Number Theory

Adam Kelly (ak2316@cam.ac.uk)

October 6, 2022

This article constitutes my notes for the 'Number Theory' course, held in Michaelmas 2020 at Cambridge. These notes are *not a transcription of the lectures*, and differ significantly in quite a few areas. Still, all lectured material should be covered.

Contents

§1 Introduction

Number theory studies the hidden properties of $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ and $\mathbb{Q} = \{m/n \mid m, n \in Z, n \neq 0\}$. It has always been an experimental science. Examining numerical data leads to conjectures, many of which are very old and still are unproven today.

§1.1 Some Examples

Here are some examples of some easy to state but still unsolved problems in number theory.

1. Let $N \geq 1$ be an integer of the form $8n + 5$, $8n + 6$ or $8n + 7$. Then does there exist right angled triangle of area N, all of whose sides have rational length?
2. Let $\pi(x)$ be the number of primes less than or equal to x, and let
$$li(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$$
be the logarithmic integral. Then for all $x \geq 3$, $|\pi(x) - li(x)| \leq \sqrt{x} \log x$.
3. There are infinitely many primes p such that $p + 2$ is also prime.

§2 Divisibility

§2.1 Euclid's Algorithm

We begin by recalling some of the basic tools of number theory.

Theorem 2.1 (Division Algorithm)
Given $a, b \in \mathbb{Z}$ with $b > 0$, there exists $q, r \in \mathbb{Z}$ with $a = bq + r$ and $0 \leq r < b$.

Proof. A natural candidate for r would be the minimal non-negative element of $S = \{a - nb \mid n \in \mathbb{Z}\}$, which exists since this set contains *some* non-negative element. Indeed this works since $r < b$ as otherwise $r - b \in S$ would contradict minimality. So $a - bq = r$ for some $q \in \mathbb{Z}$, or $a = bq + r$ as required. □

Definition 2.2 (Divides)
We say that a **divides** b, written $a \mid b$, if there exists $q \in \mathbb{Z}$ such that $b = aq$.

Now given a bunch of integers $a_1, \dots, a_n \in \mathbb{Z}$, we can form the set $I = \{\lambda_1 a_1 + \dots + \lambda n a_n \mid \lambda_i \in \mathbb{Z}\}$, and this is closed under linear combinations of elements.

Lemma 2.3
$I = d\mathbb{Z} = \{md \mid m \in \mathbb{Z}\}$ for some $d > 0$.

Proof. Let d be the minimal non-negative element of I. Then $d\mathbb{Z} \subset I$. Also for $a \in I$, we can write $a = qd + r$ for some $0 \leq r < d$. But then $a - qd \in I$ so $r \in I$ and since d is minimal, we must have $r = 0$ and thus $a = qd$, and $a \in d\mathbb{Z}$, so $I = d\mathbb{Z}$. □

In particular, $d \mid a_i$ for all i, and if $c \mid a_i$ for all i then $d\mathbb{Z} = I \subset c\mathbb{Z}$ and $c \mid d$.

Definition 2.4 (Greatest Common Divisor)
We write $d = \gcd(a_1, \dots, a_n) = (a_1, \dots, a_n)$, and say d is the **greatest common divisor** of $a_1, \dots, a_n$.

The construction of this set I along with our definition of greatest common divisor gives us a nice way to handle linear equations involving integers.

Corollary 2.5 (Bézout's Lemma)
Suppose $a, b, c \in \mathbb{Z}$ with a and b ot both 0. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $(a, b) \mid c$.

The process of actually finding suitable x, y occurs through the use of Euclid's algorithm.

Theorem 2.6 (Euclid's Algorithm)
Suppose we had $a, b \in \mathbb{Z}_+$ with $a > b$. Then letting $b = r_0$, we can apply the division

algorithm repeatedly to get

$$\begin{aligned} a &= q_1 r_0 + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

where $0 < r_i < r_{i-1}$ for $i \leq k$. Then $r_k = (a, b)$.

Proof. Note that $r_k \mid r_0$ and $r_k \mid a$ so $r_k \mid (a, b)$. Also if there's m such that $m \mid a$ and $m \mid b$, then $m \mid r_k$, hence $(a, b) \mid r_k$, and $r_k = (a, b)$. □

If $d = (a, b)$, then by Bézout's lemma there exists $r, s \in \mathbb{Z}$ such that $ra + sb = d$. Euclid's algorithm may be used not just to compute d but also to find r and s such that this holds (by substituting backwards).

