Numbers and Sets

Adam Kelly

October 27, 2020

This set of notes is a work-in-progress account of the course 'Numbers and Sets', originally lectured by Professor Imre Leader in Michaelmas 2020 at Cambridge. These notes are not a transcription of the lectures, but they do roughly follow what was lectured (in content and in structure).

These notes are my own view of what was taught, and should be somewhat of a superset of what was actually taught. I frequently provide different explanations, proofs, examples, and so on in areas where I feel they are helpful. Because of this, this work is likely to contain errors, which you may assume are my own. If you spot any or have any other feedback, I can be contacted at ak2316@cam.ac.uk.

Contents

0 Introduction

Numbers and sets is one of the first course in pure mathematics that you will take as an undergraduate at Cambridge. In a sense, it is the 'starting course', in that it will introduce you to the 'pure maths' way of thinking about things. This introduction will happen through the lense of thinking about objects, beginning with the natural and real numbers. You will be introduced to the 'thoughtful way' of thinking about such objects, that you can carry through to almost every other course in pure mathematics.

§0.1 Structure of the Course

This course is divided into four sections.

1. *Elementary Number Theory*

   This is a section that almost everybody enjoys. We deal with number theory first, which is elementary not in the sense that it is easy but in the sense that it is our 'first steps' in the subject. The main aim of this section is to get used to the additive and multiplicative structure of the natural numbers.

   It is like that some of you will be familiar with this material already, but nothing in this section will be assumed, and everything will be built from the ground up.

2. *The Reals*

   This section has a different perspective, centering on the questions of *what is a real number* and *what can we assume about them?* This is one of the harder parts of this course, and many of the definitions contain a subtlety that is not present in other sections.

3. *Sets and Functions*

   This is a 'terminology' section. There is no exciting theorems, mostly notation, definitions, and so on. It is a short section, but it is somewhat boring in that sense.

4. *Countability*

   This section is best described as 'fun with infinite sets'. It is to do with the concepts introduced in section 3 (in the sense that we are thinking about sets and functions), but it has a very different flavour. You will find results in this section that are both interesting and surprising. Almost everyone likes this section.

Everything in the sections above makes up the 'course'. If you are wondering what is examinable, it will be everything that was lectured. It is possible that this set of 'lecture notes' will contain additional content that was both not in lectures and not examinable. If you want to be sure whether something you are reading here or elsewhere is examinable, you can get a more formal answer in the schedules.

§0.2 Books

As with most mathematics courses in Cambridge, you will not need a textbook to follow this course. What is covered in lectures is enough to do both the example sheets and the examinations for this course. Still, you might find that a textbook can provide a different perspective, additional worked examples, and additional material that you may find informative, helpful or fun.

In particular, the following books are quite relevant/good, but there is no expectation that you will look at these.

- R. T. Allenby, *Numbers and Proofs*.

  This book is readable, easy to understand and clear.

- A. G. Hamilton, *Numbers, Sets and Axioms*.

  Another readable and clear book, but with a different flavour to the previous book.

- H. Davenport, *The Higher Arithmetic*.

  This book can be thought of as showing 'where things go next'. It is very interesting, and goes quite a bit beyond this course. It is worth noting however that this book contains no exercises.

You should be able to find all of these books in either your college library or the university library.

§0.3 Example Sheets

As is normal for a 24 lecture course, there will be 4 example sheets. You should be able to have a good go at the first one after lecture 3 or 4.

§0.4 A Brief Note About These Notes

This set of notes differs from what was lectured in a number of areas. I have attempted to briefly outline these changes below.

In the original lecture course, there was two lectures that (informally) introduced the idea of a proof, along with examples and non-examples of what a proof is. This material has been purposefully excluded, and familiarity with proofs (and common logical notation such as $\forall$, $\exists$, and $\implies$) is assumed. If you are interested in reading a brief introduction to proofs, I will direct you to this quite readable introduction.

I have also included additional exposition on the Peano axioms, along with a more detailed look at how addition, multiplication, etc are defined. In the original lectures, this material was purposefully omitted. The exposition included in these notes closely follows the development in Tao's *Analysis I* (see the bibliography).

1 Elementary Number Theory

Number theory is the branch of mathematics that studies the properties of *numbers*, with a particular emphasis on the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$ and occasionally the rationals $\mathbb{Q}$. In this section, we will study some of the *additive* and *multiplicative* structure of the integers, looking at divisors, primes and tools such as modular arithmetic.

One of the aims of this course (and this section in particular) is to study numbers 'from the ground up', being quite careful about what we assume. This goal immediately presents us with a question: what exactly is a 'number'?

§1.1 The Peano Axioms

What are the natural numbers? Intuitively, we might say that they are a set[1] $\mathbb{N} = \{1, 2, 3, \dots\}$, created by starting at 1 and counting forward indefinitely, each time obtaining an object distinct from all of the previous ones. This does answer our question (a natural number is any element of $\mathbb{N}$), but has created a series of other questions. For example, what does it mean to 'count forward', and how can it be done 'indefinitely'? How are we allowed to use these natural numbers, in regard to defining things like addition and multiplication?

Instead of attempting to answer these questions using our informal, intuitive definition of the natural numbers, we will instead use a definition that is more precise. Namely, we will define the natural numbers using the Peano axioms. We will state the rules or *axioms* that natural numbers satisfy, which will define the natural numbers in terms of *how they work*, rather than *what they are*. After clearly setting out this definition, we will be in a much stronger position to write concrete mathematical proofs about the natural numbers.

Definition 1.1.1 (Peano Axioms)

The **natural numbers** are a set $\mathbb{N}$, along with a function $S : \mathbb{N} \to \mathbb{N}$ and an object '1' satisfying the following axioms:

1. $1 \in \mathbb{N}$.
2. If $n \in \mathbb{N}$, then $S(n) \in \mathbb{N}$.
3. $S(n) \neq 1$ for every $n \in \mathbb{N}$.
4. If $n, m \in \mathbb{N}$ and $n \neq m$, then $S(n) \neq S(m)$.
5. *Induction.* Let $P(n)$ be any property about a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(S(n))$ is also true. Then $P(n)$ is true for every natural number n.

This should match with our original, informal definition of the natural numbers. We have formalized the 'counting forward' process with the *successor function* $S(n)$.

[1] We will look at sets later in the course, but an informal familiarity will be assumed from the beginning

Remark. We are going to assume various things about the way we write down natural numbers using the decimal system. You can assume that when we write something like $n = 3$, we really mean $n = S(S(1))$ etc.

