Part II – Number Theory

Based on lectures by Prof. A. Scholl

Notes taken by Bhavik Mehta

Michaelmas 2017

0 Introduction

Number theory is concerned with the (non-obvious, sometimes mysterious) properties of the integers, $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ and the rationals, $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$. It has been around for thousands of years, and has always been an experimental science where one can conduct experiments with numbers to spot their properties. Experimental data leads to conjectures which can turn out to be very hard to prove, for instance:

1. Congruent number problem: Let $N \geq 1$ be an integer of the form $8n + 5$, $8n + 6$ or $8n + 7$. Does there exist a right-angled triangle with sides of rational length, and area equal to N?

2. Twin prime conjecture: Does there exist infinitely many primes p such that $p + 2$ is also prime? Very recently, we know there are infinitely many primes p such that $\{p + 2, p + 4, \dots, p + 246\}$ contains a prime.

3. $\pi(x)$ refers to the prime counting function, the number of prime numbers $p \leq x$. The prime number theorem says that $\pi(x) \sim \mathrm{li}(x) := \int_2^x \frac{dt}{\log t}$. It is not known whether or not $|\pi(x) - \mathrm{li}(x)| \leq \sqrt{x} \log(x)$, which is equivalent to the Riemann hypothesis - a statement about a certain complex analytic function.

Problem 1 follows from the Birch-Swinnerton-Dyer conjecture, related to algebraic geometry. Often these proofs can require sophisticated theorems, well beyond the statement of the problem.

1 Euclid's algorithm and factoring

Definition (Division algorithm)**.** Given $a, b \in \mathbb{Z}$, with $b > 0$, there are $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and $a = bq + r$, that is, we can divide a by b, giving a quotient q and remainder r.

Proof. Let $S = \{a - nb \mid n \in \mathbb{Z}\}$, which contains some non-negative integers. Let r be the least integer in S which is ≥ 0, which exists by the well ordering property of the non-negative integers. Claim $r < b$, since if not then $r - b \in S$, and $r - b \geq 0$, contradicting the choice of r. □

Notation. If $r = 0$ (that is, $a = bq$ for some $q \in \mathbb{Z}$), write $b \mid a$ (read as 'b divides a'), otherwise write $b \nmid a$.

Given $a_1, \dots, a_n \in \mathbb{Z}$ not all zero, let

$$I = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\}$$

We recognise this from GRM as the ideal generated by $\{a_1, \dots, a_n\}$. Note if $a, b \in I$, for any choice $l, m \in \mathbb{Z}$ then $la + mb \in I$.

Lemma 1.1. $I = d\mathbb{Z} = \{\lambda d \mid \lambda \in \mathbb{Z}\}$ for some $d \leq 1$, clearly unique.

Proof. As not all of a_i are 0, I contains some positive integer, let d be the least of them. So, $d \in I$, and hence $d\mathbb{Z} \subset I$. On the other hand, for $a \in I$ the division algorithm gives us $a = qd + r$ with $0 \leq r < d$. But then $r = a - dq \in I$ so by minimality of d we have $r = 0$, and so $a \in d\mathbb{Z}$, giving $I \subset d\mathbb{Z}$ as required. □

Remark. $a_i \in I = d\mathbb{Z}$ so $d \mid a_i$. If in addition, we have that $\forall i,\ e \mid a_i$, then e divides every element of I, so $e \mid d$. Write $d = \gcd(a_1, \dots, a_n) = (a_1, \dots, a_n)$, the greatest common divisor (alternatively the highest common factor).

The study of **Diophantine equations** involves solving equations with integer solutions, and may have more variables than equations. The simplest case is is linear in two variables.

Corollary. Let $a, b, c \in \mathbb{Z}$ with not both a, b equal to 0. Then we can find $x, y \in \mathbb{Z}$ such that $ax + by = c \Leftrightarrow (a, b) \mid c$.

The definition of the greatest common divisor given here is non-constructive, but **Euclid's algorithm** is an efficient way to compute it.

Euclid's algorithm Assume $a > b > 0$. Apply successively the division algorithm:

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

for some k, so $r_k \mid r_{k-1}$ We claim $r_k = (a, b)$. Indeed, $(a, b) = (a - q_1 b, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k$.

Remark. By lemma 1.1, $(a, b) = ra + sb$ for some integers r, s. Euclid's algorithm give such r, s.

Recall that if $n > 1$ then n is **prime** if its only positive divisors are $\{1, \dots, n\}$, otherwise n is **composite**.

Lemma 1.2. Let p be prime, $a, b \in \mathbb{Z}$. Then $p \mid ab \implies p \mid a$ or $p \mid b$.

Proof. Suppose $p \mid ab$, $p \nmid a$. Then $\gcd(a, b) \neq p$, so it must be 1. So $\exists r, s \in \mathbb{Z}$ such that $ar + ps = 1$. Therefore, $b = (ab)r + p(bs)$, and hence $p \mid b$. □

This lets us prove the fundamental theorem of arithmetic.

Theorem (Fundamental theorem of arithmetic)**.** Every integer $n > 1$ can be written as a product of primes, and this repreestnation is *unique* up to ordering.

Proof. Existence is trivial. Uniqueness: suppose $n = p_1 \dots p_r = q_1 \dots q_s$. $p_1 \mid n$, so p_1 divides some q_j. Hence $p_1 = q_j$ and so we can cancel p_1 and q_j from the relation, and repeat the process for $\frac{n}{p_1}$, eventually giving that the $\{p_1, \dots, p_r\}$ are the same as the $\{q_1, \dots, q_s\}$, up to ordering. □