Summer School in Mathematics, 2022
The Congruent Number Problem

Sjoerd de Vries, Stockholm University

Introduction

These are notes for a summer school taught in June 2022 at Stockholm University. It was a two-week school for high school students in their penultimate year, and meant to give an impression of what research in mathematics is like. The notes are meant to give an accessible introduction to the congruent number problem and several areas of university-level maths. A student learning about these topics for the first time should probably try to focus on one specific topic and try to get familiar with this, rather than try to understand everything.

The schedule of the summer school was as follows. In the first week, I taught the material from these notes, with the time divided roughly equally between lessons and exercise sessions. The second week was dedicated to projects of the students' choosing, either in groups or individually, concluding with a presentation by each group.

I am sharing these notes in the hope that other teachers will find it inspiring or useful for their own teaching, but perhaps they will also be useful for beginning mathematicians learning about one or more of the topics covered.

Contents

1. Project description

This chapter can be seen as an introduction to the summer school. I will sketch an idea of the kind of maths we will be working with, and introduce a particular problem (the *congruent number problem*) that could be the subject of your project. On the other hand, if you feel like this kind of problem isn't very interesting, or if there is another mathematical problem that fascinates you, I encourage you to explore that in your project instead. Finally, you don't need to understand everything in this project description - but the hope is that you will understand it after the two weeks are over. Have fun!

1.1 Pythagorean triples

Let's start off with something familiar. You know from school that a right-angled triangle satisfies Pythagoras's theorem: if the side lengths are a, b and c, with c being the length of the hypotenuse, then $a^2 + b^2 = c^2$.

This is a very nice equation. In particular, what's nice about it is that all the coefficients are integers. This means that we can look at the equation

$$X^2 + Y^2 = Z^2$$

and ask what solutions (X, Y, Z) exist, not only when X, Y and Z are any positive real numbers (that's not so interesting), but also in the particular case when X, Y and Z are integers. If we have such an integer solution where all of the numbers are positive, we say (X, Y, Z) is a *Pythagorean triple.*

Number theorists are often interested in equations of the above form, and they might ask the following questions:

- Do any Pythagorean triples exist?
- If so, how many? Are there infinitely many?
- Even if there are infinitely many, can we find a formula or algorithm to describe them all?

You probably know some Pythagorean triples: for example, $(3, 4, 5)$ is a solution, as is $(5, 12, 13)$. So the first question has a positive answer. In fact, it turns out that all of these questions have a positive answer - and we will see how to get to the solution at a later point in the summer school.

For some reason, it tends to be the case that many easily formulated questions in number theory are extremely difficult to answer. Sometimes mathematicians simply don't know how to answer them, and sometimes it has even been proved that no answer exists! (Google "Hilbert's tenth problem" if you're interested.) For example, if you change the above equation to

$$X^n + Y^n = Z^n,$$

where now n is a positive integer which is at least 3, you can ask the same questions. Pierre de Fermat conjectured around 1637 that this equation actually never has any positive integer solutions. Since then, mathematicians have been trying to prove it - and for centuries, nobody knew how. In 1994, Andrew Wiles finally completed his proof of Fermat's conjecture (better known as Fermat's Last Theorem), using incredibly complicated and deep mathematics. As of today, there are many number-theoretic problems which are similarly easy to state, but which are still wide open.

1.2 The congruent number problem

Let's move on to a related problem: the congruent number problem. We'll begin by defining what a congruent number is.

Definition 1.2.1. A positive integer n is said to be a *congruent number* if it can be obtained as the area of a right-angled triangle with rational side lenghts.

A rational number is nothing else than a fraction, i.e. a number of the form $\frac{p}{q}$ for integers p and q, with $q \neq 0$. So compared to the Pythagorean setting, we have made a step: whereas first we considered only triangles with integer side lengths, we now allow them to be rational. The congruent number problem can now be stated as follows:

Which positive integers are congruent numbers?

In other words, if I give you a number n, say 41, I want you to be able to tell me whether or not that number can be obtained as the area of a triangle with rational side lengths. If you can do this for any n, you have solved the congruent number problem.

When you think about it, this really seems like a hard problem. Of course, you can come up with some congruent numbers: for example, for each Pythagorean triple, you get that the area of the corresponding triangle is a congruent number. The triple $(3, 4, 5)$ gives that $n = \frac{1}{2} \cdot 3 \cdot 4 = 6$ is a congruent number. But what about numbers for which you can't easily find such a triangle? You can't just try every possible triangle, because there are infinitely many rational numbers. Can you still decide whether or not such a triangle exists?

The congruent number problem is actually unsolved at the moment. There is a conjectural solution - but it depends on one of the Millenium Prize Problems, namely the Birch and Swinnerton-Dyer conjecture. If you prove this conjecture, you win a million dollars, and you also confirm that the congruent number problem has a nice solution.

Let's try to attack the congruent number problem a little. We can rewrite the definition as follows: n is a congruent number if and only if there exist rational numbers a, b and c such that the following hold:

$$a^2 + b^2 = c^2; \tag{1.1}$$

$$n = \frac{a \cdot b}{2}. \tag{1.2}$$

Given such a triple (a, b, c) of rational numbers, we can transform it into something else, namely a triple (s, t, u) with the following properties:

$$s^2 + n = t^2; \tag{1.3}$$

$$t^2 + n = u^2. \tag{1.4}$$

Conversely, given such a triple (s, t, u), there is a triple (a, b, c) which exhibits n as a congruent number. Let's prove this.

Proof. Suppose we have a triple (a, b, c) which exhibits n as a congruent number. Define

$$\begin{aligned} s &:= \frac{1}{2}|a-b|; \\ t &:= \frac{c}{2}; \\ u &:= \frac{1}{2}(a+b). \end{aligned}$$

Then we get

$$s^2 + n = \frac{1}{4}(a^2+b^2-2ab) + \frac{ab}{2} = \frac{a^2+b^2}{4} = \frac{c^2}{4} = \left(\frac{c}{2}\right)^2 = t^2,$$

and

$$t^2 + n = \frac{c^2}{4} + \frac{ab}{2} = \frac{a^2+b^2+2ab}{4} = \frac{(a+b)^2}{4} = \left(\frac{1}{2}(a+b)\right)^2 = u^2.$$

We also claimed that we could go in the other direction. So let (s, t, u) be three positve rational numbers such that $s^2 + n = t^2$ and $t^2 + n = u^2$. Define

$$\begin{aligned} a &:= u - s; \\ b &:= u + s; \\ c &:= 2t. \end{aligned}$$

Then we get

$$a^2 + b^2 = (u-s)^2 + (u+s)^2 = 2(u^2+s^2) = 2(t^2+n+t^2-n)^2 = 2(2t^2) = 4t^2 = c^2,$$

and

$$\frac{1}{2}ab = \frac{1}{2}(u-s)(u+s) = \frac{1}{2}(u^2-s^2) = \frac{1}{2}\cdot 2n = n.$$

So (a, b, c) exhibits n as a congruent number. □

It's not immediately clear that the description in terms of s, t and u is easier to work with than the original setting, but at least we've reformulated the problem. Sometimes this makes it easier to work with: for example, you may have more intuition about triples of squares which differ by n than about triangles with rational side-lengths. But there is another reformulation of the problem which is very powerful.

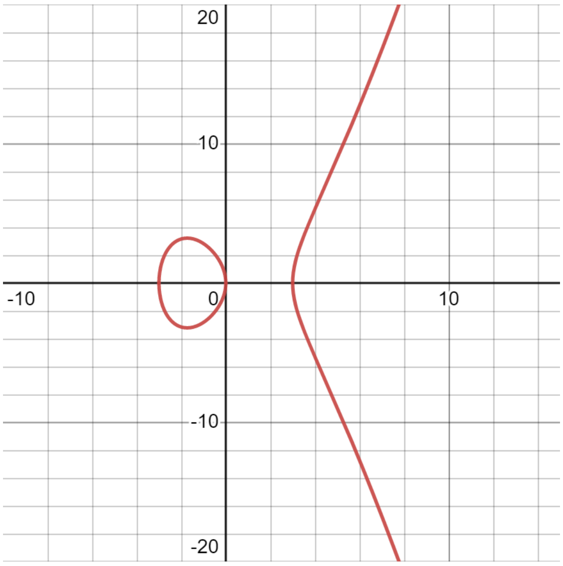
If (a, b, c) exhibits n as a congruent number, then define

$$\begin{aligned} x &:= \frac{n(a+c)}{b}; \\ y &:= \frac{2n^2(a+c)}{b^2}. \end{aligned}$$

Then one can show in a similar way to the proof above that triples (a, b, c) are in one-to-one correspondence with pairs (x, y), where x and y are rational numbers with $y \neq 0$, satisfying

$$y^2 = x^3 - n^2 x.$$

This is a very special equation: it describes an *elliptic curve*. Here is a picture of the elliptic curve $y^2 = x^3 - 9x$ in the xy-plane:



Note that the red line consists of all pairs of real numbers (x, y) which satisfy the equation $y^2 = x^3 - n^2x$. If one of these points has rational coordinates and $y \neq 0$, then n is a congruent number. If no such point exists, n is not a congruent number. It turns out that this is equivalent to a question about the *rank* of such elliptic curves: if the rank is zero, no such point exists, and if the rank is at least 1, such a point does exist. However, determining the rank of an elliptic curve is a hard problem! On the other hand, there are some tools to study this, and so we can make progress on the congruent number problem.

Elliptic curves are very rich number-theoretic objects, and in the summer school we will try to understand why and what this means. Because elliptic curves have been so well-studied, they give us ways to attack the congruent number problem, and it is possible to explore these in your project. Here are some examples of (difficult) questions you could try to answer:

- Does there exist a non-congruent number? Do there exist infinitely many?
- Can you show that a particular number, say the number 1, is not congruent?
- What proportion of all numbers is congruent?
- Can you come up with a sufficient condition for a number to be congruent?

2. Set theory

Sets are among the most basic objects mathematicians work with. More fundamentally, set theory is often used as the foundation of mathematics: everything is a set, and there are certain rules (the ZFC axioms) for working with them, from which all other mathematics is built up. For this reason, it is important to know how to work with sets: they will inevitably come up when you read mathematics, or try to do mathematics yourself.

2.1 Sets

Definition 2.1.1. A *set* is a collection of elements, denoted inside curly brackets.

For instance, the set

$$S = \{1, 55, \text{book}\}$$

is a set consisting of the three elements $1, 55$ and book.

There is a special set called the *empty set*:

$$\emptyset := \{\ \}.$$

(The notation ":=" means "is defined to be".) It is a set without elements, and it comes up in mathematics quite often.

We use the notation $a \in S$ to say that an element a belongs to the set S. For example, $4 \in \{1, 2, 3, 4, 5\}$. Because the empty set has no elements, the statement $a \in \emptyset$ is always a contradiction, i.e. a false statement. Similarly, we write $a \notin S$ to mean that a is not an element of S.

Here are some more examples of sets.

Examples 2.1.2.
1. The natural numbers:

$$\mathbb{N}_0 := \{0, 1, 2, 3, ...\}$$

This is a set with infinitely many elements. We could also write it as follows:

$$\mathbb{N}_0 = \{x \mid x \text{ is a non-negative integer}\},$$

although this feels a little bit less rigorous.[1] The symbol "|" is to be read as "such that", i.e. $\mathbb{N}_0$ is the set of all elements x such that x is a non-negative integer.
2. The integers:

$$\mathbb{Z} := \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

This is once again an infinite set of numbers, but in contrast to the natural numbers, it also contains all negative integers.