§1.1.1 Addition

Now we have defined natural numbers, but as of yet we can do nothing more look upon them fondly and increment them using the function $S(n)$. We will now begin to remedy that by defining addition and multiplication.

Definition 1.1.2 (Addition)

We define **addition** to be an operation $+$ such that for $m, n \in \mathbb{N}$, we have $m + 1 = S(m)$, and $m + (n + 1) = (m + n) + 1$.

This definition defines addition for all natural numbers by induction. We are now able to state and prove various properties of addition.

Proposition 1.1.3 (Properties of Addition)

For all $a, b, c \in \mathbb{N}$. Then

(i) *Addition is commutative.* $a + b = b + a$.

(ii) *Addition is associative.* $(a + b) + c = a + (b + c)$.

(iii) *Cancellation law.* If $a + b = a + c$ then $b = c$.

Proof Sketch. Use induction.[a] □

[a] The proofs for these sorts of statements tend do be slightly dull and laborious, and for this reason they have been excluded. If you wish to read them, I encourage you to consult a textbook/some other reference material.

§1.1.2 Order

We can now use addition to define an ordering on the natural numbers.

Definition 1.1.4 (Ordering of the Natural Numbers)

Let $n, m \in \mathbb{N}$. We say that n is **greater than or equal to** m, written $n \geq m$ if and only if $n = m$ or $n = m + a$ for some $a \in \mathbb{N}$. We say n is **strictly greater than** m if $n \geq m$ and $n \neq m$.

Proposition 1.1.5 (Properties of Ordering)

Let $a, b, c \in \mathbb{N}$. Then

(i) *Order is reflective.* $a \geq a$.

(ii) *Order is transitive.* If $a \geq b$ and $b \geq c$, then $a \geq c$.

(iii) *Order is anti-symmetric.* If $a \geq b$ and $b \geq a$, then $a = b$.

(iv) *Addition preserves order.* $a \geq b$ if and only if $a + c \geq b + c$.

(v) $a > b$ if and only if $a \geq b + 1$.

Proposition 1.1.6 (Trichotomy)

Let a and b be natural umbers. Then exactly one of the following is true: $a < b$, $a = b$ or $a > b$.

§1.1.3 Multiplication

We can also define another familiar operation, multiplication, in the same inductive/recursive fashion that we defined addition.

Definition 1.1.7 (Multiplication)

We define **multiplication** to be an operation $\times$ such that for $m, n \in \mathbb{N}$, $m \times 1 = m$, and $m \times (n + 1) = (m \times n) + m$.

As before, induction implies that this is defined for all natural numbers. It also guarantees that multiplying two natural numbers is a natural number.

Notation. We will use $a \times b = a \cdot b = ab$ when referring to multiplication.

Proposition 1.1.8 (Properties of Multiplication)

For all $a, b, c \in \mathbb{N}$. Then

(i) *Multiplication is commutative.* $a \times b = b \times a$.

(ii) *Multiplication is associative.* $(a \times b) \times c = a \times (b \times c)$.

(iii) *Distributive law.* $a \times (b + c) = a \times b + a \times c$.

(iv) *Cancellation law.* If $a \times b = a \times c$ then $b = c$.

(v) *Multiplication preserves order.* If $a < b$, then $a \times c < b \times c$.

Remark. The final two statements in the proposition above, the cancellation law and that multiplication preserves order, only hold because we are dealing with natural numbers. These properties do not hold in general if we allow a, b or c to be integers.

We could go further and define other common operations such as exponentiation, factorials and so on, all of which can be defined in the same fashion. However, in the interest of space, these definitions have been omitted.

§1.2 Strong Induction

There is a more useful form of induction that can be used, now that we have defined an ordering on the natural numbers.

Proposition 1.2.1 (Strong Induction)

Suppose that we have some property $P(n)$ about a natural number n. If we have $P(1)$, and for all $n \in \mathbb{N}$ we have that $P(m)$ for $m \leq n$ implies $P(n+1)$, then $P(n)$ holds for all $n \in \mathbb{N}$.

Proof. This follows from ordinary induction using the property "$P(n)$ for all $m \leq n$". □

Informally, the principle of strong induction means that whenever we are proving some property $P(n)$ holds for all $n \in \mathbb{N}$ by induction, we can feel free to assume that $P(m)$ holds for $m \in \mathbb{N}$ with $m < n$.

Remark (For Pedants)**.** Technically, we don't need to check the case $P(1)$ separately, as it is implied by the condition if suitably interpreted. Still, it's safer to just check $P(1)$.

Some other equivalent but useful[2] forms of induction are listed below. Let $P(n)$ be a property, then

- *Existence of a Minimal Counterexample*

  If $P(n)$ is false for some $n \in \mathbb{N}$, then there exists $n_0 \in \mathbb{N}$ such that $P(n_0)$ is false but $P(m)$ is true for all $m < n$.

- *The Well-Ordering Principle*

  If $P(n)$ is true for some $n \in \mathbb{N}$, then there exists a minimal n_0 such that $P(n_0)$ is true.

§1.3 The Integers and Rationals

The previous section defined the natural numbers, along with some ways that we can use them. We will now go one step further and define the *integers*, and the *rationals*.

Definition 1.3.1 (Integers)

The **integers** are a set $\mathbb{Z}$ consisting of all symbols n, $-n$ and 0, where $n \in \mathbb{N}$.

We can then define addition, multiplication and subtraction in (and subtraction) on the integers by extending our definition on the natural numbers in the obvious way. We can also check that the properties of addition we had before still hold. There are some additional properties that the integers have.

Proposition 1.3.2 (Algebraic Properties of the Integers)

Let $a, b \in \mathbb{Z}$. Then[a]

(i) *Identity.* $a + 0 = a$.

(ii) *Existence of an Additive Inverse.* For all $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0$.

[2] Some texts will claim that we can replace the induction axiom in Peano axioms with one of these other forms. This is incorrect, and typically one will need to add additional axioms alongside to keep the set of axioms equivalent.

[a] These properties imply that the integers are a *group*.

Proof. $a+0 = a$ holds automatically due to our definition of addition on the integers. Then, we always have a $b \in \mathbb{Z}$ such that $a + b = 0$, as we can let $b = -a$. □

We also obtain another interesting property of multiplication.

Proposition 1.3.3 (Zero Product Law)

Let a and b be integers such that $a \times b = 0$. Then either $a = 0$, $b = 0$ or both.

