# Numbers and Sets

Adam Kelly

Michaelmas 2020

None of the notes here have been reviewed at all, and are just exactly what was taken down live in the lectures. I would turn around now and come back in a few days, when I have gone back, cleaned things up, fixed explanations and added some structure.

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 chapters.

1. *Elementary Number Theory*

   This is a chapter 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 chapter 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 chapter will be assumed, and everything will be built from the ground up.

2. *The Reals*

   This chapter 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 chapters.

3. *Sets and Functions*

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

4. *Countability*

   This chapter is best described as 'fun with infinite sets'. It is to do with the concepts introduced in Chapter 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 chapter that are both interesting and surprising. Almost everyone likes this chapter.

Everything in the chapters above makes up the 'course'. If you are wondering what is examinable, it will be everything in these lecture notes (unless otherwise stated). For a more formal answer to that question, have a look at 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

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.

# §1 Elementary Number Theory

This chapter is looking at the properties of the natural numbers. We will begin by defining exactly what they are, in a way that hopefully matches your own intuition.

## §1.1 The Peano Axioms

Intuitively, the natural numbers $\mathbb{N}$ consist of the list of numbers

$$1, 1+1, 1+1+1, 1+1+1+1, \dots$$

In this list, every 'number' is distinct from the previous, and then it goes on forever with some vague notion of '…'. Let's try and make this precise.

Instead of trying to say what a natural number *is*, we will instead define *how they work*, that is, *what we can assume about them.* We do this by specifying the axioms that the natural numbers satisfy, that (hopefully) define that structure in a way that matches our intuitive idea of the natural numbers.

**Definition 1.1** (Peano Axioms)

The natural numbers, written $\mathbb{N}$, is a set containing an element '1', and an operation '$+1$' that satisfies the following axioms.

(i) For all $n \in N$, $n+1 \neq 1$.

(ii) If $n \neq m$, then $n+1 \neq m+1$.

(iii) For any property $p(n)$, if it is the case that $p(1)$ is true, and for every $n$ we have $p(n) \implies p(n+1)$, then $p(n)$ is true for all $n \in \mathbb{N}$. This is the **induction axiom**.

**Remark.** We will write 2 for $1+1$ and so on.

With the operation $+1$ defined, we can define the operation $+k$ for any $k \in \mathbb{N}$.

**Definition 1.2** (Addition)

We define the operation of *addition* so that

$$n + (k+1) = (n+k) + 1,$$

for every natural number $k \in \mathbb{N}$.

This is defined for all natural numbers by induction. In a similar way, we can define multiplication, powers, order, etc, and we can prove the basic properties that they satisfy. Some of these are listed below.

**Proposition 1.3**

For all $a, b \in \mathbb{N}$:

(i) $a + b = b + a$.

(ii) $ab = ba$.

(iii) $a + (b + c) = (a + b) + c$.

(iv) $a(bc) = (ab)c$.

(v) $a(b+c) = ab + ac$.

(vi) If $a < b$ then

- $a + c < b + c$.
- $ac < bc$.
- If $b < c$ then $a < c$.

**Remark.** This is the last time that we'll dump a bunch of statements – that's not what this class is about.

## §1.2 Strong Induction

There is a more useful form of induction called **strong induction**.

**Proposition 1.4** (Strong Induction)
If $p(n)$ is some property and 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 Sketch.* We can deduce this from ordinary induction by considering the property $q(n)$, where $q(n)$ is the statement '$p(n)$ for all $m \leq n$'. □

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

**Remark** (The Correct View of Induction)**.** Normally, to prove $p(n)$ for every $n \in \mathbb{N}$, we take an $n$ and we show $p(n)$. Strong induction says: if it would help to assume $p(m)$ for some $m < n$, feel free to do so.

We also have some equivalent forms of (strong) induction.

1. If $p(n)$ is false for some $n$, then for some $n$ we must have $p(n)$ false but $p(m)$ is true for all $m \geq n$.

   "If there is a counterexample, then there is a *minimal* counterexample".

2. If $p(n)$ for some $n$, then there is a *least* $n$ with $p(n)$. This is known as the **well-ordering principle**.

## §1.3 The Integers

The integers $\mathbb{Z}$ consists of all symbols $n$, $-n$ and 0, where $n \in \mathbb{N}$. We can define addition, multiplication, etc on $\mathbb{Z}$ from $\mathbb{N}$. We can also check all of the algebraic rules that we had before.

- $\forall a$, $a + 0 = a$;
- $\forall a$, $\exists b$ such that $a + b = 0$.
- Define $a < b$ if $\exists c \in \mathbb{N}$ such that $a + c = b$. All of the normal riles still hold, except we need to have the following:

$\forall a, b, c$, If $a < b$ and $c > 0$ then $ac = bc$.

## §1.4 The Rationals

The rationals, written $\mathbb{Q}$, consist of all expressions $\frac{a}{b}$, where $a, b$ are integers with $b \neq 0$ We regard $\frac{a}{b} = \frac{c}{d}$ if $ad = bc$.

We can define addition to be

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

We can check that it does not matter how we wrote $\frac{a}{b}$ or $\frac{c}{d}$.