Having defined the integers, we can define the natural numbers in a more mathematical way:

$$\mathbb{N}_0 = \{n \in \mathbb{Z} \mid n \geq 0\}.$$

[1] Speaking of rigour, we will not worry too much about the definition of numbers in this summer school.

3. The rational numbers:

$$\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

This is the set of all fractions. Technically this definition is not completely correct, because many expressions $\frac{a}{b}$ will be identified. In fact, $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. This is not clear from the definition of $\mathbb{Q}$ given above, but once again, I will rely on your knowledge and intuition about numbers in order not to overcomplicate notation.
4. The real numbers:

$$\mathbb{R} := \{x \mid -\infty < x < \infty\}.$$

This set contains the rational numbers, but is strictly larger: it also contains numbers such as $\sqrt{2}$ and π which cannot be written as fractions. (Can you prove that $\sqrt{2}$ is not a fraction? What about π?)
5. The complex numbers:

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}.$$

We won't talk much about the complex numbers in this summer school, but they are fundamental to many areas of maths and science, so it's a good idea to learn about them.
6. Elements of sets don't need to be numbers. For instance, the set {Stockholm University, KTH} is a perfectly fine set with two elements.
7. We can also have sets of sets, for example $\{\emptyset\}$ is a set with one element. However, there is no set of all sets; this is known as Russell's paradox. Can you explain why the set of all sets can't possibly exist?

There is a notion of containment of sets: for example, the set $\{1, 3, 10\}$ is contained in the set $\mathbb{N}_0$. We write this as $\{1, 3, 10\} \subseteq \mathbb{N}_0$ or $\{1, 3, 10\} \subset \mathbb{N}_0$. The sign $\subseteq$ means the two sets are possibly equal, whereas $\subset$ means that the first set is a strict subset of the second set. Let's make this into a formal definition:

Definition 2.1.3. Let S be a set. A *subset* of S is a set A such that $a \in A \implies a \in S$. (The symbol " $\implies$ " means "implies".) In other words, it is a set A all of whose elements also belong to S.

It is important to distinguish between containment ($\subseteq$) and membership ($\in$). The former is about sets, the latter about elements of sets. For example, $\{1\} \subset \mathbb{R}$, but $\{1\} \notin \mathbb{R}$; instead, we have $1 \in \mathbb{R}$.

Note that we have inclusions $\mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Before moving on to operations on sets, we discuss one more property of sets, which is the size of a set. The mathematical term for this is cardinality.

Definition 2.1.4. Let S be a set. The number of elements of S is called the *cardinality* of S, denoted either $|S|$ or $\#S$. This is either a natural number or infinity.

There are many different kinds of infinity when talking about the cardinality of sets. The smallest infinity is $|\mathbb{N}_0|$, which we call *countably infinite.* There are also bigger sets, such as $\mathbb{R}$, which are *uncountably infinite.* We will not go into detail about this, but we will briefly touch upon it again when we discuss functions.

2.2 Operations on sets

We will now discuss ways to create new sets out of old ones. There are many ways to do this.

Definition 2.2.1. Let A and B be sets. The *product* of A and B is defined to be

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

The elements (a, b) are called *pairs* or *tuples*.

Example 2.2.2. Consider the product of $\mathbb{R}$ with itself:

$$\mathbb{R}^2 := \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \text{ are real numbers}\}$$

This can be pictured as the xy-plane.

Definition 2.2.3. Let S be any set. Define the *power set* of S to be

$$\mathcal{P}(S) := \{T \mid T \text{ is a subset of } S\}.$$

Example 2.2.4. If $S = \{0, 1\}$, the power set is

$$\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Definition 2.2.5. Let A and B be sets. We define the *union* of A and B as

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

and the *intersection* of A and B as

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

Example 2.2.6.
1. Let $A = \{0, 1, 2, 3\}$ and $B = \{1, 3, 5\}$. Then

$$A \cup B = \{0, 1, 2, 3, 5\}, \qquad A \cap B = \{1, 3\}.$$

2. Let $A = \{\text{even integers}\}$ and $B = \{\text{odd integers}\}$. Then

$$A \cup B = \mathbb{Z}, \qquad A \cap B = \emptyset.$$

2.3 Functions

Perhaps the most important way set theory is used in mathematics is for defining functions between sets. In high school, you spend a lot of time studying functions from $\mathbb{R}$ to $\mathbb{R}$, but not much attention is usually devoted to what a function really is. Set theory makes this precise. First, here is an informal definition of a function $f : S \to T$, where S and T are sets: it is a rule which assigns to each element $s \in S$ an element $f(s) \in T$. This is often a good way to think about functions, but it is not very precise: what do we mean by "a rule"? This is why we have the following definition.

Definition 2.3.1. A *function* $f : S \to T$ is a subset $\Gamma_f \subseteq S \times T$ such that for each $s \in S$, there is a unique $t \in T$ such that $(s, t) \in \Gamma_f$. Write $t = f(s)$ or $f : s \mapsto t$ if $t \in T$ is the unique element such that $(s, t) \in \Gamma_f$.

The set Γ_f is also called the *graph* of the function f. According to our definition, a function and its graph are actually the same thing. Note that this notion generalizes the graph of a function from $\mathbb{R}$ to $\mathbb{R}$: for example, the graph of the function $f(x) = x^2$ is the set of all $(x, y) \in \mathbb{R}^2$ such that $y = x^2$, which can be drawn as a parabola in the xy-plane.

Examples 2.3.2.
1. $S = \{*\}$ (a one-element set) and $T = \mathbb{N}_0$. A function $S \to T$ is a rule assigning an element $t \in \mathbb{N}_0$ to the element $* \in S$. So $f(*) = t$. In other words, defining a function $f : S \to T$ is equivalent to choosing a natural number t.
We can also see f as $\Gamma_f = \{(*, b)\} \subset \{*\} \times \mathbb{N}_0$. Note that the set of functions from $\{*\}$ to $\mathbb{N}_0$ is $\{\{(*, b)\} \mid b \in \mathbb{N}_0\}$.
2. $S = \{0, 1\}$ and $T = \mathbb{N}_0$. Then a function $f : S \to T$ is equivalent to choosing a pair of natural numbers (t_0, t_1): indeed, any function sends 0 to some t_0 and 1 to some t_1. The graph is $\Gamma_f = \{(0, t_0), (1, t_1)\} \subset S \times T = \{0, 1\} \times \mathbb{N}_0$.
3. $S = T = \mathbb{R}$. A function $f : S \to T$ assigns to every real number s another real number t. For example $f(s) = s$ or $f(s) = s^2$. These can be visualised by drawing the graph $\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R} =: \mathbb{R}^2$.
4. For any set S, there is the identity function $\mathrm{id}_S : S \to S$ which sends $s \mapsto s$. Its graph is

$$\Gamma_{\mathrm{id}_S} = \{(s, s) \mid s \in S\} \subset S \times S.$$

We have names for certain special kinds of functions.

Definition 2.3.3. Let $f : S \to T$ be a function.

1. We say f is *injective* if for all $t \in T$, there exists at most one $s \in S$ such that $f(s) = t$.

2. We say f is *surjective* if for all $t \in T$, there exists at least one $s \in S$ such that $f(s) = t$.

3. We say f is *bijective* if it is both injective and surjective. If such a bijective function $f : S \to T$ exists, we also say S and T are bijective.

There are functions which are neither injective nor surjective. Injective functions are also called embeddings; the reason is that if $f : S \to T$ is injective, one may view S as a subset of T through the function f. That is, the subset $\{f(s) \mid s \in S\} \subseteq T$ is a set which is bijective with S, and two bijective sets can for many purposes be treated in the same way: as long as one doesn't care about the specific elements of the sets, bijective sets have the same properties. To illustrate this, we will prove the following result.

Theorem 2.3.4. Let $f : S \to T$ be a bijection, with S and T finite sets. Then $|S| = |T|$.

Proof. We prove the theorem in two steps.

Step 1. Suppose $f : S \to T$ is injective. Then $|S| \leq |T|$.

Proof of Step 1. If f is injective, then for every $t \in T$, either $f^{-1}(t) = \emptyset$ or $f^{-1}(t) = \{s\}$ for a unique $s \in S$. (Here $f^{-1}(t) := \{s \in S \mid f(s) = t\}$ is the *pre-image* of t.) Thus $|f^{-1}(t)|$ is either 0 or 1 for any $t \in T$. In particular, $|f^{-1}(t)| \leq 1$.
Note also that

$$S = \bigcup_{t \in T} f^{-1}(t).$$

Putting this together, we get

$$|S| = \left|\bigcup_{t\in T} f^{-1}(t)\right| = \sum_{t\in T} |f^{-1}(t)| \leq \sum_{t\in T} 1 = |T|.$$

Here the second equality follows because the intersection $f^{-1}(t) \cap f^{-1}(t') = \emptyset$ for $t \neq t'$. Thus, Step 1 is proven.

Step 2. Suppose $f : S \to T$ is surjective. Then $|S| \geq |T|$.

Proof of Step 2. We will construct an injective function $g : T \to S$; then Step 1 will give us the required inequality.
Because f is surjective, we know that for any $t \in T$, there exists some $s \in S$ such that $f(s) = t$. Define a function $g : T \to S$ by letting $g(t) = s$ for some s such that $f(s) = t$ (there may be multiple $s \in S$ satisfying this criterion, but we just pick one of them). This function g is injective. Indeed, if $g(t) = g(t') = s$, then $t = f(s) = t'$. This is equivalent to saying that g is injective (see Exercise 6 on the problem sheet). Thus by Step 1, we have $|T| \leq |S|$.

Combining Step 1 and Step 2, we see that if $f : S \to T$ is bijective, then $|S| \leq |T| \leq |S|$. Since $|S| = |S|$, the inequalities must in fact be equalities, so $|S| = |T|$. □

Bijective functions are also sometimes called invertible functions. We will first define composition of functions, and afterwards prove Theorem 2.3.6 justifying this name.

Definition 2.3.5. Let $f : S \to T$ and $g : T \to U$ be functions. Define the *composition* of f and g to be the function

$$\begin{aligned} g \circ f : S &\longrightarrow U \\ s &\longmapsto g(f(s)). \end{aligned}$$

Visually, the composition looks as follows:

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & T \arrow[r, "g"] & U \end{tikzcd}$$

Theorem 2.3.6. Let $f : S \to T$ be a bijective function. Then there exists $g : T \to S$ such that $g \circ f = \mathrm{id}_S$ and $f \circ g = \mathrm{id}_T$. (In other words, $g(f(s)) = s$ for all $s \in S$ and $f(g(t)) = t$ for all $t \in T$.)

Proof. We construct the function $g : T \to S$ in the same way as in Step 2 of the proof of the previous theorem. What we need to show is that, if f is bijective, then $g(f(s)) = s$ and $f(g(t)) = t$. The fact that $f(g(t)) = t$ is how we constructed g. We still need to show that $g(f(s)) = s$.

Note that $f(g(f(s)) = f(s)$, by setting $t = f(s)$ in the equality $f(g(t)) = t$. But f is injective. Hence $g(f(s)) = s$. This is what we wanted to show. □

Remark 2.3.7. If $f : S \to T$ is bijective, then the function $g : T \to S$ from the above theorem is also denoted by f^{-1}. One can always define $f^{-1}(t)$, for $t \in T$, as the set $\{s \in S \mid f(s) = t\}$, but only when f is bijective will this set always contain one element, and thus only when f is bijective does f^{-1} define a function $T \to S$.

In view of the above theorem, one can philosophically move between bijective sets without losing information, through the invertible functions f and g. So it's reasonable to compare sizes of sets by looking at functions between them: if there is a bijection, the sets have the same size. This is true for finite sets by Theorem 2.3.4, and if we extend this notion to infinite sets, we can compare the sizes of different infinite sets.