Proof. Assume for the purposes of contradiction that both $a \neq 0$ and $b \neq 0$. Then we must have either $a > 0$ or $a < 0$ by trichotomy. If $a > 0$, then $a \times b > 0$ if $b > 0$, or $a \times b < 0$ if $b < 0$. Otherwise, if $a < 0$, then $a \times b < 0$ if $b > 0$, or $a \times b > 0$ if $b < 0$. These are all possible cases, and thus we never have that $a \times b = 0$. Thus at least one of a and b must be zero. □

Remark (Caveats)**.** We noted earlier that there was some properties of the natural numbers that don't hold over the integers. Specifically, if we have $a < b$ for $a, b \in \mathbb{Z}$, and we multiply by a negative number, then the order is no longer preserved (it is switched). Also, the cancellation law only applies when we are cancelling a non-zero integer.

We can now use the integers to define the *rationals*.

Definition 1.3.4 (Rationals)

The **rationals** are a set $\mathbb{Q}$ of expressions a/b for some $a, b \in \mathbb{Z}$, with $b \neq 0$. We will define equality between rationals such that $a/b = c/d \iff ad = bc$.

This definition implicitly defines $\mathbb{Q}$ using *equivalence classes*, which will be discussed later. We need to be slightly more careful in defining addition on $\mathbb{Q}$, as we will need to ensure that it respects the equality relation between rationals.

Definition 1.3.5 (Addition on $\mathbb{Q}$)

For a/b and $c/d \in \mathbb{Q}$, we define addition such that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

We will now need to explicitly check that this definition is valid.

Proposition 1.3.6

Addition is well defined on $\mathbb{Q}$.

Proof. Let $a/b = a'/b'$ and $c/d = c'/d'$ be rationals. We show that

$$\begin{aligned} &\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \\ \iff &\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \\ \iff &(ad+bc)(b'd') = (a'd'+b'c')(bd) \\ \iff &(ab')dd' + (cd')bb' = (a'b)d'd + (c'd)bb', \end{aligned}$$

which follows from $ab' = a'b$ and $cd' = c'd$. □

To see why such a check was needed, consider the following example.

Example 1.3.7

We *cannot* define an operation on $\mathbb{Q}$ sending $a/b \to a^2/b^3$, as we would have $1/2 \to 1/8$ and $2/4 \to 4/64 = 1/16$, which is inconsistent.

We can then define multiplication in the same way as it was defined for integers, and we can check that all of the usual properties still hold. We can also define ordering, where $a/b < c/d$ if $ab < bc$. The rules from ordering $\mathbb{Z}$ still hold.

With all of these definitions in place, we can now start looking at some of the more interesting properties of numbers.

§1.4 Primes and Divisibility

We will now begin to discuss some actual number theory, beginning with the incredibly important concept of *divisibility*. You are likely to be familiar with this already, so we will jump into some definitions.

Definition 1.4.1 (Divisibility)

For $a, b \in \mathbb{N}$, we say that a **divides** b, written $a \mid b$ if there exists some $c \in \mathbb{N}$ such that $b = ac$.

If this is the case, we say that b is a **multiple** of a, and that a is a **divisor** of b. We can now define one of the most fundamental objects in number theory, the *primes*.

Definition 1.4.2 (Primes)

A natural number $n \geq 2$ is a **prime** if its only divisors are 1 and n. If a natural number is not prime, then it is **composite**.

With this definition, we can begin to state and prove some interesting results about the primes, which should hint at their importance in number theory.

Theorem 1.4.3

Every natural number is expressible as a product of primes.

Proof. We use induction on n. For $n = 2$ this is true, as 2 is prime. Now given $n > 2$, if n is prime, then we are done. If not, then n is composite so $n = ab$ for some $1 < a, b < n$. By our induction hypothesis, we have $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_l$ for some (not necessarily distinct) primes $p_1, \cdots p_k, q_1, \cdots, q_l$, hence $ab = p_1 \cdots p_k q_1 \cdots q_l$, which is the product of primes. Thus we are done by induction. □

A nice consequence of this theorem is that the primes go on forever.

Theorem 1.4.4 (Euclid)

There are infinitely many primes.

Proof. Suppose there was finitely many primes, say $p_1, \cdots, p_k$. Then consider the number $N = p_1 p_2 \cdots p_k + 1$. Then N has no prime factors, contradicting the fact that n can be written as the product of primes[a]. □

[a] This theorem has an amusingly large number of proofs. A short discussion can be found in the book 'Proofs from the Book'.

Remark. There is no 'pattern' to the primes, in the sense that there is no algebraic formula for the nth prime.

So we know that a number can be written as the product of primes, but is this unique (up to some reordering)? This would seem to be true from experience, so why can't we write a number as the product of primes in two ways. For example, why can't we have $41 \times 101 = 67 \times 73$? Informally, we might think that this is impossible because we can't have 41 dividing 'a bit of' 67 and 'a bit of 73'. What we really need to show that prime factorization is unique is the following: For a prime p, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Now should this lemma be easy to prove, or hard to prove? That is, should this follow straight from definitions, or not? The answer is that it *cannot* follow straight from definitions. This is because it's about 'primes dividing things', but we define the primes with 'things diving it'. This is the wrong way round! It will take some amount of work to be able to prove this.

§1.4.1 Greatest Common Divisors

This section will begin to build some machinery that will allow us to tackle the problem of showing that prime factorizations are unique. We will begin by defining the notion of *greatest common divisor*, also known as *highest common factor*[3].

Definition 1.4.5 (Greatest Common Divisor)

For $a, b \in \mathbb{N}$, a natural number d is the **greatest common divisor** of a and b, written $d = \gcd(a, b)$ if

(i) $d \mid a$ and $d \mid b$;

(ii) If $c \mid a$ and $c \mid b$, then $c \mid d$.§

We want to show that the greatest common divisor always exists.

[3] This was the term used in the lectures, but I prefer greatest common divisor, so I will use that instead.

Proposition 1.4.6 (Divison Algorithm)

For $n, k \in \mathbb{N}$, we can write $n = qk + r$, where $q, r \in \mathbb{N}$ and $0 \leq r < k$.

Proof. We use induction on N. For $n = 1$, this is clearly true. Otherwise, given $n > 1$, we can write $n - 1 = qk + r$ by our inductive hypothesis. Then, if $r < k - 1$, we can write $n = qk + (r + 1)$, and if $r = k - 1$, we can write $n = q(k + 1)$. □

The division algorithm is related to the greatest common divisor using the following lemma.

