquad \text{which is true!}
\end{aligned}$$

How could we mend this? There are several ways:

Just write it backwards,

but it would perhaps be better to

Simplify both sides to $\frac{k^2+3k+2}{2}$.

Help your reader

It is often well worthwhile supplying an example or a diagram. If your proof depends critically on it, on the other hand, you are probably not supplying enough information. But it's quite sensible to use an example or a diagram as an aid.

Let the proof fit the statement

This is perhaps my vaguest (but perhaps also my most helpful) piece of advice.

Often (but not always) it's possible to guess what a proof will look like, at least roughly, based on the appearance of the thing you're trying to prove. Don't try to fight it.

Here are some examples:

- If you're trying to prove $P \wedge Q$, you're likely to prove P and then prove Q.
- If you're trying to prove $P \vee Q$, you're likely to prove P or prove Q (after fiddling around to try to see which of those is easiest).

- If you're trying to prove something of the form $P \Rightarrow Q$, your proof is likely to start with "We'll assume P" and to continue by deducing Q.

- If you're trying to prove something of the form $\forall x \in X, \quad P(x)$, your proof is likely to start "Let x be an element of X" and then continue by proving $P(x)$.

- If you're trying to prove something of the form $\exists x \in X \quad \text{s.t.} \quad P(x)$, your proof is likely to start by giving one particular (cleverly chosen) value of x, and then proving that $P(x)$ is true of it.

- If you're trying to prove something about a sequence with a recurrence relation, your proof may well be by an induction, where the induction step refers to the same previous cases as the recurrence relation.

Elementary Number Theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.

This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Remark 8.32. In the sense that mathematicians use the word, "elementary" doesn't mean "easy": it means "using no deep theory" (we're only four weeks into your first semester, so haven't had time to develop any deep theory). It can still be difficult, and in fact it can still be deep.

Divisibility and primes

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!

Here's the basic definition:

Definition 8.33. Let a and b be integers. We say that a *divides* b if there exists an integer n such that $an = b$.

We also might say that b *is a multiple of* a, or that a *is a divisor of* b, or that a *is a factor of* b, or that a *goes into* b.

In symbols, we write $a \mid b$ to say that a divides b, and write $a \nmid b$ to say that a does not divide b.

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.

However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark 8.34. What does it mean to say that a does not divide b? Well, it means:

> there does not exist any integer n, such that $an = b$,

or (equivalently)

> for all $n \in \mathbb{Z}$, we have $an \neq b$.

Lecture 9

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

- When do we have $a \mid 1$?

  When $a = \pm 1$.

- When do we have $1 \mid b$?

  Always (since $1b = b$ for all b).

For the next few lectures, we'll be studying the integers from the point of view of divisibility.

The following definition is a natural one:

Definition 9.35. An integer $p > 1$ is said to be *prime* if it has no positive factors except for 1 and p itself.

Primes are clearly a good thing to study: they're the numbers with no complicated factors.

It's good to have a word meaning roughly the same thing as "not prime":

Definition 9.36. An integer $n > 1$ is said to be *composite* if it is not prime: that is, if it does have positive factors other than 1 and n.

Remark 9.37. Notice that we have chosen our definitions so that 1 will be neither prime nor composite. This was a choice, and it seems a bit mysterious at first.

Indeed, until the late 19th century, mathematicians treated 1 as prime. But it was found to be so much simpler to do it this way that nobody considers 1 to be prime any more.

The main thing about primes is that all other positive integers are built from them by multiplication:

Theorem 9.38. *Every positive integer n can be written as a product of primes (in at least one way).*

Proof. We'll prove this by strong induction on n.

For our base case, we observe that when $n = 1$, we can write n as the product of no primes at all. (A product of no numbers at all is 1. You know that already: for example, 2^0 is the product of no 2s, and you know that that is 1).

So now we have to do our induction step: let k be a positive integer. We assume that every positive integer i with $1 \leqslant i \leqslant k$ can be written as a product of primes, and we try to prove that $(k + 1)$ can.

Now, either $(k + 1)$ is prime, or it is composite. If it is prime, then $(k + 1)$ is the product of just one prime (namely, $(k + 1)$ itself).

If, however, $(k+1)$ is composite, then it has a positive integer factor a which is not 1 nor $(k + 1)$ itself: in other words, we have

$$k + 1 = ab,$$

where both a and b are between 1 and $(k + 1)$.

By the strong induction hypothesis, that means that a and b can both be written as products of primes, say:

$$a = p_1 p_2 \cdots p_m, \quad \text{and}$$
$$b = q_1 q_2 \cdots q_n.$$

But then we have

$$k + 1 = ab = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n,$$

which proves it for $(k + 1)$. That completes the induction step (and the proof). □

Remark 9.39. Later on, we'll prove a stronger result, that every number can be written as a product of primes in *exactly* one way (rearranging the factors doesn't count). That's much, much harder.

Because of this we can be sure that primes are reasonably important. The first few are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

What are sensible questions to ask? Here are some obvious examples:

(a) How many primes are there?

(b) There's quite a lot of primes between 1 and 50. Do they tend to get rarer as we go on?

(c) Other than 2 and 5, all primes must end in 1, 3, 7 or 9. Is there a bias: do more end in 3 than in 9, for example?

(d) There seem to be several pairs of small primes which differ by 2 (eg 3 and 5, and 5 and 7, and 11 and 13). How many such pairs are there?

(e) Are there quick ways of testing if a number is prime?

(f) Are there quick ways of finding large primes?

Some of these have had well-known answers for more than a century, some are still unsolved, and some are currently the focus of tremendous interest.

We'll start off by giving the answer that first question, which was known to the ancient Greeks:

Theorem 9.40 (Euclid's theorem)**.** *There are infinitely many prime numbers.*

Here's the proof, the way I prefer to think of it:

Proof. We'll construct a sequence $p_1, p_2, p_3 \ldots$ of different primes by induction (so, the statement we're doing induction on is, "there are at least n different primes").

For our base case we take $n = 1$, and then take $p_1 = 2$, which is a prime.

For our induction step we suppose we have primes $p_1, \ldots, p_n$, and our job is to show that there's another prime.

Consider the natural number

$$p_1 p_2 \cdots p_n + 1$$

obtained by multiplying all our primes so far and adding 1.

This number is not a multiple of p_1, because $p_1 \cdots p_n$ is: so $p_1 \cdots p_n + 1$ leaves a remainder of 1 when you divide by p_1.

Similarly, it's not a multiple of p_i for any $i = 1, \ldots, n$, because $p_1 \cdots p_n$ is, and so $p_1 \cdots p_n + 1$ leaves a remainder of 1 upon division by p_i.

Butby Theorem9.38 this number has at least one prime factor: we can take our next prime p_{n+1} to be one such prime factor, and that completes the induction step.

□

Here's pretty much exactly the same proof, phrased in a slightly different way.

Proof (ofTheorem 9.40 again). We prove this by *contradiction*: we show that it's true by showing that the negation is absurd.

Indeed, suppose there were only finitely many primes, $p_1, \ldots, p_n$. Then consider (as before) the natural number

$$p_1 \cdots p_n + 1.$$

This isn't divisible by any of the primes $p_1, \ldots, p_n$ (since it leaves a remainder of 1 upon division by any of them). But that's absurd, since we were assuming those were all the primes, andTheorem 9.38 says that every number can be written as a product of primes.

□

Remark 9.41. Some people find proof by contradiction slightly startling when they see it first.

In fact, it's perfectly familiar in daily life. When you find someone who disagrees with you, you show that you are right by pointing out that if you were wrong, then that would contradict something well-known to be correct.

From a logical perspective, it's all to do with the contrapositive. Suppose P is some result we desperately want to prove, for example

$$P = \text{“there are infinitely many primes”},$$

and T something we know is true, for example

$$T = \text{“every positive integer has a prime factor”}.$$

(That was Theorem 9.38).

Now, we proved that if there are only finitely many primes, then some number doesn't have a prime factor. That's exactly $\neg P \Rightarrow \neg T$. But that means that its contrapositive $T \Rightarrow P$ is true. And once we know that, then, since we know T is true, we also know P is true.

Remark 9.42. The second form above, the proof by contradiction, is a more standard form. It appears in the majority of textbooks (and maybe the majority of mathematicians' minds).

This makes me sad, because it's not as good. The proof by contradiction spends all its time making fun of the idea that there might not be infinitely many primes; the first one just goes and builds them.

That means that you can actually use the first proof to construct primes:

- We start with $p_1 = 2$.
- We find that $p_1 + 1 = 3$ is prime, so we can take $p_2 = 3$.
- In fact, $p_1 p_2 + 1 = 7$ is also prime, so we can take $p_3 = 7$.
- Further, $p_1 p_2 p_3 + 1 = 43$ is also prime, so we take $p_4 = 43$.
- Now, $p_1 p_2 p_3 p_4 + 1 = 1807$. It turns out that's not prime: in fact, $1807 = 13 \times 139$. So we could take p_5 to be either 13 or 139...

This is genuinely a way of producing primes. Admittedly, it's not a very intelligent one.

Lecture 10

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm 10.43 (The Sieve of Eratosthenes). [2] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

1. Find the first untouched number and mark it as a prime.
2. Mark all its multiples as being composite.

Remark 10.44. The Sieve of Eratosthenes doesn't prove that there are infinitely many primes: it just finds them. Unless we'd found a proof of Euclid's theorem, we could have nightmares that one day we'll find ourself crossing off all the remaining naturals and not finding any more primes.

Remark 10.45. There are (quite a lot of) other proofs of Euclid's theorem, but Euclid himself probably only knew the way we've discussed.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, and its factors, it's going to turn out to be really useful to consider two numbers and their factors.

Definition 10.46. Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$. The *greatest common divisor* of a and b, written $\gcd(a, b)$ (or sometimes as $\mathrm{hcf}(a, b)$ or sometimes even just (a, b) for short) is the largest common divisor of a and b.

Remark 10.47. That definition probably just says that a greatest common divisor is what you'd expect it to be, given the name!

Remark 10.48. That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function.

There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every positive integer, and so will certainly be a common divisor.
- *There may be lots of common divisors, but no largest one.* That's not a problem either, here. It's easy to see that if $d \mid a$ then $|d| \leqslant |a|$, which means we can't get arbitrarily large divisors.

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we just count down from $|a|$ and stop when we reach the first common divisor.

For example,

$$\gcd(9, 15) =$$

3,

and

$$\gcd(-30, 42) =$$

6.

This approach to finding greatest common divisors is pretty terrible: imagine being asked to find

$$\gcd(123456789, 987654321)$$

by this approach!

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b. That's also a pretty terrible way, because factorising numbers is hard work: it seems like a lot of work to find all factors of 123456789 still.

We will see a much better way soon, but, first, let's spot some easy properties of greatest common divisors.

Remark 10.49. For all integers a and b, we have

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

because the definition is symmetric in a and b.

Also, for all positive integers a, we have

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

and

$$\gcd(a, 1) = 1,$$

and

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

A slightly less obvious property is:

Proposition 10.50. *Let a, b and k be integers. Then*

$$\gcd(a, b) = \gcd(a + kb, b).$$

Proof. We'll show that the common divisors of a and b are the same as the common divisors of $a + kb$ and b.

Suppose first that d is a common divisor of a and b; in other words, $d \mid a$ and $d \mid b$. Then we can write $a = md$ and $b = nd$ for some integers m and n. But then

$$a + kb = md + knd = (m + kn)d,$$

so $d \mid a + kb$, so d is a common divisor of $a + kb$ and b.

Similarly, if d is a common divisor of $a + kb$ and b, then we can write $a + kb = ld$ and $b = nd$. But then

$$a = a + kb - kb = ld - knd = (l - kn)d,$$

so $d \mid a$, so d is a common divisor of a and b.