It turns out that not all infinite sets are in bijection with each other. This means that there are different kinds of infinity: some are bigger than others. The smallest kind of infinity is called *countably infinite*, which is the cardinality of $\mathbb{N}_0$. Many infinite sets are countable: for example, $\mathbb{Z}$ is countable, because there is a bijection $\mathbb{N}_0 \to \mathbb{Z}$, sending

$$0 \longmapsto 0, \quad 1 \longmapsto 1, \quad 2 \longmapsto -1, \quad 3 \longmapsto 2, \quad 4 \longmapsto -2, \quad \text{etc.}$$

Can you think of an infinite set which is not countably infinite? Can you prove that there is no bijection between this set and $\mathbb{N}$?

2.4 Exercises

Exercise 1

Two sets are equal if they contain the same elements. For example, $\mathbb{N}_0 = \{n \in \mathbb{Z} \mid n \geq 0\}$.

1. Prove that if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
2. Prove that $\{1, 1\} = \{1\}$. In general, repetition of elements does not change the set.

Exercise 2

Let S and T be finite sets of cardinality n, resp. m.

1. What is the cardinality of $S \times T$?
2. What is the cardinality of $\mathcal{P}(S)$ (the power set of S)?
3. Can you say anything about the cardinality of $S \cap T$ and $S \cup T$?

Exercise 3

Write down a function which is

1. injective but not surjective;
2. surjective but not injective;
3. bijective, but not the identity function;
4. neither injective nor surjective.

Exercise 4

Let S be a set with 5 elements and T be a set with 7 elements. How many functions $f : S \to T$ are there? How many of these are injective? How many are surjective? How many are bijective?

Exercise 5

The set $\mathbb{R}^2$ can be seen geometrically as the xy-plane. Subsets X of $\mathbb{R}^2$ are functions if (by definition) for any $x \in \mathbb{R}$, there exists a unique $y \in \mathbb{R}$ such that $(x, y) \in X$.

Is there a geometric way of seeing whether a subset X of $\mathbb{R}^2$ is (the graph of) a function?

Exercise 6

Let $f : S \to T$ be a function. Prove that the following are logically equivalent:

1. f is injective.
2. For all $s, s' \in S$, if $f(s) = f(s')$ then $s = s'$.

Exercise 7

Let $f : S \to T$ and $g : T \to U$ be functions. Prove the following assertions.

1. If f and g are both injective, then $g \circ f$ is injective.
2. If f and g are both surjective, then $g \circ f$ is surjective.
3. If $g \circ f$ is injective, then f is injective.
4. If $g \circ f$ is surjective, then g is surjective.

Moreover, give a concrete example where $g \circ f$ is bijective but g is not injective and f is not surjective.

Exercise 8

Prove that for any $n \in \mathbb{Z}_{>0}$, the following sets are bijective:

$$\left\{(a, b, c) \in \mathbb{Q}^3_{>0} \mid a^2 + b^2 = c^2 \text{ and } \frac{ab}{2} = n\right\}$$

and

$$\{(x, y) \in \mathbb{Q}^2_{>0} \mid y^2 = x^3 - n^2 x\}.$$

Exercise 9

Prove the following statements about $f : S \to T$:

1. f is injective $\iff$ for any set U and for any two functions $g, g' : U \to S$ such that $f \circ g = f \circ g'$, we have $g = g'$.
2. f is surjective $\iff$ for any set U and for any two functions $g, g' : T \to U$ such that $g \circ f = g' \circ f$, we have $g = g'$.

3. Group Theory

Groups are fundamental objects in mathematics. They form the basis of many other constructions, and they are also used in physics, chemistry, and biology. Group theory is part of the area of abstract algebra, in which we study sets endowed with additional structure. Understanding groups allows one to dive deeper into this area and learn about rings, fields, modules, and other algebraic structures. In these notes, we will simply focus on getting a basic understanding of what a group is.

To motivate the definition of groups, we need to understand what is meant by "endowing a set with additional structure". A set is, by definition, nothing more than a collection of elements. But sometimes we have an idea of what a set looks like: for instance, $\mathbb{R}^2$ can be visualised as the xy-plane. In our minds, the elements $(0,0)$ and $(0,1)$ are closer together than the elements $(0,0)$ and $(5,5)$, but set-theoretically there is no interplay between any of these elements. What we can do is endow the set $\mathbb{R}^2$ with a certain "distance function" $d : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$, where $d(p_1, p_2)$ gives the distance between p_1 and p_2. (Can you write down an explicit formula for this distance function in terms of the coordinates of p_1 and p_2?)
This distance function formalizes our intuition about $\mathbb{R}^2$ as a space, rather than a set, and when one wants to study $\mathbb{R}^2$ as a space, it is convenient to study the pair $(\mathbb{R}^2, d)$ – i.e. to always see $\mathbb{R}^2$ not just as a set, but as a set endowed with the additional structure given by the function d.

This is perhaps still a bit vague, but the idea is that sets themselves don't contain much information. Here is another example, which is more in the spirit of group theory. Consider the set of integers $\mathbb{Z}$. This is a set of numbers, and when we think about numbers, we never just think about them as being arbitrary elements. Rather, there are relations between different numbers, for example $1 + 1 = 2$. However, when we view $\mathbb{Z}$ as a set, mathematically there is no addition rule. If we want to have the relation $1 + 1 = 2$ between the elements 1 and 2 in $\mathbb{Z}$, we need to endow $\mathbb{Z}$ with the additional structure of an addition rule.

So how do we do this? Well, addition is just a function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$: it takes as input two integers and gives one integer as an output. But it's not just any function - it satisfies some special properties. For example, $a + b = b + a$ for all $a, b \in \mathbb{Z}$. Another property is that $a + 0 = a$ for all $a \in \mathbb{Z}$. In fact, the pair $(\mathbb{Z}, +)$ is an example of an *abelian group*. There are so many interesting mathematical objects which come equipped with a certain "addition rule" or "multiplication rule" that mathematicians decided to create a name for them, and this is what a group is.

3.1 Definition and examples

So the idea is that we want to define groups as sets endowed with a certain function which behaves a bit like multiplication or addition. We build up towards the definition step by step.

Definition 3.1.1. Let S be a set. A *binary operation* on S is a function $\cdot : S \times S \to S$. We write $\cdot(s_1, s_2)$ as $s_1 \cdot s_2$ or simply $s_1 s_2$.

Example 3.1.2. If $S = \mathbb{N}$, some examples of binary operations $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ are

1. $a \cdot b := ab$ (standard multiplication);
2. $a \cdot b := a + b$;
3. $a \cdot b := a + b + 10$;

4. $a \cdot b := 0$ for all $a, b \in \mathbb{N}$.

What is not a binary operation is subtraction: if $a \cdot b := a - b$ and $b > a$, then $a - b < 0$ and so the result is not a natural number. In other words, subtraction is not a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (but one could define subtraction as a function $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$). One often phrases this as saying that $\mathbb{N}$ is not closed under subtraction.

Binary operations are very general. We want to distinguish certain classes of binary operations with good properties, which is the purpose of the following definition.

Definition 3.1.3. Let $\cdot : S \times S \to S$ be a binary operation.

1. We say $\cdot$ is *associative* if for all $a, b, c \in S$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. We say $\cdot$ is *commutative* if for all $a, b \in S$, we have $a \cdot b = b \cdot a$.

If an operation is associative, it means we don't have to care about how we place brackets when we multiply more than two elements. This makes things much easier, and in almost every situation you will encounter in mathematics, binary operations will be associative. However, note that the order of multiplication still matters when the binary operation is not commutative: for example, $g_1 \cdot g_2 \cdot g_3 \neq g_2 \cdot g_3 \cdot g_1$ in general.

Example 3.1.4. Let S be a set. We define $\mathrm{End}(S) := \{f : S \to S\}$ to be the set of *endomorphisms* of S, i.e. functions from S to itself. There is a binary operation on $\mathrm{End}(S)$ given by composition: $(f, g) \mapsto f \circ g$. This operation is associative (the proof is very short), but not commutative in general. Exercise: demonstrate the failure of commutativity by giving a set S and two functions $f, g : S \to S$ such that $f \circ g \neq g \circ f$.

We can now give the definition of a group.

Definition 3.1.5. A *group* is a pair $(G, \cdot)$, where G is a set and $\cdot$ is a binary operation on G, such that the following conditions are satisfied:

(G1) The binary operation is associative;

(G2) There exists an element $e \in G$ such that $e \cdot g = g = g \cdot e$ for all $g \in G$;

(G3) For every $g \in G$, there exists some $g^{-1} \in G$ such that $g \cdot g^{-1} = e = g^{-1} \cdot g$.

If the binary operation is also commutative, we say G is an *abelian group.*

We call $e \in G$ the *identity element* of G. If $g \in G$ is any element, we call g^{-1} the *inverse* of g. Note that $e^{-1} = e$.

In groups, we can perform cancellation in equations. In fact, proving this uses all the group axioms. Let's state it as a theorem.

Theorem 3.1.6. Let G be a group, and suppose that $g \cdot h = g \cdot h'$ for some elements $g, h, h' \in G$. Then $h = h'$. Similarly, if $h \cdot g = h' \cdot g$, then $h = h'$.

Proof. Suppose that $g \cdot h = g \cdot h'$. By (G3), g has an inverse. Multiply both sides by g^{-1} on the left to get

$$g^{-1} \cdot (g \cdot h) = g^{-1} \cdot (g \cdot h').$$

By associativity (G1), this is the same as

$$(g^{-1} \cdot g) \cdot h = (g^{-1} \cdot g) \cdot h',$$

i.e.

$$e \cdot h = e \cdot h'.$$

But by (G2), this just says $h = h'$, which is what we wanted to show. The argument is similar if we start with $h \cdot g = h' \cdot g$. □

I stated before that there are many examples of groups. Try to see if you can prove that the following are really groups.

Examples 3.1.7.
0. The *trivial group* is the group with one element (equipped with the unique binary operation on this set).
1. All of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are abelian groups under addition, with $e = 0$. Note that $\mathbb{N}$ is not a group under addition (why not?).
2. The positive real numbers $\mathbb{R}_{>0}$ form an abelian group under multiplication. Likewise for $\mathbb{Q}_{>0}$.
3. Let S be either $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Then $S \setminus \{0\}$ (i.e. S without the element 0) is a group under multiplication.
4. Let G be the set $\{0, 1\}$ and define a binary operation $+ : G \times G \to G$ by setting

$$0 + 0 = 0; \qquad 0 + 1 = 1; \qquad 1 + 0 = 1; \qquad 1 + 1 = 0.$$

Then G is an abelian group.
5. More generally, let $n \in \mathbb{Z}_{>0}$ be a positive integer. Then one can define the *integers modulo n* as the set

$$\mathbb{Z}/n\mathbb{Z} := \{0, 1, 2, \ldots, n-1\},$$

which has a binary operation $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined as follows:

$$a + b = \begin{cases} a + b & \text{if } a + b < n; \\ a + b - p & \text{if } a + b \geq n. \end{cases}$$

This is an abelian group. The definition above is very ad-hoc and not so intuitive, but we will come back to this example (and prove that it is a group) when we talk about modular arithmetic. Note that example 4 actually describes $\mathbb{Z}/2\mathbb{Z}$.
6. Let $n \in \mathbb{Z}_{\geq 1}$. Define the *cyclic group of order n* to be the set

$$C_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}.$$

These are the n-th roots of unity in $\mathbb{C}$. They all lie on the unit circle and form a group under multiplication.
7. Let X be a finite set. Define the group $(\mathrm{Sym}(X), \circ)$ whose elements are bijections $f : X \to X$ and whose binary operation is given by composition.
If $X = \{1, 2, \ldots, n\}$ is the set of the first n positive integers, then $\mathrm{Sym}(X)$ is usually denoted by S_n. Elements of S_n are denoted by *products of cycles*: e.g. the cycle $(12) \in S_2$ is the bijection sending $1 \mapsto 2$ and $2 \mapsto 1$, and the product of cycles $(152)(34)$ in S_5 is the bijection sending $1 \mapsto 5 \mapsto 2 \mapsto 1$ and $3 \mapsto 4 \mapsto 3$.
8. Define an abelian group $G = \{e, a, b, c\}$ with identity e and multiplication law $ab = c$, $ac = b$, $bc = a$. This is a group called the *Klein four group.*

3.1.1 Products of groups

Let $(G, \circ)$ and $(H, \bullet)$ be groups. Then we can endow the product $G \times H$ with a group structure, in the following way: we define

$$(g, h) \cdot (g', h') := (g \circ g', h \bullet h').$$

The identity element is (e_G, e_H), and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

This gives new examples of groups. For example, $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $S_n \times \mathbb{C}$ are groups. Note that $G \times H$ is abelian if and only if G and H are both abelian.