Lemma 1.4.7 (Euclid)

For $a, b \in \mathbb{N}$, we can write $a = bq + r$ using the division algorithm. Then $\gcd(a, b) = \gcd(b, r)$.

Proof. If $d \mid a$ and $d \mid b$, then $d \mid a - bq = r$. Otherwise, if $d \mid b$ and $d \mid r$, then $d \mid bq + r = a$, hence the set of common divisors between a and b is the same as the set of divisors between b and r. Thus $\gcd(a, b) = \gcd(b, r)$. □

Theorem 1.4.8 (Euclidean Algorithm)

For $a, b \in \mathbb{N}$, if we repeatedly apply the division algorithm to get

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1}, \end{aligned}$$

then $\gcd(a, b) = r_{n-1}$.

Proof. We repeatedly apply Lemma 1.4.7 until we have $\gcd(a, b) = \gcd(r_{n-1}, 0) = r_{n-1}$. □

The Euclidean Algorithm gives us both a proof that $\gcd(a, b)$ exists for any natural numbers a and b, and it also gives us an efficient way to find it.

Example 1.4.9

To find $\gcd(87, 52)$, we perform the following series of steps.

$$\begin{aligned} 87 &= 1 \times 52 + 35 \\ 52 &= 1 \times 35 + 17 \\ 35 &= 2 \times 17 + 1 \\ 17 &= 17 \times 1, \end{aligned}$$

thus $\gcd(87, 52) = 1$.

Notation. We will sometimes write $\gcd(87, 52) = \text{hcf}(87, 52) = (87, 52) = 1$. And when $\gcd(a, b) = 1$, we say that a and b are **coprime** or **relatively prime**.

The example above showed that $\gcd(87, 52) = 1$, so is it possible to write $1 = 87x + 52y$ for some $x, y \in \mathbb{Z}$? Looking at the computation we performed to find the greatest common divisor, we can work backwards to get

$$\begin{aligned} 1 &= 1 \times 35 - 2 \times 17 \\ &= 1 \times 35 - 2 \times (52 - 35) \\ &= -2 \times 52 + 3 \times 35 \\ &= -2 \times 52 + 3 \times (87 - 52) \\ &= 3 \times 87 - 5 \times 52, \end{aligned}$$

so it is indeed possible. In fact, there was nothing special about 87 and 52 here, we just used the sequence of steps performed in the Euclidean algorithm. We can formalize this.

Theorem 1.4.10

For all $a, b \in \mathbb{N}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

Proof. Run the Euclidean algorithm on a and b, say with some output r_n. Then we can write r_n as some integer linear combination of r_{n-1} and r_{n-2}. We can continue this to write any r_i as an integer linear combination of r_{i-1} and r_{i-2}. Thus eventually, we be able to write $r_n = ax + by$ for some $x, y \in \mathbb{Z}$, and as $r_n = \gcd(a, b)$, we are done. □

Alternate Proof. Let h be the least positive integer linear combination of a and b. We claim that $h = \gcd(a, b)$. If $d \mid a$ and $d \mid b$, then $d \mid ax + by$ for any $x, y \in \mathbb{Z}$, thus $d \mid h$. Now suppose that $h \nmid a$. Then $a = qh + r$ for some $q, r \in \mathbb{Z}$, with $0 < r < h$. So $r - ah = a - q(ax + by)$, which is also a linear combination of a and b. But this is impossible, as it contradicts the minimality of h. Thus $h \mid a$, and by the same argument $h \mid b$. Thus $h = \gcd(a, b)$. □

Remark. The second proof of the theorem above tells us that the greatest common divisor exists, but offers no way to find it, nor a way to find x or y.

This theorem has an interesting application: solving linear diophantine[4] equations.

Corollary 1.4.11 (Bezout's Lemma)

Let $a, b, c \in \mathbb{N}$. Then the equation

$$ax + by = c$$

has an integer solution if and only if $\gcd(a, b) = c$.

Proof. Let $h = \gcd(a, b)$. If we have a solution $ax + by = c$, then $h \mid a$ and $h \mid b$, thus $h \mid c$. Now, if $h \mid c$, then we have $h = ax + by$ for $a, b \in \mathbb{Z}$ by our previous theorem, and thus we can write $c = \frac{c}{h}ax + \frac{c}{h}by$. Note that $\frac{c}{h}$ is guaranteed to be an integer by our previous argument. □

[4] A diophantine equation is one where you seek only integer solutions.

§1.4.2 The Fundamental Theorem of Arithmetic

We are now in a position to prove the lemma that was discussed quite a few pages ago, which will lead us directly to the uniqueness of prime factorizations.

Theorem 1.4.12 (Euclid's Lemma)

Let p be a prime, and $a, b \in \mathbb{N}$. Then $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proof. Suppose that $p \nmid a$. We wish to show that $p \mid b$. Then we have $\gcd(a, p) = 1$, which implies that we can write $ax + py = 1$, for some integers x and y. Then we can multiply by b to get $abx + pby = b$. But then $p \mid ab$ by our hypothesis, and thus $p \mid abx + pby = b$, and so we are done. □

Remark. This theorem implies that if $p \mid a_1 a_2 \cdots a_k$, then p must divide at least one of a_i, for $1 \leq i \leq k$.

Theorem 1.4.13 (Fundamental Theorem of Arithmetic)

Every natural number $n \geq 2$ is uniquely expressible as a product of primes, up to re-ordering.

Proof. We already proved that such a product exists, so we will now prove that such a product is unique. We use induction on n. Suppose that $n = p_1 \cdots p_k = q_1 \cdots q_l$, where p_i, q_i are all primes. We wish to show that $k = l$, and after reordering, $p_i = q_i$ for all i. We have $p_1 \mid q_1 \cdots q_k$, so $p_1 \mid q_i$ for some i. We can (without loss of generality) label that prime q_1. Hence $p_1 = q_1$. So $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_l$, thus by induction $k = l$ and $p_2 = q_2$, $p_3 = q_3$, etc. □

Aside: Why Unique Factorization Isn't Obvious

In the fundamental theorem of arithmetic, we took the 'things that can't be broken up' (the primes) and we broke up every number as a product of these, uniquely. The same concept makes sense in other places.

Consider instead $\mathbb{Z}[\sqrt{-3}]$, the set of complex numbers of the form $x + y\sqrt{-3}$, where $x, y \in \mathbb{Z}$. For example, $2 + 7\sqrt{-3}$. With these objects, we can both addition and multiplication two elements in $\mathbb{Z}[\sqrt{-3}]$, and always get back an element in $\mathbb{Z}[\sqrt{-3}]$. This allows us to talk about the notions of 'divides' and 'multiple of' etc in $\mathbb{Z}[\sqrt{-3}]$.