Since we've now proved that a and b have the same common divisors as $a+kb$ and b, it follows that they have the same *greatest* common divisor.

□

We should also mention that the greatest common divisor has a close cousin:

Definition 10.51. Given two positive integers a and b, the *least common multiple* $\operatorname{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark 10.52. Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab).

The last piece of terminology we might want is this:

Definition 10.53. Two integers a and b are said to be *coprime*, or *relatively prime*, if $\gcd(a, b) = 1$.

Division with Remainder

The above Proposition10.50 looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?

It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors. We can use it to make the numbers smaller.

The question is, given a and b, how small can a number of the form $a+kb$ (for k an integer) be? It turns out that this is something familiar to you all:

Proposition 10.54 (Division with Remainder)**.** *Let a and b be integers, with $b > 0$. One can write*

$$a = qb + r$$

for integers q (the quotient*) and r (the* remainder*) such that $0 \leqslant r < b$.* □

Remark 10.55. It is not too hard to prove this: one can do it with two inductions, for example, (one for the negative and one for the positive integers), but I won't do so here.

Remark 10.56. It's reasonable to ask why we had to take $b > 0$. It's true for $b < 0$, too, we just have to say that the remainder r satisfies $0 \leqslant r < -b$ instead.

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example.

Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

$$\begin{aligned}\gcd(126, 70) &= \gcd(56 + 70 \times 1, 70) \\ &= \gcd(56, 70) \quad \text{(using Proposition 10.50)} \\ &= \gcd(70, 56).\end{aligned}$$

That made the problem much smaller, and we can do the same trick repeatedly:

$$\begin{aligned}\gcd(70, 56) &= \gcd(14 + 56 \times 1, 56) \\ &= \gcd(14, 56) \\ &= \gcd(56, 14).\end{aligned}$$

That's smaller still. Let's see what happens next:

$$\begin{aligned}\gcd(56, 14) &= \gcd(0 + 14 \times 4, 14) \\ &= \gcd(0, 14) \\ &= 14.\end{aligned}$$

As 56 is a multiple of 14, of course we get remainder 0, so we can stop here and get the greatest common divisor to be 14.

Here's the general case:

Algorithm 10.57 (Euclid's algorithm). Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them overby Remark 10.49 earlier.

By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.

But then we have

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

and since $b < a$ and $r < b$ we've made both numbers smaller.

If we keep doing this repeatedly, we'll end up making one of the numbers zero and can stop.

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4) = \gcd(0, 4) = 4.
\end{aligned}$$

Remark 10.58. One might reasonably wonder just *how fast* Euclid's algorithm really is. Proving it is (slightly) beyond the scope of this course, but one good answer is that if you're trying to work out $\gcd(a, b)$ and $b < a$, then the number of steps you need is always less than five times the number of digits of b.

So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ steps (actually, this one takes a lot less than 45 steps, if you try it). Compared with the other methods we discussed, this makes it seem really good.

Lecture 11

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!

Let's see how this works with an example. We saw earlier that $\gcd(126, 70) = 14$, so we expect to be able to find integers m and n such that $126m + 70n = 14$.

Along the way we found that:

$$126 = 1 \times 70 + 56, \tag{1}$$
$$70 = 1 \times 56 + 14. \tag{2}$$

Working through that backwards, we get that

$$\begin{aligned}
14 &= 1 \times 70 - 1 \times 56 \qquad \text{(using (2))} \\
&= 1 \times 70 - 1 \times (1 \times 126 - 1 \times 70) \qquad \text{(using (1))} \\
&= 2 \times 70 - 1 \times 126.
\end{aligned}$$

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))}\\ &= 29 \times 296 - 33 \times 260\\ &= 29 \times 296 - 33 \times (556 - 296) && \text{(using (3))}\\ &= 62 \times 296 - 33 \times 556. \end{aligned}$$

One can prove without too much difficulty that this technique always works (though we won't):

Proposition 11.59 (Bezout's Lemma)**.** *Let a and b be two integers with $\gcd(a, b) = d$. Then there are integers m and n such that $ma + nb = d$.* □

In fact, slightly more is true:

Proposition 11.60. *Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.*

Proof. **The "if" part:** We must prove that, if $d \mid e$, then we can write e as a linear combination of a and b.

However, since $d \mid e$, we can write $e = dk$ for some k. Also, by the above Proposition11.59 we can write $d = ma + nb$ for some m and n. But then

$$e = dk = (mk)a + (nk)b,$$

as required.

The "only if" part: We must prove that if $e = ma + nb$, then $d \mid e$. But, since $d = \gcd(a, b)$ we have $d \mid a$ and $d \mid b$, and hence also $d \mid ma$ and $d \mid nb$, and therefore $d \mid ma + nb$ as required. □

The fundamental theorem of arithmetic

We'll go on now and describe three uses of this result. Firstly, we return to the question of unique factorisation into primes. Of course we'veproved (as Theorem 9.38) that every positive integer can be written as a product of primes. The question is, can every positive integer be written as a product of primes in *only one way*?

Of course, we should be careful to say what we mean by "only one way". We certainly do have:

$$\begin{aligned} 420 &= 2 \times 2 \times 3 \times 5 \times 7 \\ &= 5 \times 2 \times 3 \times 7 \times 2 \\ &= 7 \times 5 \times 3 \times 2 \times 2, \quad \text{and so on...} \end{aligned}$$

Clearly, what we mean is that every positive integer can be written as a product of primes in only one way, where reordering doesn't count as different. Or, more precisely, that any two ways of writing a positive integer as a product of primes differ only by reordering. Mathematicians say, "in only one way, up to reordering".

So the question we ask ourselves is (for example) why we can't have

$$487 \times 205339 = 7 \times 17 \times 59 \times 14243,$$

(I promise you that all six of those numbers are prime).

One wants to say something like "as the right-hand side is clearly divisible by 7, the left-hand side must be divisible by 7 too, but there isn't a 7 listed among the primes on the left".

But if we have $7 \mid (487 \times 205339)$, why must we have either $7 \mid 487$ or $7 \mid 205339$? It wouldn't be true if 7 weren't a prime. But this is true for primes!

Proposition 11.61. *Let p be a prime, and a and b be integers. Then, if $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Remark 11.62. This result is not only not obvious, we should expect it to be *difficult*. The definition of "p being prime" talks about what things divide p. But this result says something about what things p divides, which is completely unrelated.

Proof of Proposition 11.61. Suppose that $p \mid ab$, and consider $\gcd(p, a)$. Since $\gcd(p, a) \mid p$, we either have $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

If $\gcd(p, a) = p$, then as $\gcd(p, a) \mid a$, we have $p \mid a$.

If $\gcd(p, a) = 1$, however, then by Proposition 11.59, we know that there are integers m and n such that $mp + na = 1$. Now suppose we multiply both sides by b; we get $mpb + nab = b$.

Clearly $p \mid mpb$, and also we have $p \mid nab$ since we are supposing that $p \mid ab$. Hence $p \mid mpb + nab$, so $p \mid b$, as needed.

□

Remark 11.63. Exactly the same proof can be used to show that, for any integers n, a and b, that if $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$.

We can also boost it to a result about a product of *lots* of terms:

Proposition 11.64. *Let p be a prime and let $a_1, \ldots, a_n$ be integers. Then if $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.*

This is an easy induction argument usingProposition 11.61 above.

Now, equipped with that tricky result, we're ready to prove the main result of this section:

Theorem 11.65 (Fundamental Theorem of Arithmetic)**.** *Any positive integer n can be written as a product of primes in exactly one way, up to reordering.*

Proof. We haveshown (Theorem 9.38) that any positive integer can be written as a product of primes. We need to show that this expression is unique. We'll prove it by contradiction.

Suppose not: there is a number n with two genuinely different prime factorisations $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$. We can suppose that the p's and the q's have nothing in common (if they do, cancel them out, and we still get an example).

Now, that means that p_1 is different to $q_1, q_2, \ldots, q_s$.

We have $p_1 \mid n$, since $n = p_1 \cdots p_r$. But then we also have $p_i \mid q_1 \cdots q_s$. But by Proposition 11.61, this means that $p_1 \mid q_j$ for some j. But, by the definition of q_j being a prime number, that means that $p_1 = q_j$, which we said didn't happen: that gives us our contradiction.

□

Lecture 12

Linear diophantine equations

A *diophantine equation* is an equation where we're interested in solutions with the variables lying in $\mathbb{N}$ or $\mathbb{Z}$. They're named after the ancient Greek mathematician Diophantus of Alexandria.

An example of a diophantine equation is the Fermat equation for exponent 7:

$$x^7 + y^7 = z^7.$$

If we were interested in solutions to this equation over $\mathbb{R}$, the story would be really, really simple: we could take any x and any y we wanted and then just take

$$z = \sqrt[7]{x^7 + y^7}.$$

The Fermat equation becomes more interesting because of our inability to reliably take nth roots in $\mathbb{Z}$ or $\mathbb{N}$: which x and y can we take for which this recipe works?

While they're much easier, a similar thing is true of *linear diophantine equations*: equations of the form

$$ax + by = c,$$

where a, b and c are integer constants.

Consider, for example, the equation $39x + 54y = 120$. (This might be of interest to forensic accountants. Indeed, suppose I can buy or sell widgets for 39p and gadgets for 54p: what combinations can I buy and sell to leave me £1.20 up?)

This equation would be simple if we cared about real solutions: we could take any x we like and then just take $y = (120 - 39x)/54$. However, because we can't do division reliably in $\mathbb{Z}$, this recipe is not very helpful: how do we know which x will give us an integer y?

However, the techniques we've developed give us a way in to the problem. Euclid's algorithm gives us that

$$\begin{aligned}
\gcd(54, 39) &= \gcd(1 \times 39 + 15, 39) = \gcd(15, 39) = \gcd(39, 15) \\
&= \gcd(2 \times 15 + 9, 15) = \gcd(9, 15) = \gcd(15, 9) \\
&= \gcd(1 \times 9 + 6, 9) = \gcd(6, 9) = \gcd(9, 6) \\
&= \gcd(1 \times 6 + 3, 6) = \gcd(3, 6) = \gcd(6, 3) \\
&= \gcd(2 \times 3 + 0, 3) = \gcd(0, 3) = 3.
\end{aligned}$$

Then, we can work backwards to find a solution to $39x + 54y = 3$:

$$\begin{aligned} 3 &= 6 - 3 \\ &= 6 - (9 - 6) = 2 \times 6 - 9 \\ &= 2 \times (15 - 9) - 9 = 2 \times 15 - 3 \times 9 \\ &= 2 \times 15 - 3 \times (39 - 2 \times 15) = 8 \times 15 - 3 \times 39 \\ &= 8 \times (54 - 39) - 3 \times 39 = 8 \times 54 - 11 \times 39. \end{aligned}$$

So

$$39 \times (-11) + 54 \times 8 = 3,$$

and we multiply both sides by 40 to get

$$39 \times (-440) + 54 \times 320 = 120,$$

or in other words, that $x = -440$, $y = 320$ gives a solution.

Now, you might wonder whether this is the *only* solution.

There's a way of analysing this. Suppose we have two solutions:

$$39x + 54y = 120 \qquad \text{and} \qquad 39x' + 54y' = 120.$$

Subtracting, we get

$$39(x - x') + 54(y - y') = 0.$$

Dividing out by the greatest common divisor, we get

$$13(x - x') + 18(y - y') = 0,$$

or

$$13(x - x') = -18(y - y').$$

This means that, as 18 divides the right-hand side, then we also have $18 \mid 13(x-x')$. But since 13 and 18 are coprime, we have $18 \mid (x-x')$ byRemark 11.63. So we can write $x - x' = 18k$. But then we can solve to get $y - y' = -13k$, and it's easy to check that any such k works.