3.1.2 Subgroups and orders

When we study groups, we usually want to break them up into smaller parts which are easier to study. Subgroups are useful for this.

Definition 3.1.8. Let G be a group. A subset $H \subset G$ is a *subgroup* of G if the following hold:

1. $e \in H$;
2. For all $h, h' \in H$, we have $h \cdot h' \in H$;
3. For all $h \in H$, we have $h^{-1} \in H$.

In other words, H is a subset which is a group in its own right under the same binary operation as G. We express property 2 in the definition by saying H is *closed* under the binary operation.

Example 3.1.9. Let G be any group, and let $g \in G$. Then the set $\langle g \rangle := \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$ is a subgroup of G, called *the subgroup generated by g*.

We now define the order of an element of a group. Slightly confusingly, the size (cardinality) of a group is also often called the order of the group.

Definition 3.1.10. Let G be a group and $g \in G$. If $\langle g \rangle$ is a finite subgroup, define $|\langle g \rangle|$ to be the *order* of g, denoted $\mathrm{ord}(g)$. Equivalently, $\mathrm{ord}(g)$ is the smallest $n > 0$ such that $g^n = e$. If such n does not exist, say g has *infinite order.*
If $G = \langle g \rangle$ for some $g \in G$, say G is *cyclic* and g is a *generator* of G.

Example 3.1.11. The cyclic group of order n is a cyclic group of order n. In other words, the group C_n has a generator, and the order of this generator is n. Let's prove this. Recall that

$$C_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}.$$

Thus, all elements of C_n are solutions of the equation $X^n - 1 = 0$. This equation has at most n distinct solutions, and you can check that each of the complex numbers

$$e^{\frac{2\pi ik}{n}}, \qquad 0 \leq k < n$$

is a solution. Thus, the above elements make up C_n, and since $e^{\frac{2\pi ik}{n}} = \left(e^{\frac{2\pi i}{n}}\right)^k$, we see that the element $\zeta_n := e^{\frac{2\pi i}{n}}$ is a generator of C_n. Moreover, the smallest positive integer m such that $\zeta_n^m = 1$ is the integer n, i.e. C_n is a group of order n.

We are now ready to prove an interesting statement about finite groups.

Theorem 3.1.12. Let G be a finite group, and let $g \in G$. Then g has finite order, and if $g^n = e$ for some $n \in \mathbb{N}$, then $\operatorname{ord}(g)$ divides n.

Proof. We first show that g has finite order. Let $|G| = n$. Because the set $\{e = g^0, g, g^2, \ldots, g^n\}$ has $n + 1$ elements, there must be two elements which are the same. This gives us $g^k = g^l$ for some integers k and l. Without loss of generality, assume that $k \geq l$. Then multiplying by $g^{-l} := (g^{-1})^l = (g^l)^{-1}$ gives

$$g^{-l} \cdot g^k = g^{k-l} = e,$$

so g has finite order $k - l$.

Next, suppose that $g^n = e$. We want to show that $\operatorname{ord}(g)$ divides n. By definition, $\operatorname{ord}(g)$ is the smallest integer $m \geq 1$ such that $g^m = e$, so $\operatorname{ord}(g) \leq n$. Since the statement holds if $\operatorname{ord}(g) = n$, we may assume that $\operatorname{ord}(g) < n$. Now divide n by $\operatorname{ord}(g)$ with remainder to get

$$n = k \cdot \operatorname{ord}(g) + r,$$

for some $k \in \mathbb{N}$ and $0 \leq r < \operatorname{ord}(g)$. Thus we get

$$e = g^n = g^{k \cdot \operatorname{ord}(g) + r} = (g^{\operatorname{ord}(g)})^k \cdot g^r = e^k \cdot g^r = g^r,$$

so $g^r = e$. But since $r < \operatorname{ord}(g)$, this means $r = 0$, so $n = k \cdot \operatorname{ord}(g)$, i.e. $\operatorname{ord}(g) \mid n$. □

Divisibility is actually a recurring theme in group theory. To demonstrate this, we state a fundamental result, whose proof is beyond the scope of this course.

Theorem 3.1.13 (Lagrange's Theorem)**.** Let G be a finite group, and let $H \subseteq G$ be a subgroup. Then $|H|$ divides $|G|$.

As a consequence, the order of any element divides the order of the group:

Corollary 3.1.14. Let G be a finite group, and let $g \in G$. Then $\operatorname{ord}(g)$ divides $|G|$.

Proof. If G is finite, then $\langle g \rangle = \{e, g, g^2, \ldots, g^{\operatorname{ord}(g)-1}\}$ is a subgroup with $\operatorname{ord}(g)$ elements. By Lagrange's Theorem, we get that $\operatorname{ord}(g) = |\langle g \rangle|$ divides $|G|$. □

3.2 Group homomorphisms (optional)

It has been said that in mathematics, one gains the most information about an object by seeing how it relates to other objects. We do this by looking at functions between the objects. However, we don't just want any functions - when we work with groups, we want the functions to take into account the group structure. This leads us to the notion of a homomorphism.

Definition 3.2.1. Let $(G, \cdot_G)$ and $(H, \cdot_H)$ be groups. A *group homomorphism* from G to H is a function $f : G \to H$ such that for all $g, g' \in G$, we have

$$f(g \cdot_G g') = f(g) \cdot_H f(g').$$

A bijective group homomorphism is called an *isomorphism*.

Examples 3.2.2.
1. Let G and H be any groups. Then the function $f : G \to H$ sending $g \mapsto e$ for every $g \in G$ is a group homomorphism: indeed,

$$f(g \cdot g') = e = e \cdot e = f(g) \cdot f(g') \text{ for all } g, g' \in G.$$

2. Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}_{>0}, \times)$. Then the exponential function $f(x) = e^x$ is an isomorphism from G to H, because it is bijective and

$$e^{x+y} = e^x \cdot e^y \text{ for all } x, y \in \mathbb{R}.$$

If f is a group homomorphism, it must send the identity element to the identity element and inverses to inverses (prove this!). Moreover, the order of an element $f(g)$ is related to the order of g in the following way:

Theorem 3.2.3. Let $f : G \to H$ be a homomorphism. Then $\mathrm{ord}(f(g))$ divides $\mathrm{ord}(g)$.

Proof. By Theorem 3.1.12, it is enough to show that $f(g)^{\mathrm{ord}(g)} = e$. Because f is a group homomorphism, it respects multiplication, which allows us to write

$$f(g)^{\mathrm{ord}(g)} = f(g) \cdot f(g) \cdot \ldots \cdot f(g) = f(g \cdot g \cdot \ldots \cdot g) = f(g^{\mathrm{ord}(g)}) = f(e) = e.$$

This finishes the proof. □

The notion of isomorphism is very important. It is similar to the notion of bijection for sets. If two groups are isomorphic, it means that the underlying sets are bijective, and that the group structures are the same. So group-theoretically, the properties of isomorphic groups are the same. When encountered with a new group, mathematicians want to find out which familiar group it is isomorphic to. In the same spirit, they want to find out which possible groups exists, up to isomorphism. This question has essentially been answered for finite groups over the past century or so, but the classification is very complicated and the proof of the classification is over 10.000 pages long.

Let's see some examples of isomorphic and non-isomorphic groups.

Examples 3.2.4.
1. Recall the Klein four group $\{e, a, b, c\}$. This is not isomorphic to the cyclic group C_4. Indeed, if this were the case, there would have to be an element of order 4 in the Klein four group (why?), but there is no such element.
2. The Klein four group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. An isomorphism is given by

$$\{e, a, b, c\} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$e \longmapsto (0,0), \quad a \longmapsto (1,0), \quad b \longmapsto (0,1), \quad c \longmapsto (1,1).$$

3. The symmetric group S_3 is isomorphic to the dihedral group D_6 of symmetries of an equilateral triangle.

Proposition 3.2.5. Let $G = \langle g \rangle$ be a cyclic group. Then any homomorphism $f : G \to H$ is determined by the image of g.

Proof. We need to show that if f and f' are two homomorphisms $G \to H$ such that $f(g) = f'(g)$, then $f = f'$.

So suppose $f(g) = f'(g)$. Because G is cyclic with generator g, any element $h \in G$ is of the form $h = g^n$ for some $n \in \mathbb{Z}$. Hence

$$f(h) = f(g^n) = f(g)^n = f'(g)^n = f'(g^n) = f'(h).$$

Thus $f = f'$. □

3.3 Exercises

Exercise 1

For each of the binary operations in Example 3.1.2, decide whether or not the operation is associative.

Exercise 2

Which of the following are groups?

1. The set $\mathbb{R}_{\geq 0}$ with the binary operation $x \cdot y := \max(x, y)$.
2. The set of all rational numbers with odd denominator, with the usual addition.
3. The set $\{a, b\}$ with the binary operation

$$a \cdot a = a, \quad b \cdot b = b, \quad a \cdot b = b, \quad b \cdot a = b.$$

Exercise 3

Let $S := \mathbb{R} \setminus \{-1\}$, i.e. the set of real numbers without the element -1. Show that the binary operation $x \star y := xy + x + y$ defines a group structure on S.

Exercise 4

Let G be a group and let $g, h \in G$. Prove the following:

1. $(g^{-1})^{-1} = g$;
2. $(gh)^{-1} = h^{-1}g^{-1}$.

Exercise 5

For every $n \geq 3$, there is a group D_{2n} called the *dihedral group of order* $2n$. It is defined as the group of symmetries of a regular n-gon. For example, if $n = 3$, the group D_6 consists of the symmetries of an equilateral triangle. This group is always generated by a rotation over $360/n$ degrees and a reflection through an axis of symmetry; in other words, all other symmetries are obtained by composing these symmetries in some order.

1. Given the above information, prove that $|D_{2n}| = 2n$.
2. Is D_{2n} ever abelian?
3. (Optional) Can you come up with a reasonable definition for an infinite dihedral group D_∞?

Exercise 6

Determine which of the following subsets H are subgroups of the given groups G.

1. $G = (\mathbb{Z}, +),\ H = \{n \in \mathbb{Z} \mid n \text{ is divisible by } 51\}$;
2. $G = S_n,\ H = \{\sigma \in S_n \mid \sigma(1) = 1\}$ (for any $n \in \mathbb{Z}_{\geq 1}$);
3. $G = (\mathbb{R}_{>0}, \times),\ H = \{x \in \mathbb{R}_{>0} \mid e^{-x} < 2\}$.