You might think that you can take the 'things you can't break up' in $\mathbb{Z}[\sqrt{-3}]$, and take any element and break it up into those. This is obviously correct (by definition). You may then want to say that this is unique, but that would not be true. For example,

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

and all of the terms in this product are 'things you can't break up' in $\mathbb{Z}[\sqrt{-3}]$. This allows us to conclude that unique factorization *fails* in $\mathbb{Z}[\sqrt{-3}]$.

The fundamental theorem of arithmetic has some useful applications.

- *Factors*

  Let's consider what are the factors of $2 \cdot 3^7 \cdot 11$ are. Certainly any $2^a \cdot 3^b \cdot 11^c$ where $0 \leq a \leq 3$, $0 \leq b \leq 7$ and $0 \leq c \leq 1$ is a factor. Also, there can't be any others. For example, if $7 \mid 2 \cdot 3^7 \cdot 11$, then we'd get a prime factorization involving a 7, which would contradict the uniqueness of prime factorization.

  In general, the factors of $n = p_1^{a_1} \cdots p_k^{a_k}$ are precisely numbers of the form $p_1^{b_1} \cdots p_k^{b_k}$, where $0 \leq b_i \leq a_i$, for all $1 \leq i \leq k$.

- *Greatest Common Divisors*

  If we wanted to find the common factors of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$, we could note that the common factors are $2^a \cdot 3^b \cdot 11^c$, where $0 \leq a \leq 3$, $0 \leq b \leq 2$ and $0 \leq c \leq 1$. So the greatest common divisor is $2^3 \cdot 3^2 \cdot 11$.

  In general the greatest common divisor of $p_1^{a_1} \cdots p_k^{a_k}$ and $p_1^{b_1} \cdots p_k^{b_k}$ (with $a_i, b_i \geq 0$) is $p_1^{\min(a_1,b_1)} \cdots p_k^{\min(a_k,b_k)}$.

- *Lowest Common Multiples*

  The common multiples of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$ are all of the form $2^a \cdot 3^b \cdot 5^c \cdot 11^d \cdot 13^e \cdot n$ (for a positive integer n) where $a \geq 4, b \geq 7, c \geq 1, d \geq 3$ and $e \geq 1$. We can then get the lowest common multiple as $2^4 \cdot 3^7 \cdot 5^1 \cdot 11^3 \cdot 13^1$.

  Then in general, the lowest common multiple of $p_1^{a_1} \cdots p_k^{a_k}$ and $p_1^{b_1} \cdots p_k^{b_k}$ (with $a_i, b_i \geq 0$) is $p_1^{\max(a_1,b_1)} \cdots p_k^{\max(a_k,b_k)}$.

§1.5 Modular Arithmetic

It is a common occurrence in number theory that we will consider numbers that differ by a multiple of some fixed number to be equivalent. An example of this is the value of $(-1)^n$, which depends only on whether n is odd or even – that is, the values of n that differ by a multiple of 2 will give the same result. To give another example, the last digit of two numbers will be the same when the numbers differ by some multiple of 10. Modular arithmetic (or congruence notation) is a way of expressing such equivalences, where we have two integers a and b that differ by some fixed number m.

Definition 1.5.1 (Integers Modulo n)

Let $n \in \mathbb{N}$. The **integers modulo** n, written $\mathbb{Z}/n\mathbb{Z}$ consist of the integers where we regard two to be the same if they differ by a multiple of n.

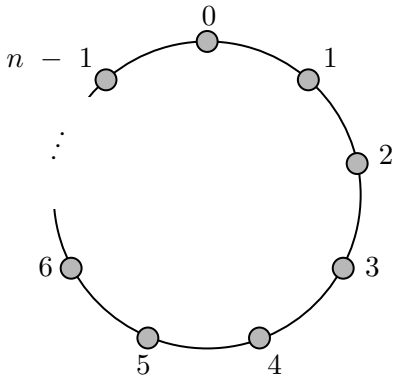
Definition 1.5.2 (Congruence Notation)

If x and y are integers that are the same modulo n, then we write

$$x \equiv y \pmod{n}.$$

This notation implies that $x \equiv y \pmod{n}$ if and only if $n \mid x - y$, that is, if $x = y + kn$ for some $k \in \mathbb{Z}$. Note that no two of $0, 1, \ldots, n-1$ are congruent $\pmod{n}$, and every $x \in \mathbb{Z}$ is congruent to exactly one of these modulo n (this follows from the division algorithm).

We can view $\mathbb{Z}/n\mathbb{Z}$ as the following picture (indeed this is the 'correct picture' of $\mathbb{Z}/n\mathbb{Z}$).



With this mental picture, we can begin to build up some properties of modular arithmetic.

Proposition 1.5.3 (Arithmetic Modulo n)

If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a+b \equiv a'+b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Proof. We have $a' = a + kn$ and $b' = b + jn$, for some $k, j \in \mathbb{Z}$. So $a' + b' = a+b+(k+j)n \equiv a+b \pmod{n}$, and $a'b' = (a+kn)(b+jn) = ab+(bk+aj+kjn)n \equiv ab \pmod{n}$. □

Many of the other rules of arithmetic are inherited from $\mathbb{Z}$, for example we have $a+b \equiv b+a \pmod{n}$ as $a+b = b+a$ in $\mathbb{Z}$. Also some of the number-theoretic facts we have previously established can be expressed in modular arithmetic.

Example 1.5.4 (Euclid's Lemma in Modular Arithmetic)

The statement that for a prime p, '$p \mid ab \implies p \mid a$ or $p \mid b$' is equivalent saying that $ab \equiv 0 \pmod{p}$ implies that $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{0}$.

§1.5.1 Modular Inverses

We will now begin to look at the multiplicative structure of $\mathbb{Z}/n\mathbb{Z}$.

Definition 1.5.5 (Modular Inverses)

For $a, b \in \mathbb{Z}$, we say that b is an **inverse** of a if $ab \equiv 1 \pmod{n}$.[a]

[a] This should be reminiscent of the notion of inverses from group theory.

Example 1.5.6

In $\mathbb{Z}/10\mathbb{Z}$, the inverse of 3 is 7, as $3 \times 7 = 21 \equiv 1 \pmod{10}$. The inverse of 4 does not exist, as for all $x \in \mathbb{Z}$, $4x \not\equiv 1 \pmod{10}$, as $4x$ is even.