§2.2 Primes and the Fundamental Theorem of Arithmetic

The reader will be familiar with the notion of primality.

Definition 2.7 (Prime)

An integer $n > 1$ is **prime** if its only positive divisors are 1 and n. Otherwise it's **composite**.

It's well known that there is infinitely many primes, and a standard proof is that of Euclid.

Theorem 2.8 (Euclid)

There are infinitely many primes.

Proof. Suppose the set of primes was finite, say $\{p_1, \ldots, p_k\}$. Then the number $N = p_1 \cdots p_k + 1$ is not divisible by any number in this set, which would imply that it's prime, but it's not in the set of primes, so we have a contradiction. □

A useful result when working with primes is *Euclid's lemma.*

Lemma 2.9 (Euclid's Lemma)

Let p be a prime and $a, b \in \mathbb{Z}$. Then $p \mid ab$ if and only if $p \mid a$ or $p \mid b$.

Proof. The forward direction is a matter of definitions. For the converse, suppose $p \mid ab$ and $p \nmid a$. Then $(a, p) \neq p$, but $(a, b) \mid p$, so $(a, b) = 1$. Then by Bézout's lemma we can write $ax + py = 1$ for some x, y. Then multiplying by b, we get $abx + pby = b$, and since p divides the left side, $p \mid b$ as required. □

It turns out that this gives us unique factorisation.

Theorem 2.10 (Fundamental Theorem of Arithmetic)

Every $n > 1$ can be written as a product of primes, and this product is unique up to reordering.

Proof. Existence follows by strong induction. For uniqueness, suppose there is an integer n with two distinct prime factorisations, $n = p_1 \cdots p_r = q_1 \cdots q_s$. Then $p_1 \mid q_i$ for some i, and by primality we have $p_1 = q_i$, and we can cancel both factors from our equation. Repeating this for n/p_1 and so on, we eventually must have that $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$, as required. □

We can use prime factorisations to write down the gcd of two numbers, in that if $n = \prod p_i^{a_i}$ and $m = \prod p_i^{b_i}$, then $(n, m) = \prod p_i^{\min\{a_i, b_i\}}$. This isn't really an efficient way to compute the gcd, but it's a good way to think about it.

§3 Congruences

§3.1 Modular Arithmetic

It is a common occurrence in number theory that we will consider numbers that differ by a common multiple of a fixed number to be equivalent. This is the idea of congruences (and modular arithmetic).

Definition 3.1 (Congruence)

Let $n \geq 1$ be an integer. We say that a is **congruent** to b **modulo** n, written $a \equiv b \pmod{n}$ if $n \mid a - b$.

This definition naturally induces an equivalence relation on $\mathbb{Z}$, and we write $\mathbb{Z}/n\mathbb{Z}$ for the set of equivalence classes $a + n\mathbb{Z}$. It is easy to check that addition and multiplication are well defined on $\mathbb{Z}/n\mathbb{Z}$, giving rise to modular arithmetic.

§3.2 Modular Inverses

A frequently used tool in modular arithmetic is that of multiplicative inverses (which more or less allow us to perform some kind of division).

Definition 3.2 (Modular Inverse)

Let $a \in \mathbb{Z}/n\mathbb{Z}$. We say that b is a **modular inverse** of a if $ab \equiv 1 \pmod{n}$. If such an inverse exists, it is denoted a^{-1}.

We have a straightforward method for knowing if a number has a modular inverse or not, which is quite natural.

Lemma 3.3 (Existence of Modular Inverses)

Let $a \in \mathbb{Z}$, then the following are equivalent:

(i) $(a, n) = 1$

(ii) There exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$.

(iii) $a + n\mathbb{Z}$ is a generator of $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proof. (i) implies (ii). As $(a, n) = 1$, there exists $b, c \in \mathbb{Z}$ such that $ab + cn = 1$. Taking this modulo n gives us our result. For the other direction, we have $ab = 1 + cn$ for some c, which implies $(a, n) = 1$ by Bezout. □