Exercise 7

Consider the symmetric group S_n. Each element $\sigma \in S_n$ has a certain *cycle shape*, which is defined as follows.

Since σ is a bijection from $\{1, \ldots, n\}$ to itself, we can consider where we map to when we start with the element 1. This gives a cycle $(1\ \sigma(1)\ \sigma(\sigma(1)) \ldots\ \sigma^m(1))$, where $\sigma(\sigma^m(1)) = 1$. If $m < n$, there are some elements in $\{1, \ldots, n\}$ which are not obtained by applying σ any number of times to the element 1. Pick the smallest integer for which this holds, say k, and write a new cycle $(k\ \sigma(k)\ \sigma(\sigma(k)) \ldots\ \sigma^{m'}(k))$ (so $\sigma(\sigma^{m'}(k)) = k$). Continue like this until all elements are in some cycle. The cycle shape of σ is the sequence of lengths of the cycles which appear.

Three examples: first, let $n = 5$. Then the element $\sigma = (125)(34)$ represents the function which sends $1 \mapsto 2 \mapsto 5 \mapsto 1$ and $3 \mapsto 4$. The cycle shape of this element is $(3, 2)$. Second, for arbitrary n, the cycle shape of the identity function $\mathrm{id} : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is (1^n), meaning there are n cycles of length 1. Third, let $n = 3$ and let σ be the function such that $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$. Then σ is represented by $(1)(23)$ and has cycle shape $(1, 2)$.

1. What are the possible cycle shapes for permutations in S_3? How many permutations are there for each cycle shape?
2. How many permutations in S_4 have cycle shape $(3, 1)$?
3. What is the order of an element with cycle shape $(1^3, 2, 3)$ in S_8?
4. Suppose that $\sigma \in S_n$ has cycles of lengths $l_1, \ldots, l_m$. What is the order of σ?

Exercise 8

Let n be an arbitrary positive integer. How many functions are there from $\mathbb{Z}/n\mathbb{Z}$ to S_4? How many of these are group homomorphisms?

4. Modular Arithmetic

In this chapter, we introduce modular arithmetic, which is essentially a study of the additive groups $\mathbb{Z}/n\mathbb{Z}$ endowed with the additional binary operation of multiplication. We will then explain some ideas relating modular arithmetic to geometry.

4.1 Division of integers

The integers $\mathbb{Z}$ come equipped with (at least) three natural binary operations, namely addition, subtraction, and multiplication. There is a fourth operation which fits into this row, namely division. However, $\mathbb{Z}$ is not closed under division: for example, 1 and 2 are elements in $\mathbb{Z}$, but $1/2$ is not an integer.

We can still talk about division when we take into account that there may be a remainder. This is how we first learned to divide in primary school. We would say something like "15 divided by 7 is 2, with a remainder of 1" to denote the fact that $15 = 2 \cdot 7 + 1$.

In general, let $n \in \mathbb{Z}_{>0}$. Then we can define a function

$$\text{mod } n : \mathbb{Z} \to \mathbb{Z},$$

which sends $m \in \mathbb{Z}$ to the remainder of m divided by n. Note that the image of this function is the set $\{0, 1, 2, \ldots, n-1\}$.
We use the notation

$$m \equiv m' \pmod{n},$$

pronounced "m is congruent to m' mod n", if m and m' map to the same element under the function mod n, or equivalently, when m and m' have the same remainder after dividing by n.

Examples 4.1.1.
1. We have $m \equiv 0 \pmod{1}$ for all $m \in \mathbb{Z}$, since $m = m \cdot 1 + 0$.
2. We have $m \equiv 0 \pmod{2}$ if and only if m is even, and $m \equiv 1 \pmod{2}$ if and only if m is odd.
3. $-1 \equiv n-1 \mod n$.
4. $-3 \equiv 5 \mod 8$.
5. $1221 \equiv 0 \mod 11$.

4.2 The integers modulo n

Fix a positive integer n. We define the set

$$\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-1\}$$

to be *the integers modulo n*. There is a natural map

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ m &\longmapsto m \pmod{n}. \end{aligned}$$

Let us also write down a function in the other direction:

$$\begin{aligned} i : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z} \\ m &\longmapsto m. \end{aligned}$$

We are defining these functions to avoid the inevitable confusion about the set which an element m lives in: as it stands, it could denote either an integer or an element of $\mathbb{Z}/n\mathbb{Z}$. I will write m or, say, 3, only if I mean the integer, i.e. $m \in \mathbb{Z}$ or $3 \in \mathbb{Z}$. If I want to consider m or 3 as an element of $\mathbb{Z}/n\mathbb{Z}$, I will either write $\pi(m)$ or $m \pmod{n}$, resp. $\pi(3)$ or $3 \pmod{n}$.[1]

Remark 4.2.1. We use the letter π because we think of this function as a projection, and we want to reserve the letter p to denote a prime number. Note that $\pi \circ i : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the identity function. This will be important later.

Using the function i defined above, we can define a binary operation on the set $\mathbb{Z}/n\mathbb{Z}$ by using the addition on $\mathbb{Z}$:

Definition 4.2.2. Define a binary operation $\oplus$ on $\mathbb{Z}/n\mathbb{Z}$ as follows: for $a, b \in \mathbb{Z}/n\mathbb{Z}$, we let $a \oplus b := \pi(i(a) + i(b))$.

In practice, this means that we add the integers a and b modulo n, but if the answer is greater than n, we again reduce it modulo n so that we end up in $\mathbb{Z}/n\mathbb{Z}$ again.

Remark 4.2.3. Another definition of $\mathbb{Z}/n\mathbb{Z}$ is in terms of subsets of $\mathbb{Z}$. In this case, define

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \dots, \overline{n-1}\},$$

where we define the sets $\overline{m} := \{k \in \mathbb{Z} \mid k = m + k'n \text{ for some } k' \in \mathbb{Z}\}$. Thus, $\mathbb{Z}/n\mathbb{Z}$ is a set of n subsets of $\mathbb{Z}$, and we have

$$\mathbb{Z} = \bigcup_{m=0}^{n-1} \overline{m}, \qquad \overline{m} \cap \overline{m'} = \emptyset \text{ whenever } m \neq m'.$$

One can then define the addition as $\overline{m} \oplus \overline{m'} = \{a + b \mid a \in \overline{m},\ b \in \overline{m'}\}$, which is arguably more natural. This definition of $\mathbb{Z}/n\mathbb{Z}$ in terms of subsets of $\mathbb{Z}$ can be made even cleaner if you know about equivalence relations, but since we have not discussed those, we will stick with the more ad hoc definition given above.

We are now going to show that $\mathbb{Z}/n\mathbb{Z}$ becomes an abelian group under $\oplus$.

Theorem 4.2.4. The binary operation $\oplus$ endows $\mathbb{Z}/n\mathbb{Z}$ with an abelian group structure.

Proof. The binary operation is associative and commutative because $+$ is associative and commutative on $\mathbb{Z}$. Indeed, for commutativity:

$$\begin{aligned} a \oplus b &= \pi(i(a) + i(b)) \\ &= \pi(i(b) + i(a)) \\ &= b \oplus a, \end{aligned}$$

and similarly for associativity (although this takes more lines to prove - do it as an exercise!).

Next we show that $0 \in \mathbb{Z}/n\mathbb{Z}$ is the identity. For any $a \in \mathbb{Z}/n\mathbb{Z}$, we have

$$0 \oplus a = \pi(i(0) + i(a)) = \pi(0 + i(a)) = \pi(i(a)) = a,$$

and similarly for $a \oplus 0$.

[1] It is also usual to write $\overline{m}$ for $m \pmod{n}$.

Finally, we show that inverses exist. If $0 \neq a \in \mathbb{Z}/n\mathbb{Z}$, let $b := n - a$. We will show that $a \oplus b = 0$:

$$a \oplus b = \pi(i(a) + i(b)) = \pi(i(a) + i(n-a)) = \pi(n) = 0.$$

This finishes the proof. □

Essentially, the theorem tells us that we can add numbers in $\mathbb{Z}/n\mathbb{Z}$ just like we are used to adding numbers in $\mathbb{Z}$, as long as we remember that $n = 0$.

We can actually be very specific about what kind of group $\mathbb{Z}/n\mathbb{Z}$ is.

Theorem 4.2.5. For any $n \geq 1$, $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is a cyclic group of order n. In other words, there exists $a \in \mathbb{Z}/n\mathbb{Z}$ such that $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$.

Proof. We prove the theorem simply by pointing out that $1 \in \mathbb{Z}/n\mathbb{Z}$ is a generator. Indeed,

$$\langle 1 \rangle = \{0, 1, 1 \oplus 1, 1 \oplus 1 \oplus 1, \ldots, 1^{\oplus \operatorname{ord}(1)}\}$$

which is, by definition of $\oplus$, equal to $\{0, 1, 2, \ldots, n-1\} = \mathbb{Z}/n\mathbb{Z}$. □

The next theorem says that $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a group homomorphism for any n, which concretely means that it doesn't matter if we first add numbers in $\mathbb{Z}$ and then reduce the result modulo n, or if we first reduce the terms modulo n and then add them in $\mathbb{Z}/n\mathbb{Z}$.

Theorem 4.2.6. For $a, b \in \mathbb{Z}/n\mathbb{Z}$, we have

$$\pi(i(a) + i(b)) = \pi(i(a)) \oplus \pi(i(b)).$$

Proof. The statement holds because both sides of the equation are equal to $a \oplus b$; namely

$$\pi(i(a) + i(b)) = a \oplus b$$

by definition of $\oplus$, and

$$\pi(i(a)) \oplus \pi(i(b)) = a \oplus b$$

because $\pi \circ i = \mathrm{id}$. □

Exercise 4.2.7. Verify that this works in some examples of your own. For example, compute $(117 + 301) \pmod{21}$ and $\pi(117) \oplus \pi(301)$ and verify that they are the same.

It turns out that we can do the exact same thing with multiplication: we can define a binary operation $\otimes$ on $\mathbb{Z}/n\mathbb{Z}$ via

$$a \otimes b := \pi(i(a) \cdot i(b)).$$

This satisfies the same property: it does not matter whether we multiply first and then reduce mod n or the other way around.

Just like $\mathbb{Z}$ is not a group under multiplication, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication. (Exercise: show that 0 can never have a multiplicative inverse.) However, although in $\mathbb{Z}$ the only elements with multiplicative inverses are 1 and -1, in $\mathbb{Z}/n\mathbb{Z}$ there are typically many more invertible elements. Try to see if you can figure out the following exercise.

Exercise 4.2.8. Can you describe the multiplicative group

$$(\mathbb{Z}/n\mathbb{Z})^{\times} := \{m \in \mathbb{Z}/n\mathbb{Z} \mid m \text{ has a multiplicative inverse}\}?$$

Can you prove that your answer is correct?

We will give an answer to the exercise in the special case where n is a prime number:

Theorem 4.2.9. Let $p \in \mathbb{Z}_{>1}$ be a prime number. Then every non-zero element in $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.

Proof. Let $0 < m < p$ be a non-zero element in $\mathbb{Z}/p\mathbb{Z}$. We first show that m generates $(\mathbb{Z}/p\mathbb{Z}, \oplus)$. By Theorem 4.2.6, we no longer need to care if we first add in $\mathbb{Z}/p\mathbb{Z}$ or in $\mathbb{Z}$. So we have that

$$\operatorname{ord}(m) = \min\{n \in \mathbb{Z}_{\geq 1} \mid nm \text{ is divisible by } p\}.$$

But since p is a prime number, if p divides nm, then it divides either n or m. Since p doesn't divide m, it must divide n, so $\operatorname{ord}(m) = p$. That is, m generates $\mathbb{Z}/p\mathbb{Z}$ as an additive group.