This example shows that inverses do not always exist for an arbitrary modulus n.

Notation. We write a^{-1} to mean the inverse of a (modulo some n).

Proposition 1.5.7 (Properties of Modular Inverses)

In $\mathbb{Z}/n\mathbb{Z}$,

(i) If a modular inverse exists, then it is unique modulo n.

(ii) If a has an inverse, and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$. That is, we can cancel invertible elements.[a]

[a] We *cannot* cancel elements in general.

Proof. To show (i), suppose there exists $b, c \in \mathbb{Z}$ such that for some a, $ab \equiv ac \equiv n \pmod{n}$. Then $b(ac) \equiv bab \implies c \equiv b \pmod{n}$. Then to show (ii), we can just multiply both sides by a^{-1}. □

When we are working modulo a prime, things tend to be 'nicer'.

Proposition 1.5.8

Let p be a prime, then every $a \neq 0 \pmod{p}$ has an inverse modulo p.

Proof. We have $\gcd(a, p) = 1$, so we can write $ax + py = 1$ for some $x, y \in \mathbb{Z}$. But then $ax = 1 - py$, and thus $ax \equiv 1 \pmod{p}$. □

Alternate Proof. In $\mathbb{Z}/n\mathbb{Z}$, consider the multiples of a: $0 \times a$, $1 \times a$, $2 \times a$, $\ldots$, $(p-1) \times a$. We wish to show that one of them is 1. We have p items written down, and I claim these are all *distinct* in $\mathbb{Z}/p\mathbb{Z}$. If $ia = ja \implies (i-j)a \equiv 0$, which implies $a \equiv 0$ or $i - j \equiv 0 \implies i \equiv j \pmod{p}$. Hence, there must be $0, 1, \ldots, p-1$ in this list, in some order. Thus $xa \equiv 1 \pmod{p}$, for some $x \in \mathbb{Z}/n\mathbb{Z}$. □

We can generalize this proposition by considering which properties of the primes we used in the previous proof.

Proposition 1.5.9

Let $n \in \mathbb{N}$. Then a has an inverse modulo n if and only if $\gcd(a, n) = 1$.

Proof. We have $\gcd(a, n) = 1 \iff ax + ny = 1$, for some $x, y \in \mathbb{Z}$. Then $ax = 1 - ny \equiv 1 \pmod{n}$. □

There is a commonly used function to count how many elements have an inverse modulo some n.

Definition 1.5.10 (Euler's Totient Function)

Euler's totient function $\phi(n)$ is the number of numbers $1, 2, \ldots, n$ that are relatively prime to n. This function counts the number of invertibles or **units** in $\mathbb{Z}/n\mathbb{Z}$.

Example 1.5.11

If p is a prime, then $\phi(p) = p - 1$, $\phi(p^2) = p^2 - p$ (we cannot have $p, 2p, \ldots, pp$). If p and q are distinct primes, then $\phi(pq) = pq - p - q + 1$.

§1.5.2 Exponentiation

Consider the powers of 2 in $\mathbb{Z}/7\mathbb{Z}$. We have the sequence

$$\begin{aligned} 2^1 &\equiv 2 \pmod 7 \\ 2^2 &\equiv 4 \pmod 7 \\ 2^3 &\equiv 1 \pmod 7 \\ 2^4 &\equiv 2 \pmod 7 \\ &\vdots \end{aligned}$$

This sequence will repeat periodically, with a period of 3. It turns out that in general, this will always occur. This can be seen in the following theorem, which turns out to be an incredibly important result which is used all the time. This theorem has many proofs, but we present one particularity nice one, which emphasizes the theory that we have developed so far.

Theorem 1.5.12 (Fermat's Little Theorem)
Let p be a prime, then for $a \not\equiv 0 \pmod p$, we have

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

Proof. Consider the numbers $1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a$ modulo p. They are distinct, as if $ai \equiv aj$ then $i \equiv j \pmod p$, because a is invertible. They are also non-zero. So we must have the numbers $1, 2, \dots, p-1 \pmod p$ in some order. Then, if we multiply together we have

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p,$$

so we can cancel $(p-1)!$ as it's the product of invertibles, to obtain $a^{p-1} \equiv 1 \pmod p$. □

As before, we can consider what happens in the case of a non-prime modulus.

Theorem 1.5.13 (Fermat-Euler Theorem)
Let $n \in \mathbb{N}$. Then for $a \not\equiv 0 \pmod n$, we have

$$a^{\phi(n)} \equiv 1 \pmod n.$$

Proof. We copy the proof of Fermat's little theorem. Let the units in $\mathbb{Z}/n\mathbb{Z}$ be $x_1, \dots, x_{\phi(n)}$. Consider $a \cdot x_1, a \cdot x_2, \dots, a \cdot x_{\phi(n)}$. They are distinct and invertible as before, so they must be $x_1, \dots, x_{\phi(n)}$ in some order. Multiplying them all together,

$$a^{\phi(n)} x_1 x_2 \cdots x_{\phi(n)} \equiv x_1 x_2 \cdots x_{\phi(n)} \pmod n,$$

and then we can cancel each x_i to obtain $a^{\phi(n)} \equiv 1 \pmod n$. □

We can pause for a moment and notice that in the proof of Fermat's little theorem, we could cancel $(p-1)! \pmod p$ because it was non-zero. So what exactly was it? We can

try an example of $p = 5$, then we have $4! = 1 \equiv 24 \equiv -1 \pmod 5$. We can also try $p = 7$ to get $6! = 720 \equiv -1 \pmod 7$. It can be proved that this is always the case.

First, we prove a small lemma.

Lemma 1.5.14

Let p be prime, then $x^2 \equiv 1 \pmod p$ implies $x \equiv 1$ or $x \equiv -1 \pmod p$.[a]

[a] Note that this is only true because p is prime. For example, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

Proof. $x^2 \equiv 1 \implies x^2 - 1 \equiv 0 \pmod p$, which we can factor as $(x+1)(x-1) \equiv 0 \pmod p$ and thus $x \equiv 1$ or $x \equiv -1 \pmod p$. □

Remark. It turns out that for a prime p, a non-zero polynomial in $\mathbb{Z}/p\mathbb{Z}$ of degree k always has at most k roots.

We can now prove our result about the value of $(p-1)! \pmod p$.