Hence the general solution is

$$x = 18k - 440, \qquad y = 320 - 13k.$$

While I haven't stated (still less proved) any theorems about it, this approach works perfectly well in general, as you can imagine.

Common divisors and the gcd

Here's a useful result about common divisors.

Proposition 12.66. *Let a and b be positive integers. Any common divisor of a and b is a divisor of the greatest common divisor.*

Proof. If $d \mid a$ and $d \mid b$, then $d \mid (a - qb)$ for any q. Hence d is a divisor of the numbers obtained after every step of Euclid's algorithm, and so it is a divisor of the gcd. □

We defined the gcd to be the greatest of all common divisors. This property is arguably a more natural one: this says that the gcd is somehow the "best" common divisor. It is clear that such a divisor must be bigger than all other divisors.

Modular arithmetic

Congruences

Repeatedly over the last few lectures (and the last few problem sheets) we have seen appearances of lots of things like:

- odd numbers;
- even numbers;
- remainders upon division;
- numbers of the form $4n + 1$ or $18k - 440$, and so on.

All these things look pretty similar, and it's time we got ourselves a language for discussing these things better.

Definition 12.67. We say that a *is congruent to* b *modulo* m if $m \mid (a - b)$. Often we abbreviate, and say congruent *mod* m.

We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a and b are congruent modulo m.

For example,

$$3167 \equiv 267 \pmod{100};$$

indeed, the fact that these two positive integers have the same last two digits means that their difference is a multiple of 100.

We can now say that an even number is a number congruent to 0 (modulo 2), and an odd number is a number congruent to 1 (modulo 2).

Rather than saying that "n is of the form $18k - 440$", we can say that "n is congruent to -440, modulo 18".

Arguments about time frequently involve understandings of congruences. For example, I was born on a Sunday, and the closing ceremony of the 2012 Summer Olympics took place on a Sunday too. So the number of days since the former is congruent to the number of days since the latter, modulo 7.

Notice that saying that a is congruent to 0, modulo m, is exactly the same as saying that a is a multiple of m (since it's saying that $m \mid (a - 0)$).

As we've defined it, a congruence modulo m doesn't say that two things are equal, just that their difference is a multiple of m.

But it does behave suspiciously like an equality, as the following basic results show:

Proposition 12.68. *Here are some properties of congruences, true for all integers:*

(a) We always have $a \equiv a \pmod{m}$*;*

(b) If $a \equiv b \pmod{m}$*, then* $b \equiv a \pmod{m}$*;*

(c) If $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$*, then* $a \equiv c \pmod{m}$*;*

(d) If $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a + c \equiv b + d \pmod{m}$*;*

(e) If $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a - c \equiv b - d \pmod{m}$*;*

(f) If $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $ac \equiv bd \pmod{m}$*.*

Proof (of some of them). (a) Since $a - a = 0$, we have $m \mid (a - a)$.

(b) If $a \equiv b \pmod{m}$, we have $m \mid (a-b)$. But then $m \mid -(a-b)$, which says $m \mid (b - a)$, or in other words $b \equiv a \pmod{m}$.

(c) As $a \equiv b \pmod{m}$, we have $m \mid (a - b)$; similarly as $b \equiv c \pmod{m}$, we have $m \mid (b - c)$. But then

$$m \mid ((a - b) + (b - c)) = (a - c),$$

which says that $a \equiv c \pmod{m}$.

(d) As $a \equiv b \pmod{m}$, we can write $a - b = km$ for some integer k; similarly, as $c \equiv d \pmod{m}$, we can write $c - d = lm$ for some integer l.

As a result, we have

$$(a+c)-(b+d) = (a-b)+(c-d) = km+lm = (k+l)m,$$

so $m \mid ((a+c)-(b+d))$, so $a+c \equiv b+d \pmod{m}$.

(e) As above, we can write $a-b = km$, and $c-d = lm$. Then

$$(a-c)-(b-d) = (a-b)-(c-d) = km-lm = (k-l)m,$$

so $m \mid ((a-c)-(b-d))$, so $a-c \equiv b-d \pmod{m}$.

(f) As $a \equiv b \pmod{m}$, then we can write $a = b+km$ for some integer k (since $a-b$ is a multiple of m). Similarly, as $c \equiv d \pmod{m}$ we can write $c = d+lm$.
But then $ac = (b+km)(d+lm) = bd + (bl+dk+klm)m$, which says that $ac \equiv bd \pmod{m}$. □

Lecture 13

I interpret all that as saying that, provided you're careful and justify any unusual steps, the language of congruences behaves somewhat like equality. (In particular, our choice of notation, looking a bit like an overenthusiastic equals sign, wasn't a bad choice).

Back at school, you probably learned facts like "an odd number times an even number is an even number". Being odd or even is about being congruent to 1 or 0 modulo 2. The language of congruences gives us ways of writing down similar facts about other moduli: for example, "a number congruent to 3 (mod 7) times a number congruent to 4 (mod 7) is a number congruent to 12 (mod 7) and hence to 5 (mod 7)".

In fact, we can use this ideas to make multiplication tables of congruences. For example, here's a multiplication table modulo 5:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

So, for example, this tells us that $2 \times 4 \equiv 3 \pmod{5}$.

Notice that this shares some features with a usual multiplication table. For example, there is a column and a row of zeroes, because if you multiply something by something congruent to zero mod 5, you get something congruent to zero mod 5. Also, multiplying by 1 doesn't change anything.

In the above multiplication table, we managed to write every number congruent to 0, 1, 2, 3 or 4 modulo 5. Is this a general feature? Yes, it is, and it turns out to be a consequence of our earlier observation on division with remainder.

Proposition 13.69. *Let a and b be integers, with $b > 0$. Then a is congruent (modulo b) to a unique integer in the set*

$$\{0, 1, \ldots, b-1\}.$$

Proof. We'll show that such a number exists, first, and then we'll show that it's unique.

By Proposition 10.54, we can write $a = qb + r$ for some integer q and some integer r with $0 \leqslant r < b$. But then that says that $a - r = qb$, and hence $a \equiv r \pmod{b}$. That shows that a is congruent to some number in that set.

Now, we'll prove uniqueness. In fact we never proved that division with a *unique* remainder was possible, so let's mend that now.

Suppose that $a \equiv r_1 \pmod{b}$ and also $a \equiv r_2 \pmod{b}$. Then $0 = a - a \equiv r_2 - r_1 \pmod{b}$ by subtracting, so $b \mid (r_2 - r_1)$.

But since $0 \leqslant r_1 < b$ and $0 \leqslant r_2 < b$, we have

$$-b = 0 - b < r_2 - r_1 < b - 0 = b.$$

So $r_2 - r_1$ is a multiple of b strictly between $-b$ and b: it must be zero, so $r_1 = r_2$, which proves uniqueness.

□

This proposition has a lot of consequences.

It means we can divide up the integers into sets, called *congruence classes* or *residue classes*, based on which number from $\{0, \ldots, b-1\}$ they're congruent to. So, for $b = 5$, we divide the integers into:

- $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$, all congruent to 0 (mod 5);
- $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$, all congruent to 1 (mod 5);
- $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$, all congruent to 2 (mod 5);
- $\{\ldots, -7, -2, 3, 8, 13, \ldots\}$, all congruent to 3 (mod 5);
- $\{\ldots, -6, -1, 4, 9, 14, \ldots\}$, all congruent to 4 (mod 5).

Many people, particularly those who like numerical calculations with integers (like computer programmers), use all this as an excuse to define a function, also called "mod", which gives the remainder upon division (so that $a \bmod b$ is an integer between 0 and b). So they say, for example, that $137 \bmod 100 = 37$.

This works fairly well for the computer programmers, but I find it a little unsatisfying. While it's true that every number is congruent (modulo 7) to a unique number from $\{0, 1, 2, 3, 4, 5, 6\}$, there's nothing much special about that set. It's also true that every number is congruent (modulo 7) to a unique number in the set $\{1, 2, 3, 4, 5, 6, 7\}$. And it's also true that every number is congruent (modulo 7) to a unique number in the set $\{-3, -2, -1, 0, 1, 2, 3\}$. And, in fact, I can think of situations where all those facts are useful.

So it's important we just think of the unique number in $\{0, \ldots, b-1\}$ as just one out of many equally good ways of describing our number, up to congruence modulo b.

Next semester, you'll come to regard the integers, considered up to congruence modulo m, as a system of numbers in its own right (and why not? We can add them and subtract them and multiply them, all considered only up to congruence modulo m). This system of numbers is commonly called $\mathbb{Z}/m\mathbb{Z}$ (for reasons which will remain obscure at least for a year or two more).

This is novel in one important sense. In the past, every time we've introduced a new system of numbers, it's contained the system we were thinking about before. We've built

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

But $\mathbb{Z}/m\mathbb{Z}$ doesn't seem to work like this in this framework. It's related to $\mathbb{Z}$, but doesn't really live inside it. Similarly, "times of day" aren't a subset of times: for example, there's no one special point of time in history called "2pm", just many examples of 2pm on many different days.

In the case where $m = 2$, you're probably comfortable with the fact that "odd" and "even" form something like a system of numbers (because you can add them and subtract them and multiply them), but while they've obviously got something to do with $\mathbb{Z}$, there's no one integer called "odd" and no one integer called "even".

Modular arithmetic, to other moduli, is similar.

Congruence equations

We've now laid the foundations of *modular arithmetic*, the study of congruences. After all that philosophy, we should do some sums.

The set of all solutions to $x \equiv 3 \pmod 7$ seems like a perfectly explicit description of a class of numbers: it's a congruence class modulo 7, the class of numbers of the form $7n + 3$. So we can start listing them easily:

$$\ldots, -11, -4, 3, 10, 17, \ldots.$$

But what is the set of solutions to $5x \equiv 3 \pmod 7$?

That's not a particularly satisfactory description of a set of numbers: it's a pain to list them, so we should ask for better.

However, we can get a more satisfactory list just using techniques we already know. The condition $5x \equiv 3 \pmod 7$ says that $7 \mid 5x - 3$, which in turn says that $7k = 5x - 3$ for some k. Rearranging, that says that $5x - 7k = 3$. But we *know* how to get a general solution for those!

Indeed, we find that $\gcd(5, 7) = 1$, and as $1 \mid 3$ there are solutions. First we try to find a single one.

We can get a solution to $5x - 7k = 1$ (by guessing, or by using Euclid's algorithm backwards) such as $x = 3, k = 2$. This means (by tripling both sides) that a solution to $5x - 7k = 3$ is given by $x = 9, k = 6$.

To find other solutions, we subtract $5 \times 9 - 7 \times 6 = 3$ from $5x - 7k = 3$ to get $5(x - 9) - 7(k - 6) = 0$.

Hence $5(x - 9) = 7(k - 6)$, so $7 \mid 5(x - 9)$. As 7 and 5 are coprime, this means that $7 \mid (x - 9)$. So it's equivalent to $x \equiv 2 \pmod 7$, which *is* a nice description!

Lecture 14

We can regard linear equations in modular arithmetic as asking about *division*. After all, asking about solutions to the linear equation

$$5x = 3$$

is asking "can we divide 3 by 5"? So the fact that $2 \times 5 \equiv 3 \pmod 7$ might be regarded as saying that we *can* divide 3 by 5 (modulo 7), and we get 2 when we do so.

But division in modular arithmetic is more complicated than in the integers. Of course, integer division is unique where it exists. In other words, if I choose integers a and b (with b nonzero) and ask about integer solutions to

$$ax = b,$$

then two things can happen: either there is a unique solution (as with $3x = 6$), or there's no solution at all (as with $4x = 7$).