We now show that m has a multiplicative inverse. We know that m generates the additive group, so $m \oplus m \oplus \ldots \oplus m = nm = 1$ for some $0 < n < p$. But then n is the multiplicative inverse of m. □

4.3 Solving equations over $\mathbb{Z}/p\mathbb{Z}$

It is common to use the standard symbols $+$ and $\cdot$ for addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ instead of $\oplus$ and $\otimes$, and we will do that from now on. We also fix a prime number p for the rest of this section.

Because we have addition and multiplication, it makes sense to look at *equations* modulo n. If we have an equation whose coefficients are integers, then we can reduce the whole equation modulo p. For example, we can reduce the function $f(x, y) = x^2 + y^2$ modulo p to get

$$f(x, y) \equiv x^2 + y^2 \pmod{p}.$$

This equation does not depend on p, but the reduction of other equations might. For example, if $g(x, y) = 5x^2 - 3x$, then

$$\begin{aligned} g(x,y) &\equiv x^2 + x \pmod{2}; \\ g(x,y) &\equiv 2x^2 \pmod{3}; \\ g(x,y) &\equiv 2x \pmod{5}. \end{aligned}$$

Exercise 4.3.1. How many solutions does the above equation $f(x, y) = x^2 + y^2$ have in $\mathbb{Z}/p\mathbb{Z}$ for $p = 2$? What about for $p = 3$ and $p = 5$? What about in $\mathbb{R}$?

There is an interesting relationship between solutions of equations modulo p and solutions of equations over $\mathbb{Z}$. As we see from the previous exercise, the number of solutions can change depending on the number system we work in. However, there is a general principle (the *Hasse principle*) which asserts that sometimes, having solutions modulo p, for all primes p, is enough to ensure integer solutions. Sometimes this principle works and sometimes it fails. We conclude with one instance of the Hasse principle which is known.

Theorem 4.3.2 (Hasse principle for quadratic forms)**.** Let $f(x, y)$ be an equation over $\mathbb{Z}$ in which all terms have degree 2, for example

$$f(x, y) = x^2 + 5xy + 2y^2.$$

Then $f(x, y)$ has a non-zero solution in $\mathbb{Z}^2$ if and only if $f(x, y) \pmod{p}$ has a non-zero solution in $(\mathbb{Z}/p\mathbb{Z})^2$ for all prime numbers p.

Note that a solution in $\mathbb{Z}^2$ gives a solution in $(\mathbb{Z}/p\mathbb{Z})^2$ for every p, but the other direction is not obvious. The main use of the theorem is that it implies the following statement: if there exists a prime number p such that $f(x, y)$ has no solutions modulo p, then there are no integer solutions either.

As a final remark, the Hasse principle works for equations $f(x_1, \dots, x_n)$ over $\mathbb{Z}$ for any number of variables n, provided every term in f has degree 2.

4.4 Exercises

Exercise 1

Using modular arithmetic, prove that for integers m and n, $m+n$ is even if m and n are both even or both odd, and $m+n$ is odd otherwise.

Exercise 2

Let n be an integer, and suppose it has a decimal expansion $n = a_1a_2\ldots a_m$ (so that $0 \leq a_i \leq 9$ for all i). Prove that n is divisible by 11 if and only if the alternating sum

$$a_1 - a_2 + a_3 - \ldots + (-1)^{m+1}a_m$$

is divisible by 11. Use this to show that 795142303703 is not a prime number.

Exercise 3

Write down the last digit of n^2 for $n = 0, 1, 2, 3, \ldots$. Do you see a pattern? Can you explain it using modular arithmetic?

Exercise 4

We saw that for a prime number p, we have

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}.$$

1. Use the above in combination with Lagrange's theorem to prove Fermat's Little Theorem: if p is a prime number and $a \in \mathbb{Z}/p\mathbb{Z}$, then $a^p \equiv a \pmod{p}$.
2. If $n \geq 4$ is not a prime number, can you say which elements of $\mathbb{Z}/n\mathbb{Z}$ belong to $(\mathbb{Z}/n\mathbb{Z})^\times$?
3. Compute the last digit of 5123^{99999}. (Hint: use your answer to Exercise 4.2 for $n = 10$ in combination with the ideas from Exercise 4.1.)

Exercise 5

Let $n \in \mathbb{Z}_{>1}$. Prove the following statements:

1. If n is a prime number, then if $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$, either $a = 0$ or $b = 0$.
2. If n is not a prime number, then there exist non-zero elements $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $ab = 0$.

Exercise 6

Check for $p = 3, 5, 7, 11$, and 13 whether or not -1 is a square in $\mathbb{Z}/p\mathbb{Z}$. In other words, verify whether $x^2 = -1$ has solutions modulo p or not. Can you give a general criterion on p that decides when -1 is a square modulo p?

Exercise 7

Use the Hasse principle to prove that the equation

$$f(x,y) = x^2 + 5xy + 7y^2$$

has no non-zero solutions $(x,y) \in \mathbb{Z}^2$.

Exercise 8

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve of discriminant $\Delta = 4a^3 + 27b^2$. Suppose that $a, b \in \mathbb{Z}$, and let p be a prime number such that $p \nmid \Delta$. Define the set

$$E(\mathbb{Z}/p\mathbb{Z}) := \{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\infty\}.$$

Then $E(\mathbb{Z}/p\mathbb{Z})$ is an abelian group with identity element ∞.

1. Prove that $E(\mathbb{Z}/p\mathbb{Z})$ always has finite order. In particular, $\mathrm{ord}(P) < \infty$ for all $P \in E(\mathbb{Z}/p\mathbb{Z})$.

2. Choose specific integers of a, b, and p as above. For the choice you made, can you write down the group structure on $E(\mathbb{Z}/p\mathbb{Z})$ explicitly?

5. Geometry

Geometry is a very broad subject. It encompasses practically all mathematics which has to do with the study of shapes or spaces. Nowadays there are many different kinds of geometry, the most classical of which is Euclidean geometry. That's what we will work with today, but in reality there is also some projective geometry and arithmetic geometry involved in what we do.

5.1 Euclidean geometry

In classical geometry, we work inside n-dimensional Euclidean space, which is defined to be the set $\mathbb{R}^n$ for some positive integer n. For $n = 1$, this is just the real line. For $n = 2$, it's the xy-plane. For $n = 3$, it's three-dimensional space, and after that it gets harder to visualise, but mathematically not much changes: we can consider points $(x, y, z, w) \in \mathbb{R}^4$, for example.

We actually see $\mathbb{R}^n$ not just a set, but as a space in which we can talk about distance. This distance is defined in terms of a *metric* $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, or a distance function, defined as follows:

$$d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) := \sqrt{(x_1 - y_1)^2 + \ldots + (x_n - y_n)^2}.$$

For $n = 1, 2$, and 3, this really gives our intuitive notion of distance between points, by Pythagoras's theorem. We won't usually write this metric on $\mathbb{R}^n$ explicitly, but when we talk about distance in this space, we are actually referring to this function.

Now let's focus on the case $n = 2$, so we are inside the xy-plane. Here we can already do a lot of interesting mathematics. For example, we can see functions $\mathbb{R} \to \mathbb{R}$ geometrically by plotting its graph and studying the function that way. But we can also draw shapes which don't come from functions, such as triangles and circles. An explicit example is the unit circle:

$$S^1 := \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}.$$[1]

Geometry can be useful because humans naturally have geometric intuition. We can often look at shapes and draw conclusions from them more easily than from long lines of equations. However, it's still important to be able to translate your geometric intuition into rigorous mathematics, to make sure that you aren't making any mistakes: maths can be counter-intuitive sometimes!

Let's now look at a nice application of geometry to solve a problem I already mentioned in the introductory lecture, namely: how many Pythagorean triples are there, and can we find all of them? Recall that a Pythagorean triple is a tuple (a, b, c) of positive integers such that $a^2 + b^2 = c^2$. Also, we will for technical reasons restrict to finding the *primitive* triples, i.e. those for which a, b and c have no common factor. Since any Pythagorean triple is a multiple of a primitive one, this is not an important restriction.

Here's how one can solve this problem. We want to find all the (primitive) solutions $(a, b, c) \in \mathbb{Z}^3_{>0}$ of the equation $X^2 + Y^2 = Z^2$. Dividing the equation by Z^2 (which we can do if $Z \neq 0$), this gives the equivalent equation

$$\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 = 1.$$

[1] This looks a lot like the graph of a function, but it isn't: there is no function $f : \mathbb{R} \to \mathbb{R}$ such that $S^1 = \Gamma_f$. Instead, one can view S^1 as the vanishing locus of the function $f(x, y) = x^2 + y^2 - 1$, which is a function $f : \mathbb{R}^2 \to \mathbb{R}$.

But if we make the substitution $x := \frac{X}{Z}$ and $y := \frac{Y}{Z}$, this just says $x^2 + y^2 = 1$. Thus, we have reduced the number of variables in the equation by one. But this comes at a cost: where before we were looking for *integer* solutions to $X^2 + Y^2 = Z^2$, we are now looking for *rational* solutions to $x^2 + y^2 = 1$. In other words, finding all Pythagorean triples is equivalent to answering the following question:

Can we find all points (x, y) on the unit circle with rational coordinates?

There are four points on the unit circle which obviously have rational coordinates, namely $\{(\pm 1, 0), (0, \pm 1)\}$. Miraculously, if we pick one of these, we can find all the other rational points by drawing lines with rational slope through the chosen point and intersecting them with the circle.

Theorem 5.1.1. Let $P = (-1, 0)$. Then there is a bijection

$$\left\{ \begin{matrix} \text{lines through } P \\ \text{with rational slope} \end{matrix} \right\} \xleftrightarrow{1:1} \left\{ \begin{matrix} (x, y) \in \mathbb{Q}^2 \setminus \{P\} \\ \text{such that } x^2 + y^2 = 1 \end{matrix} \right\}$$

Proof. The bijection works as follows: for any line l through P with rational slope, l intersects the circle in exactly one other point. We claim that this point has rational coefficients, and moreover that any point on the circle with rational coefficients can be obtained in this way.

Let $y = a(x + 1)$ be the line through P with slope $a \in \mathbb{Q}$. Then we calculate the point of intersection as follows:

$$\begin{aligned} x^2 + y^2 = 1 \ \text{ and } \ y = a(x+1) \quad &\Longrightarrow \quad x^2 + a^2(x+1)^2 = 1 \\ &\Longleftrightarrow \quad (x+1)^2 - 2x - 1 + a^2(x+1)^2 = 1 \\ &\Longleftrightarrow \quad (x+1)^2(1+a^2) - 2(x+1) = 0 \\ &\Longleftrightarrow \quad (x+1)((x+1)(1+a^2) - 2) = 0 \\ &\Longleftrightarrow \quad x = -1 \text{ or } x = -1 + \frac{2}{a^2+1} = \frac{1-a^2}{1+a^2}. \end{aligned}$$

The solution $x = -1$ corresponds to the point P, whereas $x = -1 + 2/(1 + a^2)$ gives

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

This shows that if $a \in \mathbb{Q}$, then indeed x and y are also rational numbers!
To show that the map is surjective, suppose that (u, v) is a rational point on the unit circle. Then the line through P and (u, v) is $y = \frac{v}{u+1}(x + 1)$, which has rational slope. Hence (u, v) is obtained by intersecting a line through P with the unit circle. □

Let's use this result to explicitly get a formula for the Pythagorean triples.

Theorem 5.1.2. Any primitive Pythagorean triple is of the form

$$\left(q^2 - p^2, 2pq, q^2 + p^2\right)$$

for some positive integers $0 < p < q$.