Theorem 1.5.15 (Wilson's Theorem)

Let p be a prime, then

$$(p-1)! \equiv -1 \pmod p.$$

Proof. Note that this is true for $p = 2$, so we may assume that $p \geq 2$. Consider the numbers $1, 2, \ldots, p-1$ modulo p. We can pair up each a with its inverse a^{-1} for $a \neq a^{-1}$. But $a = a^{-1} \iff a^2 = 1$, so the only elements that are their own inverse are 1 and -1. Thus $1, 2, \ldots, p-1$ consists of some pairs a, a^{-1} and 1 and -1. Thus when we multiply, $(p-1)! \equiv 1^{\frac{p-3}{2}} \cdot 1 \cdot -1 \equiv -1 \pmod p$. □

To see how we can use both Wilson's theorem and Fermat's little theorem together, we can consider another question that follows naturally from Lemma 1.5.14.

Lemma 1.5.16 ($x^2 + 1$ Lemma)

Let p be an odd prime. Then $x^2 \equiv -1 \pmod{-1}$ has a solution if and only if $p \equiv 1 \pmod 4$.

Proof. If $p = 4k + 3$, suppose that $x^2 \equiv -1 \pmod p$. Then we have from Fermat's little theorem that $x^{4k+2} \equiv 1 \pmod p$, but $x^{4k+2} \equiv (x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1$, which is a contradiction.

We now construct an example to show that $p \equiv 1 \pmod 4$ works. By Wilson's theorem, $(4k!) \equiv -1 \pmod p$. Then, noting that $4k - j \equiv -j - 1 \pmod p$, $(2k)!^2 \equiv (2k!)^2 \cdot (-1)^{2k} \equiv (4k)! \equiv -1 \pmod p$, so a solution exists. □

§1.5.3 Congruence Equations and the Chinese Remainder Theorem

We now return back to the topic of linear diophantine equations, this time looking specifically at linear congruence equations. Let's look at an example.

Example 1.5.17 (Solving a Linear Congruence Equation)
Solve $7x \equiv 4 \pmod{30}$.

Solution. First we *find a solution.*

We have $\gcd(7, 30) = 1$, so we can run the Euclidean algorithm on 7 and 30 to obtain $7 \times 13 - 30 \times 3 = 1$. So $7 \times 13 \equiv 1 \pmod{30}$, hence $7 \times 52 \equiv 4 \pmod{30}$. So $x \equiv 52 \pmod{30}$ is a solution.

Now we show there is *no more solutions.*

If x' is a solution, then we have $7x \equiv 4 \pmod{30}$ and $7x' \equiv 4 \pmod{30}$. Thus $7x \equiv 7x' \pmod{30}$, which implies that $x \equiv x' \pmod{30}$ as 7 is invertible. So $x \equiv 52 \pmod{30}$ is the only solution. □

There is a shorter method that can be used too, if we can quickly spot the inverse of the coefficient of our variable.

Example 1.5.18
Solve $3x \equiv 9 \pmod{28}$.

Solution. $3x \equiv 9 \pmod{28} \iff 19 \cdot 3x \equiv 19 \cdot 9 \pmod{28}$, as 19 is invertible. Thus $x \equiv 171 \equiv 3 \pmod{8}$. □

If we don't have that the coefficient and the modulus is coprime, it's typically easier to write the equation as a standard linear diophantine equation.

Example 1.5.19
Solve $10x \equiv 12 \pmod{34}$.

Solution. $10x \equiv 12 \pmod{34} \iff 10x = 12 + 34y$ for some $y \in \mathbb{Z}$. Then $10x = 12 + 34y \iff 5x = 6 + 17y$, which we can write as $5x \equiv 6 \pmod{17}$. We can then solve as before. □

Now consider a simultaneous congruence equation. Specifically, consider the equations

$$\begin{aligned} x &\equiv 6 \pmod{17} \\ x &\equiv 2 \pmod{19}. \end{aligned}$$

Do we expect a solution to this? We might guess yes, as 17 and 19 are coprime, so intuitively 'modulo 17 and modulo 19 should be independent of each other'. What about these equations:

$$\begin{aligned} x &\equiv 6 \pmod{34} \\ x &\equiv 11 \pmod{36}. \end{aligned}$$

We shouldn't expect solutions to these equations. Even if you try and figure out if x is even or odd, you'll run into issues. This intuition can be formalized into a theorem.

Theorem 1.5.20 (Chinese Remainder Theorem)

Let m and n be relatively prime positive integers. Then for any integers a and b, there is solution to

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n, \end{aligned}$$

and this solution is unique modulo mn.

Proof. First we prove existence. We have $ms + nt = 1$ for some $s, t \in \mathbb{Z}$ by Bezout's lemma. Then $ms \equiv 0 \mod m$ and $1 \pmod n$ and $nt \equiv 0 \pmod n$ and $1 \pmod m$. Hence $x = a(nt) + b(ms)$ has $x \equiv a \pmod m$ and $x \equiv b \pmod n$.

To show uniqueness, certainly any $x' \equiv x \pmod{mn}$ is also a solution. Conversely, suppose x' has $x' \equiv a \pmod m$ and $b \pmod n$. Then $x' \equiv x \pmod m$ and $x' \equiv x \pmod n$, that is, $m \mid x' - x$ and $n \mid x' - x$. Thus $mn \mid x' - x$, as $\gcd(m, n) = 1$, and thus $x' \equiv x \pmod{mn}$. □

This theorem generalizes directly.

Theorem 1.5.21 (General Chinese Remainder Theorem)

Let $m_1, \ldots, m_k$ be pairwise relatively prime positive integers, and let

$$M = m_1 m_2 \cdots m_k.$$

Then for all integers $x_1, \ldots, x_k$, the equations

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_k \pmod{m_k} \end{aligned}$$

have a solution x that is unique modulo M.

Proof Sketch. Reduce the number of equations by applying the two variable Chinese remainder theorem to the last two equations. □

§1.5.4 An Application of the Fermat-Euler Theorem: RSA Encryption

RSA is an algorithm that underpins a huge amount of modern cryptography and security.

Normally, to send a coded message to someone, you would encode the message, which you could then send to the intended receiver who would decode it. This decoding would be performing the encoding operation in reverse – they are inverse operations. Because of this, it would seem obvious in this way that knowing how to encode is the same as knowing how to decode. For example, if your encoding is 'add 1 to each letter', a *Caesar cipher*, then you immediately know how to decode: 'take 1 from each letter'. For another example, if your encoding is 'add 1 to each letter then reverse each word', then to decode you 'reverse each word and subtract 1 to each letter'. This belief, that

knowing how to encrypt implies knowing how to decrypt, was held for centuries, but it isn't quite correct. We will see this in the RSA encryption system.