That's not true in modular arithmetic, as the following examples show:

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 6$?

None: the lhs is even and the rhs odd.

- How many residue classes of solutions are there to $2x \equiv 5 \pmod 7$?

  One: $x \equiv 6 \pmod 7$.

- How many residue classes of solutions are there to $2x \equiv 6 \pmod 8$?

  Two: $x \equiv 3 \pmod 8$ and $x \equiv 7 \pmod 8$.

- How many residue classes of solutions are there to $4x \equiv 4 \pmod 8$?

  Four: $x \equiv 1, 3, 5, 7 \pmod 8$.

Even if you don't want to do division in modular arithmetic, you still have to be careful about *cancellation*.

In ordinary arithmetic over the integers, we know that $ax = ay$ implies $x = y$ (provided that a isn't zero, of course). This is true even though we don't know how to divide integers in general.

But we can't always cancel in modular arithmetic: the third example above tells (for example) that $2 \cdot 3 \equiv 2 \cdot 7 \pmod 8$, but that $3 \not\equiv 7 \pmod 8$.

Here's a fact, mostly a repackaging of some observations we made in a previous lecture, about diophantine equations, saying when we can divide 1 by things.

Proposition 14.70. *Let a and m be integers. There is an integer b such that $ab \equiv 1 \pmod m$ if and only if $\gcd(a, m) = 1$.*

When such a number b does exist, it's unique (modulo m).

Proof. Using Proposition 11.60, we know what we can find integers b and c such that

$$ab + mc = 1$$

if and only if $\gcd(a, m) \mid 1$.

But $\gcd(a, m) \mid 1$ if and only if $\gcd(a, m) = 1$, and the equation $ab + mc = 1$ says exactly that $ab \equiv 1 \pmod m$.

Suppose that we have two numbers b and b' such that $ab \equiv 1 \pmod m$ and $ab' \equiv 1 \pmod m$. Then

$$b \equiv b1 \equiv b(ab') \equiv (ba)b' \equiv 1b' \equiv b' \pmod m,$$

which shows uniqueness modulo m.

□

When there is a number b such that $ab \equiv 1 \pmod{m}$, we call it the *inverse* of a, modulo m (and we say that a is *invertible*). We write a^{-1} for the inverse of a.

Notice that, as a consequence modular arithmetic modulo a prime p is *fantastically* well-behaved: any nonzero residue $a \not\equiv 0 \pmod{p}$ has an inverse (since we have $\gcd(a, p) = 1$ unless a is a multiple of p).

Spotting inverses modulo m is quite difficult; in general the best way is to use Euclid's algorithm.

There are a few exceptions:

- The inverse of 1 modulo m is always

  1.

- The inverse of -1 modulo m is always

  -1.

- If m is odd, then 2 is invertible modulo m, because $\gcd(m, 2) = 1$. The inverse is:

  $(m + 1)/2$.

Lecture 15

Two other fairly easy, but useful, facts are as follows:

Proposition 15.71. *If a is invertible modulo m, then so is a^{-1}, with inverse given by $(a^{-1})^{-1} \equiv a \pmod{m}$.*

Proof. We have $aa^{-1} \equiv 1 \pmod{m}$, which says that a is an inverse for a^{-1}. □

Proposition 15.72. *If a and b are both invertible, then ab is too, with inverse given by*

$$(ab)^{-1} \equiv b^{-1}a^{-1} \pmod{m}.$$

Proof. We have $(ab)b^{-1}a^{-1} \equiv aa^{-1}bb^{-1} \equiv 1 \cdot 1 \equiv 1 \pmod{m}$. □

Just by way of example (and partly as a reminder of the whole Euclid's algorithm thing), let's find an inverse for 37, modulo 100.

So we want x with $37x \equiv 1 \pmod{100}$. In other words, we seek a solution to $37x + 100k = 1$ in the integers. We'll get one from working through Euclid's algorithm:

$$\begin{aligned}
\gcd(37, 100) &= \gcd(37, 2 \times 37 + 26) \\
&= \gcd(37, 26) \\
&= \gcd(26, 37) \\
&= \gcd(26, 1 \times 26 + 11) \\
&= \gcd(26, 11) \\
&= \gcd(11, 26) \\
&= \gcd(11, 2 \times 11 + 4) \\
&= \gcd(11, 4) \\
&= \gcd(4, 11) \\
&= \gcd(4, 2 \times 4 + 3) \\
&= \gcd(4, 3) \\
&= \gcd(3, 4) \\
&= \gcd(3, 1 \times 3 + 1) \\
&= \gcd(3, 1) = 1.
\end{aligned}$$

So we have that

$$\begin{aligned}
1 &= 1 \times 4 - 1 \times 3 \\
&= 1 \times 4 - 1 \times (11 - 2 \times 4) \\
&= 3 \times 4 - 1 \times 11 \\
&= 3 \times (26 - 2 \times 11) - 1 \times 11 \\
&= 3 \times 26 - 7 \times 11 \\
&= 3 \times 26 - 7 \times (37 - 26) \\
&= 10 \times 26 - 7 \times 37 \\
&= 10 \times (100 - 2 \times 37) - 7 \times 37 \\
&= 10 \times 100 - 27 \times 37.
\end{aligned}$$

That means that $(-27) \times 37 \equiv 1 \pmod{100}$, so the inverse of 37 is -27, which is equivalent to 73 (mod 100).

And, of course, we can check this easily: $37 \times 73 = 2701 \equiv 1 \pmod{100}$ as claimed.

The Chinese Remainder Theorem

We've come to understand congruence equations: given something like

$$123x \equiv 456 \pmod{789},$$

we can, with some effort, turn it into something nice like

$$x \equiv 132 \pmod{263}.$$

Now we'll discuss a different sort of problem with congruences: what if we have two of them for the same number? For example,

$$x \equiv 1 \pmod{4}$$
$$x \equiv 3 \pmod{7}?$$

These things happen all the time: two things happening periodically with different periods.

And it turns out we can solve them using exactly the same machinery as we've been using all along. Indeed, these equations say that

$$x - 1 = 4a$$
$$x - 3 = 7b,$$

for some numbers a and b.

That means that

$$1 + 4a = 3 + 7b,$$

or in other words $4a - 7b = 2$. We have lots of experience solving these, and, since $\gcd(4, 7) = 1$, it's possible.

A solution to $4a - 7b = 1$ is given by $a = 2$, $b = 1$, and so a solution to $4a - 7b = 2$ is given by doubling that to get $a = 4$, $b = 2$.

What's the general solution? Well, if we have $4a-7b = 2$, then subtracting $4 \times 4 - 7 \times 2 = 2$ gives

$$4(a - 4) - 7(b - 2) = 0.$$

This means that $7 \mid 4(a - 4)$, so $7 \mid (a - 4)$. Hence a is of the form $7k + 4$. and in fact any such a works.

So $4a$ is of the form $28k + 16$, so x is of the form $28k + 17$, in other words:

$$x \equiv 17 \pmod{28}.$$

There need not always be solutions to simultaneous congruences. For example, the simultaneous congruences

$$x \equiv 4 \pmod{6}$$
$$x \equiv 3 \pmod{8}$$

don't have solutions. Why is this obvious?

The first equation implies x even, the second x odd.

Of course, if we go through the same solution process as above it will fail. We set

$$x = 4 + 6a$$
$$x = 3 + 8b$$

and find that $4 + 6a = 3 + 8b$, and hence $8b - 6a = 1$. This has no solutions(thanks to Proposition 11.60) because $\gcd(8, 6) = 2$, and $2 \nmid 1$.

It would be good to know something that reassures us that there *will* be a solution in some family of cases, and here's a result, named after its discovery by the ancient Chinese:

Theorem 15.73 (Chinese Remainder Theorem)**.** *Let m_1 and m_2 be coprime, and let a_1 and a_2 be any integers. The simultaneous congruences*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

have a solution modulo $m_1 m_2$.

Proof. Suppose given m_1 and m_2 coprime.

We'll solve two of the easiest imaginable pairs of simultaneous congruences first, and then we'll observe that, in fact, that's enough work to do anything.

That easy pair of simultaneous congruences are

$$y \equiv 1 \pmod{m_1}$$
$$y \equiv 0 \pmod{m_2}.$$

The first equation says that $y = 1 - km_1$ for some k, and the second says that y is a multiple of m_2. In other words, we have $m_2 \mid 1 - km_1$, so

$$km_1 \equiv 1 \pmod{m_2}.$$

But m_1 and m_2 are coprime, so we know we can do this (this is Proposition 14.70).

Another easy pair of simultaneous congruences are

$$z \equiv 0 \pmod{m_1}$$
$$z \equiv 1 \pmod{m_2}.$$

This looks exactly the same, but the other way around: the second says that z is of the form $z = 1 - lm_2$ for some l, and the first says that z is a multiple of m_1. In other words, we need

$$lm_2 \equiv 1 \pmod{m_1}.$$

We know we can do this (Proposition 14.70 again).

In fact, instead of going through Proposition 14.70, the same process does *both* these pairs of congruences: if we use Euclid's algorithm to give a solution to

$$rm_1 + sm_2 = 1,$$

then it's easy to see that taking $z = rm_1$ and $y = sm_2$ gives us what we want: $sm_2 \equiv 1 \pmod{m_1}$ and $sm_2 \equiv 0 \pmod{m_2}$, while $rm_1 \equiv 0 \pmod{m_2}$ and $sm_2 \equiv 1 \pmod{m_2}$.

What then of our original equations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}? \end{aligned}$$

I claim that if we take $x = a_1y + a_2z$, we have what we need.

Indeed, since $y \equiv 1 \pmod{m_1}$ and $z \equiv 0 \pmod{m_1}$, we have

$$x = a_1y + a_2z \equiv a_1 \pmod{m_1},$$

while, since $y \equiv 0 \pmod{m_2}$ and $z \equiv 1 \pmod{m_2}$, we have

$$x = a_1y + a_2z \equiv a_2 \pmod{m_1}.$$

Both of those are exactly what we needed.

□

This gives us a new way of finding solutions, which I'll show off: What are the solutions to:

$$\begin{aligned} x &\equiv 11 \pmod{14} \\ x &\equiv 10 \pmod{17}? \end{aligned}$$

We'll use our "building blocks" from the proof of the Chinese Remainder Theorem. In order to find this, we discovered we needed to invert 17 mod 14: we need to solve

$$14x + 17y = 1.$$

This has a solution $5 \times 17 - 6 \times 14 = 1$.

As a result $5 \times 17 = 85$ is congruent to 1 mod 14 and 0 modulo 17, and $-6 \times 14 = -84$ is congruent to 0 mod 14 and 1 modulo 17.

Hence our solution is

$$11 \times 85 + 10 \times (-84) \equiv 95 \pmod{238}.$$

Lecture 16

More calculations modulo primes

Earlier, we pointed out that modular arithmetic modulo primes is very well-behaved: every nonzero residue is invertible.

We'll going to go on and use that.

The first thing we'll talk about is *exponentiation* in modular arithmetic.

In integer arithmetic, it's usually stupid to try to calculate very large powers: for example, 3^{1234} has a huge number of digits (589 of them, to be precise).

But, in modular arithmetic there are no large numbers. For example 3^{1234} will be congruent to something between 0 and 9 modulo 10, and it's not unreasonable to ask what.

One very stupid way of working it out would be to do the multiplication in the integers, then divide by 10 and find the remainder.