Proof. For any rational number $a \in \mathbb{Q}$, we can define a line $l_a : y = a(x+1)$ through P with rational slope a. By Theorem 5.1.1, such a line gives a rational point (x, y) on the unit circle, with

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

This corresponds to a Pythagorean triple as follows: we had reduced $X^2+Y^2 = Z^2$ to $x^2+y^2 = 1$ by dividing the equation by Z^2. This procedure kills common factors between X, Y and Z, so going in the other direction might not give us all Pythagorean triples anymore, but it will at least give the primitive ones (and some more - can you give a criterion which says which non-primitive triples occur?). So we need to recover X, Y and Z from x and y. Note that we are not interested in points with $x = 0$ or $y = 0$, since this will give $X = 0$ or $Y = 0$.

Write the rational number a as $a = p/q$, where p and q have no common factors. Then we have

$$x = \frac{1-\frac{p^2}{q^2}}{1+\frac{p^2}{q^2}} = \frac{q^2-p^2}{q^2+p^2}; \qquad y = \frac{2\frac{p}{q}}{1+\frac{p^2}{q^2}} = \frac{2pq}{q^2+p^2}.$$

Now these are fractions of integers, so we get $X = q^2 - p^2, Y = 2pq, Z = q^2 + p^2$. If we want X, Y and Z to all be positive, we need $0 < a < 1$, i.e. p and q have the same sign and $p < q$. Thus, it suffices to take $p, q \in \mathbb{Z}$ with $0 < p < q$. □

The well-known triple $(3, 4, 5)$ is obtained for $(p, q) = (1, 2)$, and the triple $(5, 12, 13)$ is obtained for $(p, q) = (2, 3)$. But we can now also easily generate big Pythagorean triples. For example, $p = 1000, q = 1717$ gives the (primitive) triple

$$(1948089, 3434000, 3948089),$$

corresponding to the fact that

$$3795050751921 + 11792356000000 = 15587406751921.$$

5.2 Solving equations over $\mathbb{Q}$

In the previous section, we have solved an equation over $\mathbb{Q}$: we found all the rational solutions to $f(x, y) = x^2 + y^2 - 1$. This is a degree two equation in two variables, and as we saw above, we have ways of getting the full in this case, although we need to do some work for it. Let's take a step back and see what happens if we only have one variable.

Theorem 5.2.1. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be an equation with rational coefficients a_i. Then any rational number b such that $f(b) = 0$ must be of the form $b = p/q$, where p and q have no common factors, $p \mid a_0$, and $q \mid a_n$.

Proof. Suppose $b = p/q$ is a solution, where the fraction is written in lowest terms, i.e. p and q have no common factors. Then $f(b) = 0$ means that

$$a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \ldots + a_1 \frac{p}{q} + a_0 = 0.$$

Multiplying the equation by q^n gives the integer equation

$$a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n = 0.$$

But all the terms on the left except $a_n p^n$ are divisible by q, and the whole sum is divisible by q (since q divides zero). Hence q also divides $a_n p^n$. But q does not divide p^n because p and q have no common factors, so q divides a_n.
Since all the terms except $a_0 q^n$ are divisible by p, the same logic shows that p divides a_0. □

The point of the theorem is that any one-variable equation over $\mathbb{Q}$ can be easily solved, because there are only finitely many rational numbers which could possibly be solutions, and we can simply try all of them.

Things get more complicated when the number of variables goes up. From now on, we work with equations in two variables x and y.

If the degree is one, we are still in good shape: we can solve equations like $6x + \frac{2}{3}y = 5$. The solutions will always look like some line in the plane.

If the degree is two, we already see different scenarios. For example, consider the equation $x^2 + y^2 = a$. This has no solutions if $a < 0$, one solution if $a = 0$, and infinitely many solutions if $a = 1$ (these are the Pythagorean triples). But what about other values of a? This is something you could explore in a project. I will make the following statement, without further arguments why this should be true (or even what all the words mean):

For degree 2 equations in two variables over $\mathbb{Q}$, there are either no solutions or infinitely many solutions in $\mathbb{Q}^2$, unless the equation is singular, in which case one could get a finite, non-zero number of solutions. If the equation is non-singular, then all solutions can be obtained from a single solution by drawing lines with rational slope and intersecting them with the curve.

While degree two curves are interesting, we now move on to degree three equations: elliptic curves.

5.3 Elliptic curves

Definition 5.3.1. An elliptic curve E over $\mathbb{Q}$ is an equation of the form

$$y^2 = x^3 + ax + b,$$

such that $a, b \in \mathbb{Q}$ and $\Delta := 4a^3 + 27b^2 \neq 0$.

The requirement that $\Delta \neq 0$ is saying precisely that E is *smooth*, i.e. that the graph is differentiable everywhere.

We have seen that elliptic curves come up in the congruent number problem: in particular, we saw that n is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2 x$ has rational points with $y \neq 0$. Mathematicians are interested in them for many different reasons. One of them is that they are the simplest equations which are still too hard to solve via a general method; in particular, we don't know how to tell, for a general elliptic curve E, if the number of solutions of E in $\mathbb{Q}^2$ is finite or infinite. But there is one other big reason, and that is the following: elliptic curves are abelian groups! We just have to add one point "at infinity" for this to work. For this reason, we make the following definition:

Definition 5.3.2. Let E be an elliptic curve over $\mathbb{Q}$. The *rational points* of the elliptic curve are defined as the set

$$E(\mathbb{Q}) := \{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

Here, ∞ can be understood as a formal symbol for an extra element that we are adding to the curve. However, it has a geometric interpretation as a point which lies at the end of the tails of the elliptic curve, infinitely far up (or down) the y-axis. Any vertical line intersects the point ∞. If you want to know more about this, I suggest doing your project about projective geometry, where this is put in a more general framework.

Theorem 5.3.3. Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is an abelian group.

Proof. We define the group law as follows. Suppose P and Q are points in $E(\mathbb{Q})$. Let Z be the third point of intersection of the line through P and Q with E (if $P = Q$, the line through P and Q is the tangent line; if one of P, Q equals ∞, the line is vertical). Draw a vertical line through the point Z; it intersects E in another point. This is the point $P + Q$.

By definition, this group law is a binary operation on $E(\mathbb{Q})$, but we still need to show that it defines an abelian group structure on $E(\mathbb{Q})$. Check the following:

1. The identity is $\infty \in E(\mathbb{Q})$.
2. If $P \in E(\mathbb{Q}) \setminus \{\infty\}$, then $-P$ is the point of intersection of E with the vertical line through P.
3. For all P and Q in $E(\mathbb{Q})$, we have $P + Q = Q + P$.
4. Forget about associativity.

Step 4 is important because associativity is hard to prove for this group structure, but I promise it works. □

We mentioned the rank of an elliptic curve before. We can now define what this is.

Definition 5.3.4. Let E be an elliptic curve over $\mathbb{Q}$. The *rank* of E is the maximal integer $n \geq 0$ such that there exist n distinct elements $P_1, P_2, \ldots, P_n \in E(\mathbb{Q})$ such that

1. $\mathrm{ord}(P_i) = \infty$ for all $i = 1, \ldots, n$;
2. If we have an equality
$$P_i = \sum_{j=1}^{n} m_j P_j$$
with all $m_j \in \mathbb{Z}$, then we must have $m_i = 1$ and $m_j = 0$ for all $j \neq i$.

Note that the rank of E is zero if and only if $E(\mathbb{Q})$ has no elements of infinite order. In fact, this is true if and only if $E(\mathbb{Q})$ is a finite group, but this is not obvious.

Mathematicians have been trying to understand ranks of elliptic curves for many decades. Perhaps the most famous open problem on ranks of elliptic curves is the Birch and Swinnerton-Dyer conjecture. It says something about the difficulty of the congruent number problem that n is a congruent number if and only if $E : y^2 = x^3 - n^2 x$ has positive rank.

The largest known rank of any elliptic curve over $\mathbb{Q}$ is "at least 28", and it is not known if there are elliptic curves with arbitrarily high rank, or if there is some uniform bound. Moreover, it is believed that 50% of all elliptic curves have rank 0 and 50% of all elliptic curves have rank 1.

5.4 Exercises

Exercise 1

The unit circle $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ is denoted by S^1 because a circle is a 1-dimensional sphere. Can you write down the 2-dimensional unit sphere $S^2 \subset \mathbb{R}^3$? What about $S^n \subset \mathbb{R}^{n+1}$?

Exercise 2

Find all solutions in $\mathbb{Q}$ of the following equation:

$$10x^3 - 13x^2 - 8x + \frac{15}{2} = 0.$$

Exercise 3

Does the equation $x^2 + y^2 = 3$ have any solutions $(x, y) \in \mathbb{Q}^2$?

Exercise 4

Consider the equation

$$y^2 = x^3 - tx + 2,$$

where t is a parameter. For which $t \in \mathbb{Q}$ does this define an elliptic curve? What happens to the graph of the equation as t varies?

Exercise 5

We know that 6 is a congruent number, corresponding to the triangle with side lengths $(3, 4, 5)$. Hence the elliptic curve $E : y^2 = x^3 - 36x$ must have a rational point with $y \neq 0$. Find such a rational point. Then use the group law on the elliptic curve to find a second rational point, and compute the side lengths of the triangle which exhibits 6 as a congruent number corresponding to this second point. (Use the bijection from Set Theory Exercise 8.)

Exercise 6

Write down an equation $y^2 = x^3 + ax + b$ over $\mathbb{Q}$ such that $\Delta = 4a^3 + 27b^2 = 0$. Sketch the graph, and find a rational point P on it. Prove that every line with rational slope through P meets the curve in another rational point (unless you chose $a = b = 0$, in which case there may be no points of intersection for some slopes).

6. Possible projects

Based on what we've learned so far, there are a bunch of possible projects you could now attempt. If there is anything that piqued your interest the past week, I encourage you to pick something related to that and explore it. You are also free to choose projects that are not in this list, if you have other ideas – just discuss it with me and we will find a way to make it work. Here are some ideas to get you started:

- Explain a concept or result from the course.
- Explain the solution to an exercise from the exercise sheets.
- Prove Lagrange's theorem from group theory.
- Understand group isomorphisms.
- Prove that a certain number, e.g. 1, is not congruent. (Hint: don't pick a number congruent to 5,6, or 7 modulo 8.)
- Take an equation over $\mathbb{Z}$, for example $y = x^2$. Can you calculate its $\mathbb{Z}/p\mathbb{Z}$-points for any prime p?
- Define $\mathbb{Z}/n\mathbb{Z}$ using equivalence relations.
- Understand for which $p, q \in \mathbb{Z}$ we get *primitive* Pythagorean triples $(p^2 - q^2, 2pq, p^2 + q^2)$, and for which ones we don't.
- Let $P \in E(\mathbb{Q})$ be a rational point on an elliptic curve. Is there any relationship between n and the coordinates of $nP = P + P + \ldots + P$? In particular, how do the sizes of the numerators/denominators of the coordinates of nP grow with n?
- If you like coding: write a function which performs elliptic curve addition.
- Understand the material from one of the appendices and solve one of the exercises from them.

Appendices

A. Projective Geometry

In this appendix, we sketch the formalism of projective geometry, which we use to define the rational points of an elliptic curve. By a *number system* N we will mean either $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}/n\mathbb{Z}$ for some integer $n > 1$.