Begin with two large distinct primes p and q, and let $n = pq$. Let's say we want to encrypt some element $x \in \mathbb{Z}/n\mathbb{Z}$ – this may involve taking the message we want to send and splitting it up in some way. We will do that in the following way.

Fix a 'coding exponent' e. To encode a message $x \in \mathbb{Z}/n\mathbb{Z}$, raise it to the power e.

$$x \longmapsto x^e.$$

Now let's figure out how to decode this message. We want some $d \in \mathbb{Z}/n\mathbb{Z}$ so that $(x^e)^d \equiv x \pmod{n}$. First, assume that x and n are coprime (ensure that the message x is constructed to have this condition). We know from the Fermat-Euler theorem that $x^{\phi(n)} \equiv 1 \pmod{n}$, and also that $x^{k\phi(n)} \equiv 1 \pmod{n}$, for all $k \in \mathbb{Z}$. So we have

$$x^{k\phi(n)+1} \equiv x \pmod{n}.$$

So it suffices to find a d such that $de = k\phi(n) + 1$, for some $k \in \mathbb{Z}$. That is, we want an inverse of e modulo $\phi(n)$. We can do this by running the Euclidean algorithm on the numbers e and $\phi(n)$. This implies we needed to have picked e coprime with $\phi(n)$.

With the encryption and decryption methods defined, we can now consider what information is needed to perform each step.

To encode, we take $x \longmapsto x^e \pmod{n}$[5]. This means we need to know that will need to know n (so you know what modulus to use) and also the power e.

To decode, we take $y \longmapsto y^d \pmod{n}$, so we need to know n and d. But we worked out d as the inverse of e modulo $\phi(n)$, so we really need n, e and $\phi(n)$. Recall that

$$\phi(n) = n - p - q + 1.$$

So to compute $\phi(n)$, we need to know the factors of n. However, the problem of factoring n is thought to be incredibly hard, and the best known methods of today would take longer than the age of the universe to factor n into two 100 digit long primes. This means that if e and n were published, then anyone could encode a message, but only you (or someone who knows the factors of n) would be able to decode. So, with RSA encryption, anyone can encrypt a message and send it to you, but only you can decrypt it.

[5]This process can be done quite quickly by squaring the number whenever possible.

2 The Reals

Moving on from number theory, this chapter will center on the questions of *what is a real number* and *what can we assume like them*. Unlike when we defined the natural numbers, in this chapter we will not just define the reals formally and then proceed as normal; instead, we will try and understand some of the more subtle aspects of the real numbers, that will eventually be carried through in 'Analysis'.

§2.1 Why We Need Real Numbers

Recall that in chapter 1, we began by defining the natural numbers $\mathbb{N}$, extended them to the integers $\mathbb{Z}$, and extended them to the rationals $\mathbb{Q}$. So why would we not stop there? In the following example, we will show that for some (many) purposes, the rationals are not adequate.

Proposition 2.1.1

There is no $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof. Assume that $x \geq 0$. If there was such a rational, we could write

$$x = \frac{a}{b},$$

where $a, b \in \mathbb{Z}$. We can square this to get

$$x^2 = \frac{a^2}{b^2} = 2 \implies a^2 = 2b^2,$$

but this is a contradiction of the fundamental theorem of arithmetic, as the power of 2 in a^2 would have to be odd[a]. □

Alternate Proof. Suppose that for some $x = a/b \in \mathbb{Q}$ where $a, b \in \mathbb{N}$, we have $x^2 = 2$. Note that for any integers c and d, the number $cx + d$ is of the form e/b, for some $e \in \mathbb{Z}$. So, if $cx + d > 0$, then $cd + d > \frac{1}{b}$. But $x^2 = 2 \implies 0 < x - 1 < 1$, we can say $0 < (x-1)^k < 1/b$ for large enough k. But this is a contradiction, because $(x-1)^k$ is of the form $cx + d$. □

[a] The same proof shows that if there exists $x \in \mathbb{Q}$ so that $x^2 = n$, for $n \in \mathbb{N}$, then n must be a square number. This is because each exponent in the prime factorisation of n must be even.

Informally, what this result shows is that $\mathbb{Q}$ has a 'gap' at $\sqrt{2}$, and in constructing the reals, we will try formally define a number system that has no such 'gaps'. This immediately raises the question of how we can define such a system, formalizing our rather vague notion of a 'gap'. This must be done while only making statements about the rationals.

Consider again our example that there is no rational x such that $x^2 = 2$. With this in mind, define the set S as follows:

$$S = \{x \in \mathbb{Q} \ : \ x^2 < 2\}.$$

It should be clear that 1.5 is an upper bound on the elements in this set. 1.42 is also an upper bound. By setting such upper bounds, we can get arbitrarily close to a number x such that $x^2 = 1$, that is there cannot be a*least* upper bound. If there was, it would have to be a number so that $x^2 = 2$, but we know there isn't such a rational. It's using this idea of 'least upper bounds' that we can define the reals.

Definition 2.1.2 (The Reals)

The reals are a set $\mathbb{R}$ with elements 0 and 1 (where $0 \neq 1$), along with operations $+$ and $\times$ and an ordering $<$ such that:

1. $+$ is commutative, associative, has an identity 0, and every $x \in \mathbb{R}$ has an inverse.
2. $\times$ is commutative, associative, has an identity 1, and every $x \in \mathbb{R}$ where $x \neq 0$ has an inverse.
3. $\times$ is distributive over $+$.
4. $\forall a, b$, exactly one of $a < b$, $a = b$ and $b < a$ holds. Also if $a < b$ and $b < c \implies a < c$.
5. $\forall a, b, c \in \mathbb{R}$, $a < b \implies a + c < b + c$ and $a < b \implies ac < bc$ if $c > 0$.
6. *Least Upper Bound.* Every set of reals is non-empty and has a least upper bound.

Definition 2.1.3

A set S is **bounded above** if there exists $x \in \mathbb{R}$ with $x \geq y$ for all $y \in S$. Such an x is a **least upper bound** of S if x is an upper bound for S, and every upper bound x' of S satisfies $x < x'$.

Bibliography

- T. Tao, *Analysis I*

  This book provides discussion of the Peano axioms, along with some relevant proofs that were (purposefully) excluded from the lectures. The treatment of the Peano axioms in these notes follow this exposition closely.