We can do better, by doing our arithmetic all modulo 10 in the first place. So:

$$\begin{aligned} 3^2 &= 3 \times 3 \equiv 9 \pmod{10}, \\ 3^3 &= 3 \times 3^2 \equiv 3 \times 9 \equiv 7 \pmod{10}, \\ 3^4 &= 3 \times 3^3 \equiv 3 \times 7 \equiv 1 \pmod{10} \ldots \end{aligned}$$

That's still going to be a lot of multiplication, if we keep multiplying by 3 (modulo 10) more than a thousand times!

There are considerably more intelligent ways. For example, we can square modulo 10 quite quickly.

That lets us do some exponents by repeated squaring. For example,

$$3^8 = 3^{2\times 4} = \left(3^2\right)^4 = \left(3^2\right)^{2\times 2} = \left(\left(3^2\right)^2\right)^2.$$

1234 isn't quite as nice, but we can do

$$3^{1234} \equiv 3^{2\times 617} \equiv \left(3^2\right)^{617} \equiv 9^{617} \equiv 9^{2\times 308+1} \equiv \left(9^2\right)^{308} 9$$

and end up getting the answer.

Tricks like that are much, much faster than multiplying by three lots of times mod 10.

But, in fact, there's a method that's even faster still for this situation. We've just computed that

$$3^4 \equiv 1 \pmod{10}.$$

That does almost all the work for us, as

$$3^{4k} = (3^4)^k \equiv 1^k = 1 \pmod{10}.$$

Hence

$$3^{1234} = 3^{4\times 308+2} = 3^{4\times 308}3^2 = (3^4)^{308}3^2 \equiv 1^{308}3^2 \equiv 3^2 \equiv 9 \pmod{10}.$$

That makes the whole thing easy.

The relevant observation here was really that there was some integer n such that $3^n \equiv 1 \pmod{10}$. So two obvious questions are:

1. When does there exist such an n?
2. When it does exist, can we compute it?

Our answer to the first is not too difficult:

Theorem 16.74. *Let a and m be coprime integers. Then there is some positive n such that*

$$a^n \equiv 1 \pmod{m}.$$

Proof. There are only m different residues modulo m, so some two of the sequence

$$1, a, a^2, a^3, a^4, \ldots, a^m$$

must be congruent modulo m (they can't all be different).

Let's say that $a^i \equiv a^j \pmod{m}$, with $i < j$.

But a is invertible modulo m (Proposition 14.70), and so

$$(a^{-1})^i a^i \equiv (a^{-1})^i a^j \pmod{m},$$

which gives that

$$a^{j-i} \equiv 1 \pmod{m}.$$

□

That proof is somewhat *nonconstructive*: it tells us it exists, but doesn't give much help looking for it.

It turns out that that we can calculate it. First we'll do an easier case, valid when the modulus is prime.

Theorem 16.75 (Fermat's Little Theorem)**.** *Let p be prime, and let a be an integer coprime to p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Recall that the *factorial* $n!$ of a natural number n is the product $1 \times 2 \cdots \times n$ of all the integers from 1 to n. We'll be thinking about $(p-1)!$ modulo p.

Consider also the product

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a).$$

The first way of thinking about it is that that's $(p-1)!$ but with every term multiplied by an a, so is equal to $a^{p-1}(p-1)!$.

The second is that the product contains a copy of every nonzero residue modulo p. For example, x is in there as $(xa^{-1})a$. Even if we don't know what a^{-1} is, we know it's in there somewhere.

For example, if $p = 5$ and $a = 3$, then the resulting product

$$3 \cdot 6 \cdot 9 \cdot 12$$

contains:

- one factor congruent to 1 (mod 5), namely 6;
- one factor congruent to 2 (mod 5), namely 12;
- one factor congruent to 3 (mod 5), namely 3; and
- one factor congruent to 4 (mod 5), namely 9.

As a result, we have

$$a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a) \equiv (p-1)! \pmod{p}.$$

because we can match up the factors on each side: for each x on the right-hand side, there is $(xa^{-1})a$ on the left-hand side congruent to it.

But, putting these observations together, we have discovered that

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

But all the residues from 1 to $p-1$ are invertible, so we can cancel out all the factors that go into $(p-1)!$. That leaves us with

$$a^{p-1} \equiv 1 \pmod{p},$$

exactly as promised.

□

Lecture 17

Remark 17.76. Fermat's Little Theorem should not be confused with *Fermat's Last Theorem*. The latter says there are no solutions in positive integers to $a^n + b^n = c^n$ with $n \geqslant 3$, and was *much, much* harder to prove.

In the proof of Fermat's Little Theorem, we multiplied one representative of each invertible residue class together. It turns out we can prove a substantially more general theorem, but it's a little more complicated. First we need a definition:

Definition 17.77. *Euler's function* (sometimes known as the *totient function* $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by taking $\varphi(n)$ to be the number of integers between 1 and n (inclusive) which are coprime to n.

For example, $\varphi(p) = p - 1$ if p is prime, since every number from 1 to $p-1$ is coprime to p (and p isn't coprime to p).

For another example, $\varphi(6) = 2$, since 1 and 5 are the only numbers between 1 and 6 which are coprime to 6.

Using this concept, we can generalise Fermat's Little Theorem considerably:

Theorem 17.78 (Fermat-Euler Theorem)**.** *Let a and n be integers with* $\gcd(a, n) = 1$. *Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. The proof is exactly the same as Fermat's Little Theorem (Theorem 16.75), but we consider just the product $x_1 x_2 \cdots x_{\varphi(n)}$ of the $\varphi(n)$ integers between 1 and n which are coprime to n.

These represent exactly the invertible residue classes modulo n, and after multiplying each of them by a we still have one from each of the invertible residue classes.

We get

$$(ax_1)(ax_2)\cdots(ax_{\varphi(n)}) \equiv a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod{n},$$

by taking out all the as (like in the proof of 16.75).

We also get

$$(ax_1)(ax_2)\cdots(ax_{\varphi(n)}) \equiv x_1x_2\cdots x_{\varphi(n)} \pmod{n},$$

since (as in the proof of 16.75 again) the terms on the left are a rearrangement of the terms on the right, when viewed modulo n. As a result,

$$a^{\varphi(n)}x_1x_2\cdots x_{\varphi(n)} \equiv x_1x_2\cdots x_{\varphi(n)} \pmod{n},$$

which simplifies to

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

just as we wanted.

□

We worked with the factorial in the proof of Fermat's Little Theorem without ever needing to calculate it. It turns out we *can* calculate it, using a clever trick.

However, we'll need a fact first:

Proposition 17.79. *Let p be a prime, and let a be an integer with the property that $a^2 \equiv 1 \pmod{p}$. Then either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.*

Proof. If $a^2 \equiv 1 \pmod{p}$, then $a^2 - 1 \equiv 0 \pmod{p}$, ie $(a-1)(a+1) \equiv 0 \pmod{p}$. In other words, $p \mid (a-1)(a+1)$.

But then,by Proposition 11.61, either $p \mid a-1$ (in which case $a \equiv 1 \pmod{p}$), or $p \mid a+1$ (in which case $a \equiv -1 \pmod{p}$). □

Remark 17.80. This theorem is not true for some composite moduli! For example, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$.

I regard this as more evidence that prime moduli behave very nicely indeed!

Now, this allows us to do this:

Theorem 17.81 (Wilson's Theorem)**.** *We have $(n-1)! \equiv -1 \pmod{n}$ if and only if n is prime.*

Proof. I'll show firstly that if n is composite, we don't get $(n-1)! \equiv -1 \pmod{n}$.

Indeed, suppose that n has a factor a such that $1 < a < n$. Then we certainly have $a \mid (n-1)!$. But if $(n-1)! \equiv -1 \pmod{n}$, then $(n-1)!$ is one less than a multiple of n, and hence also one

less than a multiple of a. That's a contradiction: it can't be a multiple of a and one less than a multiple of a.

Now I'll show that if n is prime we do get $(n-1)! \equiv -1 \pmod{n}$.

Given that n is prime, the product

$$(n-1)! = 1 \cdot 2 \cdot \cdots \cdot (n-1)$$

consists of one representative of each invertible residue class.

We can pair each up with its inverse. Mostly, this splits the residues into pairs consisting of a and a^{-1}.

However, just sometimes, a might be its own inverse. But this happens exactly when $a \equiv a^{-1} \pmod{n}$, which is the same as having $a^2 \equiv 1 \pmod{n}$, which is the same as having $a \equiv 1 \pmod{n}$ or $a \equiv -1 \pmod{n}$ (by Proposition 17.79 above).

So, our product

$$1 \cdot 2 \cdot \cdots \cdot (n-1)$$

consists of a lot of pairs of inverses (whose product modulo n is 1), together with the odd ones out 1 and -1, which are self-inverse: so the product is -1 as claimed.

□

Here's an example or two:

- 4 is composite, and $(4-1)! = 3! = 6 \equiv 2 \pmod{4}$.
- 5 is prime, and $(5-1)! = 4! = 24 \equiv -1 \pmod{5}$.
- 6 is composite, and $(6-1)! = 5! = 120 \equiv 0 \pmod{6}$.
- 7 is prime, and $(7-1)! = 6! = 720 \equiv -1 \pmod{7}$.

Remark 17.82. You could use this as a way of testing if a number is prime.

As a matter of fact, it's not a good way of doing it: if we want to check a large number N, it's quicker to do trial division to see if N has any factors, than it is to multiply lots of numbers together.

But this result was psychologically important in the development of modern fast primality tests: it was the first evidence that there are ways of investigating whether a number N is prime or not by looking at how arithmetic modulo N behaves.

Lecture 18

Public Key Cryptography

In this section, we'll show off a major modern application of all the ideas above. The aim is to talk about (one small but key part of) modern cryptography.

Cryptography is the study of how to send messages in a form which cannot be read except by the intended recipients. To *encrypt* the messages is to put them in a form which cannot be read easily; to *decrypt* the messages is to take such messages and recover them in readable form.

The literature of cryptography usually talks about three people:

- **Alice** who wishes to send a private message to Bob,
- **Bob** who wishes to receive a private message from Alice, and
- **Eve** who wishes to find out what Alice is telling Bob.

Alice and Bob are of course named so as to start with the letters A and B respectively. Eve is so named because she is an *eavesdropper*, or perhaps because she is *evil*.

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message. Perhaps you've seen many of these techniques already! For example, you could substitute the letters of the alphabet according to some agreed system: then the key would describe that system and would be a list of facts like $A \mapsto Q$, $B \mapsto J$, etc.

The big disadvantage with that is that Alice and Bob have to exchange the key somehow at the beginning: if Eve can spy on that conversation, she has the key and can decrypt Alice's message just as easily as Bob can.

The problem with this old-time approach is that the same secret is used to encrypt and decrypt the message, so needs exchanging.

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.
2. Bob takes the key which tells you how to decrypt messages, the *private key*, and keeps it to himself, never telling anyone.
3. Bob takes the key which tells you how to encrypt messages, the *public key*, and shares it with everyone who wants it, with no secrecy whatsoever. In particular, he sends Alice a postcard telling her his public key. Of course Eve finds it out quickly, but Bob doesn't care.

4. Alice uses Bob's public key to encrypt a message for Bob.

5. Alice sends Bob the encrypted message.

6. Bob uses his private key to decrypt it, and read Alice's message.

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman. (A British mathematician, Cocks, invented it a few years earlier, but he was working in secret for the government, so this was not known for many years). RSA is still in very widespread use on the internet.

The secret of RSA is to work modulo pq, where p and q are (different) primes. We're going to need to do modular arithmetic mod pq, including exponentiation. So we'll need to see what Fermat-Euler says:

Proposition 18.83. *Let p and q be different primes. Then the number $\varphi(pq)$, of integers between 1 and pq coprime to pq, is given by*

$$\varphi(pq) = (p-1)(q-1).$$

Proof. The (positive) factors of pq are 1, p, q, and pq, and so these are the possible values of $\gcd(a, pq)$.