**Example 1.5**

We *cannot* define an operation on $\mathbb{Q}$ sending $\frac{a}{b}$ to $\frac{a^2}{b^3}$, as $\frac{1}{2}$ and $\frac{2}{4}$ are sent to different places.

Similarity for $\cdot$, we can check that the usual arithmetic rules hold, and allow $\forall a \neq 0$, $\exists b$ such that $ab = 1$.

We can define an ordering on the rationals, so that $\frac{a}{b} < \frac{c}{d}$ (where $b, d > 0$) if $ab < bc$. We can check that the rules from ordering on $\mathbb{Z}$ still hold.

**Remark.** We can view $\mathbb{Z}$ as being inside $\mathbb{Q}$, by identifying $a \in \mathbb{Z}$ with $\frac{a}{1} \in \mathbb{Q}$.

THE MATHS NOW STARTS!

## §1.5 Primes

The additive structure of $\mathbb{N}$ is straightforward. We can start with 1, keep applying the operation '+1', and eventually we will get all of the natural numbers. The multiplicative structure of $\mathbb{N}$ is not as straightforward

**Definition 1.6** (Multiples and Divisors)

For a natural number $n$, the **multiples** of $n$ are all the integers of the form $kn$ for some integer $k$.

If $m$ is a multiple of $n$, we can say that $n$ **divides** $m$, or that $n$ is a **divisor** or **factor** of $m$. This is written $n \mid m$.

We can now define what a prime is.

**Definition 1.7** (Primes)

A natural number $n \geq 2$ is **prime** if its only divisors are 1 and $n$.

If $n \geq 2$ is not prime, then it is **composite**. Our aim is to 'break up' any number into primes – for example $63 = 3 \times 3 \times 7$.

**Proposition 1.8**

Every natural number $n \geq 2$ 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. □

**Remark.** We can define an empty product (i.e. of *no* primes) to be 1.

**Theorem 1.9** (Euclid)

There are infinitely many primes.

*Proof.* Suppose there was finitely many primes, say $p_1, \ldots, p_k$. 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.[1] □

**Theorem 1.10** (Euclid's Lemma)

For any prime $p$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

**Remark.** Should this theorem be 'hard' to prove, in the sense of will it follow directly from definitions or not? The answer is that it will not come directly from the definitions. We defined primes with 'things dividing it' but this question deals with 'primes dividing things'! This means that it is going to be 'hard'.

*Proof.* We will get back to this later. □

**Proposition 1.11**

The prime factorisaion of a number is unique.

*Proof.* We will also get back to this later. □

## §2 Greatest Common Divisors

**Definition 2.1**

For $a, b \in \mathbb{N}$, we say $c$ is the **greatest common divisor** of $a$ and $b$ if $c$ is a common factor, that is, $c \mid a$ and $c \mid b$, and if $d \mid a$ and $d \mid b$ then $d \mid c$. We write $\gcd(a, b) = c$.

**Example 2.2**

$\gcd(18, 12) = 6$, as the factors of 18 are $1, 2, 3, 6, 9, 18$, and the factors of 12 are $1, 2, 3, 4, 6, 12$, so the common factors are $1, 2, 3, 6$, the greatest of which is 6.

We want to show that we always have a greatest common divisor. We are going to need the following result.

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

**Proposition 2.3** (Divison Algorithm)
Let $n, k \in \mathbb{N}$. Then we can write $n = qk + r$, where $q, r \in \mathbb{Z}$, where $0 \leq r < k$.

*Proof.* Fill this in. □

We will now present the *euclidean algorithm*, which will show the existance and give an efficient way to calculate the greatest common divisor.

**Theorem 2.4** (The Euclidean Algorithm)
Let $a, b \in \mathbb{N}$, and write $a = qb + r$ using the division algorithm. Then $\gcd(a, b) = \gcd(b, r)$.

*Proof.* Fill this in □

Repeatedly applying this, we get the greatest common divisor, as you will see in the following example.

**Example 2.5** (Using the Eucldiean Algorithm)
Let's say we wanted to find $\gcd(a, b)$. Then we can do the following.

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_{n+1} r_n + 0, \end{aligned}$$

then $r_n$ is $\gcd(a, b)$.

there are some details here that need to be fleshed out.]

We can run Euclids algorithm in reverse, writing the $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

**Theorem 2.6**
For all $a, b \in \mathbb{N}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

*Proof.* Run Euclidean algorithm on $a, b$, then move up the chain of steps and you can rewrite as a sum in terms of $a$ and $b$. □

*Alternate Proof.* Let $h$ be the least positive linear combination of $a$ and $b$. Then $h = \gcd(a, b)$. □

This has a nice application in solving some integer linear combination.

**Corollary 2.7** (Bezout's Lemma)
Let $a, b \in \mathbb{N}$. Then the equation $ax + by = c$ has an integer solution if and only if $\gcd(a, b) \mid c$

Now we can prove Euclid's Lemma.

**Theorem 2.8**

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

We can now prove the fundamental theorem of arithmetic.

**Theorem 2.9** (Fundamental Theorem of Arithmetic)

State theorem here.