A.1 Polynomials

What we have been calling "equations", mathematicians usually call *polynomials.* A polynomial f in n variables over a number system N is an expression

$$f(x_1, \ldots, x_n) = \sum_{\overline{m} \in \mathbb{N}_0^n} a_{\overline{m}} x_1^{m_1} \ldots x_n^{m_n},$$

where:

1. the sum runs over all tuples $\overline{m} = (m_1, \ldots, m_n) \in \mathbb{N}_0^n$;
2. $a_{\overline{m}} \in N$ for all $\overline{m} \in \mathbb{N}_0^n$;
3. $a_{\overline{m}} \neq 0$ only for finitely many $\overline{m}$.

The *degree* of a polynomial f is the highest power appearing in f, i.e.

$$\deg(f) = \max\{m_1 + m_2 + \ldots + m_n \mid a_{\overline{m}} \neq 0\}.$$

We say f is *homogeneous* if every term in f has the same degree.

Examples A.1.1.
1. $f(x) = x^2$ can be considered as a homogeneous degree 2 polynomial over any number system.
2. $f(x, y) = 3x^2 + \frac{1}{2}xy^3$ is a degree 4 polynomial over $\mathbb{Q}$ (or any other number system containing 3 and 1/2). It is not homogeneous.
3. $f(x, y, z) = 3x^3 + 2y^3 + z^3 - xyz$ is a homogeneous polynomial of degree 3.

A.1.1 Homogenisation of polynomials

Let $f(x_1, \ldots, x_n)$ be a polynomial. There is a way to make f into a homogeneous polynomial, at the cost of introducing an extra variable x_0.

Definition A.1.2. Let $f(x_1, \ldots, x_n)$ be a polynomial of degree d. The *homogenisation* of f is defined to be

$$\tilde{f}(x_0, \ldots, x_n) := x_0^d f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

Exercise A.1.3. Compute the homogenisation of some polynomials f, and confirm that they are indeed homogeneous polynomials of the same degree as f.

Once you get what's going on, you won't need the definition of the homogenisation anymore to write down what it looks like; the procedure is very intuitive.

A.1.2 Solutions of polynomials

Given a polynomial $f(x_1, \ldots, x_n)$ with coefficients in a number system N, we can look at its solutions in the set N^n. This is by definition the set of all elements $(x_1, \ldots, x_n) \in N^n$ such that $f(x_1, \ldots, x_n) = 0$. For instance, if we take $N = \mathbb{R}$, the solutions of $f(x, y) = x^2 + y^2 - 1$ form the unit circle in $\mathbb{R}^2$.

If f is homogeneous, we make the following observation. Suppose $f(x_1, \ldots, x_n) = 0$. Then if $\lambda \in N$ is a non-zero number, we also have

$$f(\lambda x_1, \ldots, \lambda x_n) = \lambda^{\deg(f)} f(x_1, \ldots, x_n) = \lambda^{\deg(f)} \cdot 0 = 0.$$

Hence, if we have found a solution to a homogeneous polynomial, then multiplying that solution by another number gives a new solution. Moreover, $0 := (0, \ldots, 0) \in N^n$ is always a solution to any non-constant homogeneous polynomial. Phrased more geometrically, if we have found a solution $0 \neq \overline{x} \in N^n$ to a homogeneous polynomial f, then any point on the line through 0 and $\overline{x}$ is also a solution to f.

It would make more sense to see every such line as a single solution to the homogeneous equation, so that the set of solutions doesn't contain "superfluous information". This motivates the following definition.

Definition A.1.4. Let $n \in \mathbb{N}_0$, and let N be a number system in which every non-zero element has a multiplicative inverse (so we just exclude $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ when n is not prime). Then *projective n-space over N* is the set

$$\{[x_0 : x_1 : \ldots : x_n] \mid x_i \in N \ \forall i, \text{ and at least one } x_i \neq 0\},$$

where by definition, $[x_0 : \ldots : x_n] = [\lambda x_0 : \ldots : \lambda x_n]$ for any non-zero $\lambda \in N$.

Thus, for any number system N, the set $\mathbb{P}^0_N$ is just a point. Going up one dimension, we get

$$\mathbb{P}^1_N = \{[1 : a] \mid a \in N\} \cup \{[0 : 1]\}.$$

Thus, $\mathbb{P}^1_N$ is in bijection with the set $N^1 \cup \{\infty\}$. For example, we can picture $\mathbb{P}^1_{\mathbb{R}}$ as the real line where both ends meet in the point $\infty := [0 : 1]$. Geometrically, $\mathbb{P}^1_{\mathbb{R}}$ looks like a circle.

Exercise A.1.5. Let $f(x_1, \ldots, x_n)$ be a polynomial over N, and let $\tilde{f}(x_0, x_1, \ldots, x_n)$ be its homogenisation. Prove that there exists an injective function

$$\{\text{solutions of } f \text{ in } N^n\} \longrightarrow \{\text{solutions of } \tilde{f} \text{ in } \mathbb{P}^n_N\},$$

and give some examples where the map is not surjective. We call the points which are not in the image of this map the *points at infinity* of $\tilde{f}$.

Exercise A.1.6. A *line* in $\mathbb{P}^2_N$ is the solution set to a homogeneous equation

$$a_0 x_0 + a_1 x_1 + a_2 x_2 = 0, \quad a_i \in N.$$

Prove that for any two distinct points x and y in $\mathbb{P}^2_n$, there is a unique line through x and y.

Exercise A.1.7. Let E be an elliptic curve over $\mathbb{Q}$, defined by the polynomial

$$f(x, y) = y^2 - x^3 - ax - b.$$

Prove that the homogenisation of f has exactly one point at infinity. Prove that any line through the point at infinity and a point on E has vertical slope.

B. The Weil Conjectures

This appendix consists of a brief introduction to the Weil conjectures for elliptic curves. The Weil conjectures are deep theorems in arithmetic geometry which took mathematicians decades to prove. If you have a good grip on the material discussed in these notes, this might be a good topic for your project. If not, I recommend you to stick with something more basic and understand that first.

B.1 Finite fields

Definition B.1.1. A *field* is a triple $(K, +, \times)$, where K is a set and $+$ and $\times$ are binary operations on K, such that the following axioms are satisfied:

(F1) The pair $(K, +)$ is an abelian group with identity $0 \in K$;

(F2) The pair $(K^\times := K \setminus \{0\}, \times)$ is an abelian group with identity $1 \in K$;

(F3) For every $a, b, c \in K$, we have $a(b + c) = ab + ac$.

Examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ for prime numbers p. We say a field is a *finite field* if it has finitely many elements. We will state, but not prove, the following theorem:

Theorem B.1.2 (Classification of finite fields)**.** *Let K be a finite field. Then K has p^n elements, for some prime number p and some $n \geq 1$. Moreover, for each $q = p^n$, there is only one example of such a field (up to isomorphism). We denote it by $\mathbb{F}_q$.*

The last part of the statement means that any two fields of the same order must have the same field structure. This is far from true for finite groups: for instance, both C_4 and the Klein four group have order 4, but the former is cyclic whereas the latter isn't (since every element of the Klein four group has order 2). Note also that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Example B.1.3. The theorem says that there is a unique field $\mathbb{F}_4$ of order 4. It can be written as $K = \{0, 1, a, b\}$, where $a^2 = b$, $b^2 = a$, $ab = 1$, and $a + b = 1$. Note that $(\mathbb{F}_4, +)$ has the structure of the Klein four group, while $(\mathbb{F}_4^\times, \times)$ is a cyclic group of order 3.

We also have the following important result:

Theorem B.1.4. *Let $f : \mathbb{F}_q \to \mathbb{F}_{q'}$ be a field homomorphism. Then the following statements hold:*

1. *$q = p^n$ and $q' = p^m$ for the same prime p;*
2. *The integers n and m satisfy $n \mid m$;*
3. *f is injective.*

B.2 Elliptic curves over finite fields

We defined elliptic curves over $\mathbb{Q}$ as equations $y^2 = x^3 + ax + b$ such that $\Delta = 4a^3 + 27b^2 \neq 0$. In particular, a pair of integers $a, b \in \mathbb{Z}$ with $\Delta \neq 0$ defines an elliptic curve over $\mathbb{Q}$. Examples are the elliptic curves $y^2 = x^3 - n^2x$ related to the congruent number problem. We also defined the rational points of an elliptic curve as

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

We can just as well define elliptic curves and their rational points over $\mathbb{F}_q$, by copying the above definition but replacing $\mathbb{Q}$ by $\mathbb{F}_q$ everywhere. (There is the small complication that for $p \in \{2, 3\}$, there are elliptic curves over $\mathbb{F}_{p^n}$ which are not given by an equation of the form $y^2 = x^3 + ax + b$. However, any such equation with $\Delta \neq 0$ still defines an elliptic curve even for these primes, so we will not care about this.)

Let E be an elliptic curve over $\mathbb{Q}$ such that the coefficients a, b of $f(x, y) = y^2 - x^3 - ax - b$ are integers. Let p be a prime number. Then we can define the reduction of E modulo p to be the elliptic curve defined by $f \pmod p$. For this to be an elliptic curve over $\mathbb{F}_p$, we need that $\Delta \not\equiv 0 \pmod p$. If this condition holds, we say p is *a prime of good reduction.* Any elliptic curve has infinitely many primes of good reduction.

Suppose now that E is an elliptic curve over $\mathbb{F}_q$, for example obtained via reduction modulo p if $q = p$. Then thanks to Theorem B.1.4, we can see E as an elliptic curve over $\mathbb{F}_{q^m}$ for any $m \geq 1$. Hence we can study the finite abelian groups

$$E(\mathbb{F}_{q^m}) = \{(x, y) \in (\mathbb{F}_{q^m})^2 \mid f(x, y) = 0\} \cup \{\infty\}.$$

In particular, one can ask the following interesting question:

Can we predict the order of $E(\mathbb{F}_{q^n})$ for any n?

The answer to this question follows from a special case of the *Weil conjectures.* The Weil conjectures are three deep statements about varieties over finite fields, conjectured by André Weil in 1949. The most difficult statement (the so-called "Riemann hypothesis", in analogy with the Riemann hypothesis for the Riemann zeta function) was proved in full generality in 1974 years later by Pierre Deligne. This concluded 25 years of intense research in arithmetic geometry inspired by the Weil conjectures, which completely transformed algebraic and arithmetic geometry. The Weil conjectures state that, rather miraculously, one only has to know $|E(\mathbb{F}_q)|$ in order to determine $|E(\mathbb{F}_{q^m})|$ for all m.

Here's how it works. Define $N_m := |E(\mathbb{F}_{q^m})|$ for all $m \geq 1$. We put these into a generating function as follows:

$$Z(E, t) := \exp\left(\sum_{m=1}^{\infty} \frac{N_m t^m}{m}\right).$$

We call $Z(E, t)$ the *Hasse-Weil zeta function* of E. Now the Weil conjectures say that in particular, the following is true:

Theorem B.2.1 (Weil conjectures for elliptic curves)**.** Let E be an elliptic curve over $\mathbb{F}_q$. Then the Hasse-Weil zeta function is a rational function:

$$\frac{qt^2 - a_E t + 1}{(1 - t)(1 - qt)},$$

where $a_E := q + 1 - |E(\mathbb{F}_q)|$. Moreover, if we write $qt^2 - a_E t + 1 = (1 - \alpha t)(1 - \beta t)$ for $\alpha, \beta \in \mathbb{C}$, then $\beta = \overline{\alpha}$ and $|\alpha| = |\overline{\alpha}| = \sqrt{q}$.

Exercise B.2.2. Use the Weil conjectures to deduce a formula for N_m.

Exercise B.2.3. Heuristically, one would expect the order of $E(\mathbb{F}_q)$ to be roughly $q+1$. Explain why, and explain how the Weil conjectures imply the so-called *Hasse bound:*

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}$$