There are pq integers a between 1 and pq; we will find how many of them have $\gcd(a, pq) = 1$ by finding all the ones that don't.

There are $q-1$ integers in that range with $\gcd(a, pq) = p$, namely the multiples of p

$$p, 2p, \ldots, (q-1)p.$$

There are $p-1$ integers in that range with $\gcd(a, pq) = q$, namely the multiples of q

$$q, 2q, \ldots, (p-1)q.$$

There is one integer in the range with $\gcd(a, pq) = pq$, namely pq itself.

The ones with $\gcd(a, pq) = 1$ are the ones left over, and there are

$$pq - (q-1) - (p-1) - 1 = (p-1)(q-1)$$

of them.

□

Remark 18.84. As a result of that, we know (from the Fermat-Euler Theorem17.78) that, for all a coprime to pq, we have

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq},$$

and indeed

$$a^{k(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

for all k.

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

His public key consists of pq and e, so he sends that to Alice (and Eve); his private key consists of pq and d. He shreds any evidence of what p and q are.

Alice represents her message as a number m between 1 and pq. It is overwhelmingly likely that her choice will be coprime to pq. She calculates

$$m^e \pmod{pq}$$

and sends it on to Bob.

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$$(m^e)^d = m^{de} = m^{1+k\varphi(pq)} = m(m^{\varphi(pq)})^k \equiv m1^k \equiv m \pmod{pq}.$$

Hence, using his private key, Bob can recover what m was from being told m^e.

The idea is that it should be very hard for anyone else to work out d from pq and e; we did this using Euclid's algorithm, but we needed to know more than just pq: we needed to know $(p-1)(q-1)$.

So the security of this approach depends (among other things) on it being difficult to factorise the number pq: if factorising large numbers were easy, we could get p and q for ourselves from Bob's public key. Currently, we know of no way to do this fast enough: we know how to generate primes that are hundreds of digits long, but not to factorise a product of two of them.

Let's see an example.

Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.

Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.

Suppose Alice decides she needs to send Bob message 1245, which they've agreed in advance should mean "please meet me after this lecture".

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\
&\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\
&\equiv 7065 \cdot 6994 \equiv 8763.
\end{aligned}$$

So she sends Bob 8763.

Bob receives this, and his task then is to calculate 8763^{431} modulo 10403. A similar strategy makes this possible, too, and he finds that

$$8763^{431} \equiv 1245 \pmod{10403},$$

so he has reconstructed Alice's message.

The real numbers

Irrational numbers

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.

Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it? Why should we feel that $\mathbb{Q}$ is not enough?

The result that set the ancient Greeks thinking was this:

Theorem 18.85. *There is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$.*

Proof. We'll prove this by contradiction; suppose there is such a number $x \in \mathbb{Q}$. Because it's in $\mathbb{Q}$, it takes the form $x = p/q$ for some integers p and q with $q \neq 0$.

We may as well take p and q to be coprime ("in lowest terms").

Then we have $p^2/q^2 = x^2 = 2$, so $p^2 = 2q^2$ with p and q coprime.

Now, the right-hand side is even (it's given as a multiple of 2, so the left-hand side, p^2 must be even too. That means that p itself must be even: so we can write $p = 2r$.

Then we have $(2r)^2 = 2q^2$, which simplifies to $4r^2 = 2q^2$, or $2r^2 = q^2$. Here the left-hand side is even, so q^2 must be even. Hence q itself must be even.

But now we've found that both p and q are even, which is a contradiction since we chose them to be coprime. This contradiction shows that our initial assumption is absurd, and there is no rational x with $x^2 = 2$.

□

Lecture 19

Remark 19.86. I felt obliged to word the statement of that theorem fairly carefully.

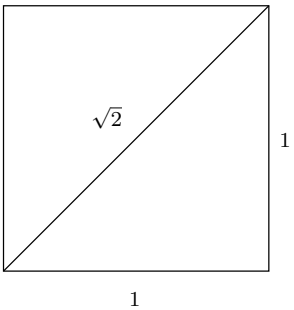
What I wanted to say, of course, was:

> The number $\sqrt{2}$ is not in $\mathbb{Q}$.

But I want to flag that up as being possibly inappropriate: our aim in this section is to say something intelligent about systems of numbers bigger than $\mathbb{Q}$. We shouldn't even be confident that $\sqrt{2}$ exists yet.

However, thanks to this theorem, we can be confident at least that there's no number *inside* $\mathbb{Q}$ which deserves to be called $\sqrt{2}$.

This, to the Greeks, was evidence that there was a world beyond $\mathbb{Q}$; a world of *irrational numbers* (numbers not in $\mathbb{Q}$). They needed a number called $\sqrt{2}$, so they could talk about the diagonal of a unit square:



Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

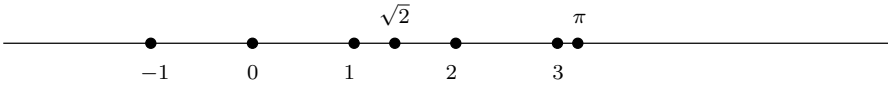
On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please...) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e, \quad \pi e, \quad \pi/e, \quad \ln \pi, \quad e^e, \quad e^{e^e}.$$

For centuries, the real numbers were considered in an informal way: nobody knew exactly how to define $\mathbb{R}$, but they knew what it ought to look like.

For the time being, and *for the time being only* we'll investigate the reals in a similar, informal way. For now, you can regard the real numbers $\mathbb{R}$ as being built out of decimals (as you did at school). In the last lecture of the course, we'll sort this out, and consider a modern construction of the reals.

Our mental picture of the reals should be a picture of a numberline. Here's a numberline with some interesting points marked on:



I've marked on the integers -1, 0, 1, 2 and 3, which are all in $\mathbb{Z}$ and hence in $\mathbb{Q}$.

I've also marked on $\sqrt{2}$, which we now know to be irrational, and π, which I've claimed to you is irrational: these things are in the set $\mathbb{R}\backslash\mathbb{Q}$ of irrational numbers.

In my mind, I think of the real numbers $\mathbb{R}$ as a solid line, and the rational numbers $\mathbb{Q}$ as a very fine gauze net stretched out within it.

Bear in mind that that the rationals $\mathbb{Q}$ are a lovely system of numbers: we can add and subtract and multiply and divide rationals and remain inside the rationals. Formally: if $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$, then $x + y$, $x - y$, xy and x/y (if y is nonzero) are all elements of $\mathbb{Q}$. We say that $\mathbb{Q}$ is *closed* under addition, subtraction, multiplication and division.

The reals $\mathbb{R}$ are also a lovely system of numbers, closed not just those four operations but many others: square roots (of positive numbers), sines, cosines, and so on.

The irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ are not a lovely system of numbers: they are not closed under any of these things.

For example, can we think of two irrational numbers whose sum is rational?

$$\sqrt{2} + (1 - \sqrt{2}) = 1.$$

Can we think of two irrational numbers whose product is rational?

$$\left(\sqrt{2}\right)\left(\sqrt{2}\right) = 2.$$

So, the irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ really are just the big messy clump left over in $\mathbb{R}$ when you remove $\mathbb{Q}$. It's a bit weird we even have a name for these: I don't know a good name for the set $\mathbb{Q}\backslash\mathbb{Z}$ of rationals which aren't integers.

However, at least the following is true (and almost obvious):

Proposition 19.87. *Let x be irrational, and y be rational. Then $x + y$ is irrational.*

Also, if y is nonzero, then xy is irrational.

Proof. We prove the first one by contradiction. Suppose that $x + y$ is rational. Then $(x + y) - y$ is also rational, being obtained by subtracting two rational numbers, but it's equal to x which we know to be irrational. That's the contradiction we wanted.

We prove the second one by contradiction too. Suppose that xy is rational. Then $(xy)/y$ is also rational, as it's obtained by dividing two rational numbers (with the latter nonzero), but it's equal to x which we know to be irrational. That's the contradiction we wanted.

□

Convergent sequences

Now our mission is to study the real numbers. When we were studying the integers, the main theme running through it all was to do with divisibility. Divisibility is, of course, not a very sensible thing to ask about over the reals.

As a result, real analysis (the study of $\mathbb{R}$), and the questions which are interesting and helpful to ask, is very different to number theory.

It turns out that the most interesting things you can ask about are to do with *approximation*. Why is the notion of approximation so important?

When we write that

$$\pi = 3.14159265358979323846264 33\cdots,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

The notion of *convergence*, which I'll define shortly, is a way of encoding this concept of increasingly good approximation. We will say that the series of rational numbers

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

"converges to π". That's supposed to mean that if you follow the address, you'll end up homing in on π.

The definition will seem complicated, and probably harder to get your head around than other definitions in the course. However, that's because it really is a subtle concept: all the simpler approaches you might think of are wrong.

The most obvious wrong definition is this:

***Completely wrong* definition 19.88.** A sequence *converges to* x if it gets closer and closer to x.

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$\begin{aligned} 1000 - 3 &= 997 \\ 1000 - 3.1 &= 996.9 \\ 1000 - 3.14 &= 996.86 \\ 1000 - 3.141 &= 996.859 \\ 1000 - 3.1415 &= 996.8585 \end{aligned}$$

Of course, this sequence never gets particularly close to 1000 (the sequence never goes above 4, so it never gets within 996 of π).

But this means that if our definition of "converging to x" were the completely wrong definition "gets closer and closer to x", then the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

would "converge to π", but it would also "converge to 1000".

But that's not what we want: this sequence is a terrible way of getting to 1000, and an awesome way of getting to π.

Here's a slightly better idea:

***Completely wrong* definition 19.89.** A sequence *converges to* x if it gets as close as you like to x.

Before we understand why this is wrong, we ought to make sure we know what this is supposed to mean.

I like to think of it as an argument with a very dangerous and unpleasant *evil opponent*. The evil opponent gets to choose a (positive real) distance, and we win if the sequence gets within that distance of x, and we lose if it doesn't.

In order to be *sure* of winning, we have to know how to beat the evil opponent whatever they say.

So, in investigating how close the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots,$$

gets to 1000, then if the evil opponent is stupid enough to ask "does the sequence get within distance 100000?" we'll win. But, being an evil *genius*, they probably won't ask that. Instead they'll ask "does the sequence get within distance 0.001 of 1000?", and we'll lose, because it never gets anywhere near there.

On the other hand, if we're investigating how close the sequence gets to π, we win no matter what they say. If they ask "does the sequence get within distance 1000000 of π?", then we say "yes, 3 is within 1000000 of π", and win. If they ask "does the sequence get within distance 0.0001 of π, then we say "yes, 3.14159 is within 0.0001 of π", and win. If they ask a question with an even tinier positive number in, we just take more digits and use that and say "yes". We're happy: the evil opponent will not beat us.

Formally, if we have a sequence

$$a_0, \quad a_1, \quad a_2, \quad a_3, \ldots$$

that gets very close to x in this sense, one could specify this concept as

$$\forall \epsilon > 0, \quad \exists n \in \mathbb{N} \quad \text{s.t.} \quad |a_n - x| < \epsilon.$$

In our minds, this says "no matter what ϵ our evil opponent chooses, we can find some term a_n of the sequence such that a_n is within ϵ of x".

This is a much better concept. But it's still not right.

Here's an example of what could go wrong. Consider the sequence

$$1.1, \quad 2.01, \quad 1.001, \quad 2.0001, \quad 1.00001, \quad 2.000001, \quad \ldots$$

Does it converge to 1? Does it converge to 2?

It's lousy as an address for either: if we give these instructions to the numberline's village postal worker, they'll get very annoyed as they keep walking from somewhere near 1 to somewhere near 2 and back again.

But according to the definition above it would "converge" to both, because it gets as close as you like to 1 and it also gets as close as you like to 2.

Lecture 20

So we need to find some way of saying that it has to make its mind up eventually. The obvious thing to do is to say is that (for any $\epsilon > 0$) it has to get within ϵ of x, and then stay within ϵ of x forever.

This leads us to our final definition:

Definition 20.90. Let x be a real number. A sequence of real numbers $a_0, a_1, a_2, \ldots$ is said to *converge to* x if we have

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} \quad \text{s.t.} \quad \forall n > N, \quad |a_n - x| < \epsilon.$$

So that says "no matter what positive real ϵ our evil opponent gives us, we can point out some N, such that all the terms $a_{N+1}, a_{N+2}, a_{N+3}, \ldots$ are all within ϵ of x".

That does an excellent job of making precise the concept of "gets close and stays close forever", and it's the right definition!

Now, suppose we ask whether the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

converges to π. It does, because no matter what ϵ our evil opponent asks about, we can find some term of the sequence beyond which all terms are within ϵ of π. For example, all terms after the $(N+1)$st term are within 10^{-N} of π.

Does that converge to 1000? No, it never comes within 1 of 1000 (for example), so it certainly doesn't stay within 1 of 1000 forever.

What about the sequence

$$a_0 = 1.1, \quad a_1 = 2.01, \quad a_2 = 1.001, \quad a_3 = 2.0001, \quad \ldots?$$

Does that converge to anything?

No, it doesn't. In particular, it doesn't converge to 1, because while it's sometimes close to 1, it's also sometimes close to 2. So there is no N where a_n is always within 0.1 of 1 for all $n > N$: all the odd-numbered a_n aren't in that range.

Similarly, it doesn't converge to 2, because while it's sometimes close to 2, it's sometimes close to 1. So there is no N where a_n is always within 0.1 of 2 for all $n > N$: all the even-numbered a_n aren't in that range.

So, given the difficulties we've had in finding the right definition, perhaps you'll have some sympathy for the fact that it took about two centuries to sort real analysis out properly. In what remains of the course I'll try to make you like this definition.

Convergence proofs

Let's take a brief detour to remind you of something that you probably know, but whose importance may not have been pointed out to you. The *triangle inequality* says that

$$|x| + |y| \geqslant |x + y|$$

for any real numbers x and y. It's easy to prove, by carefully analysing what can happen: which combinations of signs of x, y and $x + y$ are possible?

We can use this to get the following:

$$|z - y| + |y - x| \geqslant |(z - y) + (y - x)| = |z - x|.$$

This embodies the following slogan:

> The distance from x to z if we go direct is less than if we go via y.

Now we get back to the subject of convergence.

We say that a sequence $(a_i)_{i\in\mathbb{N}} = a_0, a_1, \ldots$ is *convergent* if it converges to some x.

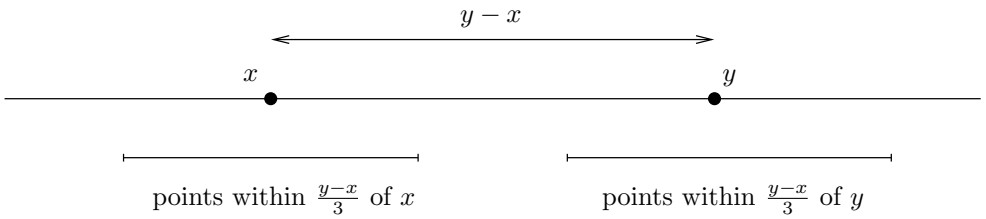
Here's a very important fact (which is only true because of all that work we put in finding a good definition):

Proposition 20.91. *A sequence $a_0, a_1, \ldots$ cannot converge to two different real numbers x and y.*

Proof. We'll prove this by contradiction. So, suppose it can: suppose that there is a sequence $a_0, a_1, \ldots$, which converges to two different real numbers x and y. Without loss of generality, we may take $x < y$.

Now the definition of convergence says that the sequence eventually gets and stays as close as we like to both x and y: this should be a contradiction since x and y are not all that close together.

Here's a picture of a numberline, to help show us what to do:



The two bars at the bottom of that diagram were deliberately chosen not to overlap (I made each of them extend one third of the distance from x to y, leaving another third of the distance between them in the middle).

And since it converges to x and y, the sequence should end up living within both those bars, which is a contradiction. Let's do the working carefully.

Since the sequence $a_0, a_1, \ldots$ converges to x, there is some N such that, for all $n > N$, we have

$$|a_n - x| < \frac{y-x}{3}.$$

Since the sequence $a_0, a_1, \ldots$ converges to y, there is some M such that, for all $n > M$, we have

$$|a_n - y| < \frac{y-x}{3}.$$

But then, using the triangle inequality, for any n bigger than both N and M, we have

$$y - x = |y - x| \leqslant |y - a_n| + |x - a_n| < \frac{y-x}{3} + \frac{y-x}{3} = \frac{2}{3}(y-x)$$

which is certainly a contradiction as $y - x$ is positive.

□

Remark 20.92. As a result, if a sequence is convergent, there is a unique real number to which it converges; we call that the *limit* of the sequence.

Let's now try proving that some sequence or other does converge, as we're not well practiced at that yet:

Proposition 20.93. *The sequence*

$$0, \quad 1/2, \quad 2/3, \quad 3/4, \quad 4/5, \quad \ldots$$

where $a_n = \frac{n-1}{n}$, *converges to* 1.

Rough version. The definition of convergence is complicated, so it may be helpful to start by reminding us what we're aiming for. So we'll start by working from the wrong end.

We need to show that, for every $\epsilon > 0$, there is some N, such that for all $n > N$ we have

$$\left|\frac{n-1}{n} - 1\right| < \epsilon.$$

The most obvious thing to do is to simplify the stuff in the absolute value brackets:

$$\left|\frac{n-1}{n} - 1\right| = \left|\frac{(n-1)-n}{n}\right| = \left|\frac{-1}{n}\right| = \frac{1}{n}.$$

So, as we can see, what we're aiming for is that, for every $\epsilon > 0$ there is some N, such that for all $n > N$ we have

$$\frac{1}{n} < \epsilon.$$

But that's the same as having

$$n > \frac{1}{\epsilon}.$$

So if we take N to be $\lceil \frac{1}{\epsilon} \rceil$, the smallest integer greater than $1/\epsilon$, that works.

□

That proof is sort-of-okay, but it's backwards. It was helpful to write it, but hard to check that it's logically valid. I'll now rewrite it forwards.

Neat version. We must show that, for every $\epsilon > 0$, there is some N such that for all $n > N$ we have

$$\left|\frac{n-1}{n} - 1\right| < \epsilon.$$

Let such an ϵ be given.

Define N to be $\lceil \frac{1}{\epsilon} \rceil$, which is the smallest integer greater than $1/\epsilon$.

Then, if $n > N$, we have

$$\left|\frac{n-1}{n} - 1\right| = \left|\frac{(n-1)-n}{n}\right| = \left|\frac{-1}{n}\right| = \frac{1}{n} < \frac{1}{N} < \frac{1}{1/\epsilon} = \epsilon,$$

exactly as required. □

That second version is obviously correct, and all the reasoning goes in the right direction. But analysis proofs often have the property that the best proof seems a bit mysterious. It's best to do the rough work and then rewrite it neatly.

I understand you will have covered the subject of convergence in MAS110.

That course is about streetfighting, and you're encouraged to use any technique you have to hand.

This is a course about fundamental techniques in mathematics and their proofs: if I set problems about convergence in MAS114, I need you to give a rigorous proof, only the definition of convergence (unless you're told otherwise), rather than using the slightly vaguer methods and extra theorems you saw there!

Lecture 21

Let's do another example:

Proposition 21.94. *The sequence defined by* $a_n = \frac{3^{n+1}}{3^n+1}$ *converges to* 3.

Rough version. We need to show that, for all $\epsilon > 0$, there exists some N such that, for all $n > N$, we have

$$|a_n - 3| < \epsilon.$$

We can rearrange the thing we're trying to work with:

$$\begin{aligned} |a_n - 3| &= \left|\frac{3^{n+1}}{3^n+1} - 3\right| \\ &= \left|\frac{3^{n+1}}{3^n+1} - \frac{3(3^n+1)}{3^n+1}\right| \\ &= \left|\frac{3^{n+1}-3(3^n+1)}{3^n+1}\right| \\ &= \left|\frac{3^{n+1}-3^{n+1}-3}{3^n+1}\right| \\ &= \left|\frac{-3}{3^n+1}\right| \\ &= \frac{3}{3^n+1}. \end{aligned}$$

So, in other words, we need to show that, for all $\epsilon > 0$, there exists some N such that, for all $n > N$, we have

$$\frac{3}{3^n+1} < \epsilon.$$

This rearranges to

$$\frac{3}{\epsilon} < 3^n + 1,$$

or

$$\frac{3}{\epsilon} - 1 < 3^n,$$

or

$$\log_3(3/\epsilon - 1) < n.$$

Hence if we take $N = \lceil \log_3(3/\epsilon - 1) \rceil$, the smallest integer greater than $\log_3(3/\epsilon - 1)$. this will work.

□

As before, here's a less informative, shorter version of the same maths:

Neat version. We need to show that, for all $\epsilon > 0$, there exists some N such that, for all $n > N$, we have

$$|a_n - 3| < \epsilon.$$

Suppose given some ϵ; we'll show that $N = \lceil \log_3(3/\epsilon - 1) \rceil$

works. Indeed, we have

$$\begin{aligned}
|a_n - 3| &= \left| \frac{3^{n+1}}{3^n + 1} - 3 \right| \\
&= \left| \frac{3^{n+1}}{3^n + 1} - \frac{3(3^n + 1)}{3^n + 1} \right| \\
&= \left| \frac{3^{n+1} - 3(3^n + 1)}{3^n + 1} \right| \\
&= \left| \frac{3^{n+1} - 3^{n+1} - 3}{3^n + 1} \right| \\
&= \left| \frac{-3}{3^n + 1} \right| \\
&= \frac{3}{3^n + 1} \\
&< \frac{3}{3^N + 1} \qquad \text{(since } N < n\text{)} \\
&= \frac{3}{3^{\lceil \log_3(3/\epsilon - 1) \rceil} + 1} \\
&\leqslant \frac{3}{3^{\log_3(3/\epsilon - 1)} + 1} \\
&= \frac{3}{3/\epsilon - 1 + 1} \\
&= \frac{3}{3/\epsilon} \\
&= \epsilon,
\end{aligned}$$

exactly as required.

□

Some more systematic methods

The examples above seem like a lot of work. In fact, they are a lot of work: the definition of convergence is genuinely complicated, so it's no surprise that it takes time when you have to use it.

However, real analysts know many situations that crop up repeatedly, and know many useful facts for saving them time in those situations.

One useful one is the following:

Theorem 21.95 (Sandwich Lemma)**.** *Suppose we have three sequences:* $a_0, a_1, a_2, \ldots$, *and* $b_0, b_1, b_2, \ldots$ *and* $c_0, c_1, c_2, \ldots$, *such that:*

(i) *the sequences* $(a_i)_{i\in\mathbb{N}}$ *and* $(c_i)_{i\in\mathbb{N}}$ *both converge to the same number* x*; and*

(ii) *for all* i *we have*

$$a_i \leqslant b_i \leqslant c_i$$

Then the sequence $(b_i)_{i\in\mathbb{N}}$ *also converges to* x*.*

I write only the neat version of the proof.

Proof. We must show that, for all ϵ, there is an N such that, for all $n > N$

$$|b_n - x| < \epsilon,$$

or in other words, for all $n > N$ we have

$$b_n - \epsilon < x < b_n + \epsilon.$$

Suppose given such an ϵ. Since $(a_i)_{i\in\mathbb{N}}$ converges to x, there is an M such that, for all $n > M$, we have

$$|a_n - x| < \epsilon,$$

or in other words

$$a_n - \epsilon < x < a_n + \epsilon.$$

Since $(c_i)_{i\in\mathbb{N}}$ converges to x, there is also an P such that, for all $n > P$, we have

$$|c_n - x| < \epsilon,$$

or in other words

$$c_n - \epsilon < x < c_n + \epsilon.$$

Given that, I claim we can take N to be $\max(M, P)$, the larger of M and P. Then we have

$$b_n - \epsilon \leqslant c_n - \epsilon < x < a_n + \epsilon \leqslant b_n + \epsilon,$$

as required. Here the outer two inequalities are because $a_i \leqslant b_i \leqslant c_i$ for all i, and the inner two are obtained from the convergence of $(a_i)_{i\in\mathbb{N}}$ and $(c_i)_{i\in\mathbb{N}}$.

□

The usefulness of this result is that we can ignore complicated features of sequences by "sandwiching" them between simpler things.

For example, using this we can show that the sequence

$$b_n = 3 + \frac{\sin(n^{7n} - \sqrt{n})}{n}$$

converges to 3.

The mess inside the sin brackets is extremely unpleasant, and we'd love to not have to work with it.

However, we can proceed by sandwiching it between $a_n = 3 - \frac{1}{n}$ and $c_n = 3 + \frac{1}{n}$ (since all values of sin are always between -1 and 1). Showing that those two sequences both converge to 3 is simple(it's a simple modification of Proposition 20.93 above).

Another sensible question to ask is to do with combining sequences. Here we'll talk about addition:

Theorem 21.96. *Let $a_0, a_1, \ldots$ be a sequence that converges to x, and let $b_0, b_1, \ldots$ be a sequence that converges to y. Then the sequence*

$$a_0 + b_0, \quad a_1 + b_1, \quad \ldots$$

converges to $x + y$.

We'll give just a neat version of the proof. The idea is that in order for a sum to be close, we can tolerate each summand being up to half the permitted distance away.

Proof. We must show that for all $\epsilon > 0$, there is some N such that for all $n > N$ we have

$$|(a_n + b_n) - (x + y)| < \epsilon.$$

Suppose we are given such an ϵ.

Since the sequence $(a_i)_{i \in \mathbb{N}}$ converges to x, there is some R such that for all $n > R$ we have

$$|a_n - x| < \frac{\epsilon}{2},$$

and since $(b_i)_{i \in \mathbb{N}}$ converges to y, there is some S such that for all $n > S$ we have

$$|b_n - y| < \frac{\epsilon}{2}.$$

That means that, if we take $N = \max(R, S)$ then for all $n > N$ we have

$$|(a_n + b_n) - (x + y)| \leqslant |a_n - x| + |b_n - y| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

There the first inequality is an instance of the triangle inequality. This is what we need.

□

A very similar argument will do subtraction.

It's also true that the sequence

$$a_0 b_0, \quad a_1 b_1, \quad a_2 b_2, \quad \dots$$

converges to xy, and that (if y and all the terms b_i are nonzero), that

$$a_0/b_0, \quad a_1/b_1, \quad a_2/b_2, \quad \dots$$

converges to x/y. These are slightly (but not much) harder.

There are many, many more facts about convergent sequences, but I'll leave it there. Ultimately the aim should not be to memorise facts, but to have enough tools that you can prove them yourself, as needed.

Cauchy sequences

We have said what it means for a sequence to converge to a number.

We're now going to explore a concept which says that a sequence "ought to converge to something (but we're not sure what)".

Recall that a sequence converges to x if, no matter what you mean by "close", the sequence eventually gets close to x and stays close to x forever. In symbols, that was

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} \quad \text{s.t.} \quad \forall n > N, \quad |a_n - x| < \epsilon.$$

If a sequence ought to converge to something, then its terms ought to "settle down" somehow. That means they should at least get close at least to each other.

This leads us to the following definition:

Definition 21.97. A sequence $a_0, a_1, a_2, \dots$ is said to be *Cauchy* if

$$\forall \epsilon > 0, \quad \exists N \in \mathbb{N} \quad \text{s.t.} \quad \forall m, n > N, \quad |a_m - a_n| < \epsilon.$$

In vaguer terms, a sequence is Cauchy if no matter what we mean by close, there is some point beyond which all the terms of the sequence are close to each other.

It's possible to prove that a sequence is Cauchy directly from the definition. Here's the simplest possible example:

Proposition 21.98. *A constant sequence is Cauchy.*

Proof. Let $a_0, a_1, a_2, \ldots$ be a constant sequence with value a; that is, $a_n = a$ for all n.

We must show that, for any rational $\epsilon > 0$, there is an N such that, for all $m, n > N$, we have $|a_m - a_n| < \epsilon$.

In fact, no matter what ϵ is, we can choose $N = 0$, because for any m and n whatsoever we have

$$|a_m - a_n| = |a - a| = |0| = 0 < \epsilon,$$

so the proof is done. □

Of course, usually we have to choose N in a way which actually depends on ϵ; it's only in very special cases like these that we can choose one N for every ϵ.

Lecture 22

In fact, more is true:

Theorem 22.99. *Any convergent sequence is Cauchy.*

Proof. Suppose we have a sequence $a_0, a_1, \ldots$ converging to x. We must show that it is Cauchy.

So suppose we're given some $\epsilon > 0$: we must find some N such that, for all $m, n > N$ we have

$$|a_m - a_n| < \epsilon.$$

Since it is convergent, there is an N such that for all $n > N$ we have

$$|a_n - x| < \frac{\epsilon}{2}.$$

We'll use that N; because then we have

$$\begin{aligned} |a_m - a_n| &\leqslant |a_m - x| + |a_n - x| \qquad \text{(by the triangle inequality)} \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &= \epsilon, \end{aligned}$$

exactly as required. □

How to construct $\mathbb{R}$

Now we have the tools to understand what the reals really are (no pun intended).

Let's give it in context. What follows is *revisionist history*: things didn't actually happen exactly like this, but maybe they should have done.

- In the beginning there was $\mathbb{N}$;
- $\mathbb{Z}$ was invented from $\mathbb{N}$ by insisting that one should be able to subtract.

  In other words, new numbers were invented, in order to be the values obtained by previously impossible subtractions in the naturals. So we invented -2 to be $0-2$ and -137 to be $0-137$.

  You don't want one new number for each subtraction. For example, we want to have $5-7=-2$ and $1000000-1000002=-2$, as well.

  But that's okay: the theory is workable, and we get $\mathbb{Z}$ by doing it. Nobody gets confused about which integers are equal. We can make definitions like

  $$a-b=c-d \qquad \text{if and only if } a+d=b+c.$$

- $\mathbb{Q}$ was invented from $\mathbb{Z}$ by insisting that one should be able to divide (by things that aren't zero).

  In other words, new numbers were invented, in order to be the values obtained by previously impossible divisions in the integers.

  So we invented $1/5$ and $-3/7$ accordingly.

  Again, we don't want one new number for each division. We also have $100/500=-2/-10=1/5$. But that's okay as well, and we don't get confused. We can make definitions like

  $$a/b=c/d \qquad \text{if and only if } ad=bc.$$

- $\mathbb{R}$ was invented from $\mathbb{Q}$ by insisting that all Cauchy sequences of rationals should converge.

  In other words, new numbers were invented, in order to be the limits of Cauchy sequences of rationals which don't converge to a rational.

  So, for example, we get π as the limit of the Cauchy sequence of rationals

  $$\begin{array}{llllll} 3, & 3.1, & 3.14, & 3.141, & 3.1415, & \dots \\ 3, & \dfrac{31}{10}, & \dfrac{314}{100}, & \dfrac{3141}{1000}, & \dfrac{31415}{10000}, & \dots. \end{array}$$

Again, we don't actually want one new number for each Cauchy sequence. There are other Cauchy sequences of rationals that converge to π (some of them more interesting, perhaps). A famous example is due to Gregory and Leibniz:

$$4, \quad 4 - \frac{4}{3}, \quad 4 - \frac{4}{3} + \frac{4}{5}, \quad 4 - \frac{4}{3} + \frac{4}{5} - \frac{4}{7}, \quad \ldots.$$

One minor issue to be clear about is which numbers we take in the definition of a Cauchy sequence of rationals.

We demand that something be true for "every positive ϵ". That had better mean "every positive *rational* ϵ" (I'd been being vague about what ϵ was). In fact it won't make any difference in meaning.

But then, given that, we could just say that the reals *are* the Cauchy sequences of rationals, subject to some restriction about which ones are the same.

We need to know how to say that two Cauchy sequences "are trying to converge to the same number", in order to say when they're describing the same rule.

There are a number of different definitions we could use, all providing the same results. Perhaps the clearest is that two Cauchy sequences $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ of rationals converge to the same real number if, for all rational $\epsilon > 0$, there is some N such that for all $m, n > N$ we have

$$|a_m - b_n| < \epsilon.$$

We might regard this as saying "no matter what is meant by close, the two sequences get close to each other and stay close to each other forever".

This seems a very sensible way of describing the real numbers: it says that they fill in the gaps in the rationals, the things that sequences might try to converge to.

In particular, I hope you agree that it's a more natural way of understanding the reals than talking about decimal expansions.

If you *insist* on working with decimals, then you can do so happily with Cauchy sequences of rationals. For example, suppose that you insist on talking about the decimal

$$1.414213562373\cdots$$

(This happens to be the decimal expansion of the square root of 2.)

Then this can be accommodated in our construction easily, using the trick I mentioned earlier: we can represent it as the limit of the Cauchy sequence

$$1, \quad \frac{14}{10}, \quad \frac{141}{100}, \quad \frac{1414}{1000}, \quad \frac{14142}{10000}, \quad \ldots.$$

But that Cauchy sequence doesn't seem too exciting. There are others, and some of them tell us more about what the square root of 2 really is.

For example, there's the Newton iteration scheme. The details of this are not really part of this course, but it tells us that if x is an approximation to $\sqrt{2}$, then

$$\frac{x}{2} + \frac{1}{x}$$

is a better approximation.

If we start with 1 as an approximation, then this gives us the sequence

$$1, \quad \frac{3}{2}, \quad \frac{19}{12}, \quad \frac{577}{408}, \quad \frac{665857}{470832}, \ldots$$

It's not hard to imagine that this is a much better way of describing $\sqrt{2}$ than its decimal expansion: easier to prove things about it than some weird string of digits.

Decimal expansions are, of course, still useful for dealing with approximate forms of reals. But it's nice to have alternatives, and extremely useful to have a system that doesn't depend on them.

Quite a lot of pre-20th century mathematics can be regarded as giving interesting facts about Cauchy sequences of rationals, either in general or in specific instances. These facts I've given you for π and $\sqrt{2}$ are just two parts of a very rich tapestry!

What's next?

If you liked some of the topics in this course, may be wondering what's next.

So far as number theory goes, our elementary methods will give out sooner or later. A good next step is to learn lots of algebra. (There are other good reasons to do that.) Next semester, Sam will take this up. You can return later in your degrees to a huge range of questions of which equations are solvable in which systems of numbers.

The way forward with real analysis is much more straightforward.

From where you are, it's easy to define the derivative formally and start proving things about it. You're probably not scared of differentiation, but you perhaps *should* be cautious of differentiating functions of several variables.

Integration is a bit more technical, and will require more work.

Sooner or later, you can try using the same techniques in more exotic surroundings: the concepts of approximation we started talking about in this course give us a way in to studying abstract concepts of space.

Index