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 $\pi(x) \sim \operatorname{li}(x) := \int_2^x \frac{dt}{\log t}$. It is not known whether or not $|\pi(x) - \operatorname{li}(x)| \leq \sqrt{x} \log(x)$, 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 to give a quotient q and remainder r.

Proof. Let $S = \{\, a - nb \mid n \in \mathbb{Z} \,\}$, which certainly contains some non-negative integers. Let r be the least of them 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 $a_1, \ldots, a_n \in \mathbb{Z}$ 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 $\{a_1, \ldots, a_n\}$. 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 ives 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. □

Definition (Greatest common divisor)**.** $a_i \in I = d\mathbb{Z}$ 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 $d = \gcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$, 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, and can be solved easily.

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 gives such r, s.

Recall that if $n > 1$ then n is **prime** if its only positive divisors are $\{1, \ldots, n\}$, 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 representation is *unique* up to ordering.

Proof. Existence is trivial. Uniqueness: suppose $n = p_1 \ldots p_r = q_1 \ldots q_s$. $p_1 \mid n$, 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 $\{p_1, \ldots, p_r\}$ are the same as the $\{q_1, \ldots, q_s\}$, up to ordering. □

If we know $a = \prod_{i=1}^k p_i^{\alpha_i}$, $b = \prod_{i=1}^k p_i^{\beta_i}$ for $\alpha_i, \beta_i \geq 0$ and p_i are distinct primes, then by uniqueness of prime factorisation,

$$(a, b) = \prod_{i=1}^{k} p_i^{\gamma_i}, \quad \gamma_i = \min(\alpha_i, \beta_i)$$

However if a, b are large, this is an inefficient way to compute GCDs.

Definition. An algorithm with input an integer $N > 0$ is **polynomial time** if $\exists b, c > 0$ for which the algorithm completes after less than $c(\log N)^b$ 'elementary operations'. Examples of elementary operations include adding or multiplying digits in some fixed base.

If there are k integer inputs, we require less than $c(\max_k(\log N_i))^b$ operations.

Example.

- Adding, multiplying integers (usual method)
- Computing GCDs by Euclid's algorithm
- Testing if N is prime (recent discovery, 2002)

Factoring What about factoring N? The obvious method is trial division by integers $\leq \sqrt{N}$. If $N = pq$, then $p, q \sim \sqrt{N}$ this will take $\sqrt{N}$ divisions - asymptotically larger than any power of $\log N$. For instance, if N has 100 digits, and we can do 2^9 divisions every second, this will take around $10^{50}/2^9$ seconds, which is about 6×10^{39} years. However, Euclid's algorithm will compute the GCD of two such numbers in a few milliseconds. However, there are better algorithms for factoring which we will see later, but so far no polynomial-time algorithm is known (important for security of encryption algorithms like RSA). These are practical for numbers with fewer than 200 digits (for a large computer - the record is 232 digits using thousands of computers and several months)

We will study the distribution of primes and the counting function later. For now,

Theorem (Euclid)**.** There are infinitely many primes

Proof. It is enough to show that given N, there is a prime $p > N$. Let q be the largest prime $\leq N$, and set $M = (2 \times 3 \times 5 \times \cdots \times q) + 1$. If p is any prime factor of M, then $p \notin \{ 2, 3, \ldots, q \}$ so $p > N$. □

Remark. This is constructive, in that it gives a way to find a prime greater than any N, but is is not efficient. For instance, if $N = 1000$, M has over 400 digits.

Finding large primes For reasonable size numbers (fewer than 1000 digits), it is reasonable to pick numbers at random and test for primality. For very large primes, there are special (faster) tests for primality of numbers of the form $N = 2^q - 1$, called Mersenne numbers. Using these, it has been shown that that $2^q - 1$ is prime when $q = 74207281$.

2 Congruences

Fix $n \geq 1$ (the modulus). Typically we will use $n > 1$.

Definition. $a \equiv b \pmod{n}$ if $n \mid a - b$, and we say 'a is congruent to b mod n'

This defines an equivalence relation on $\mathbb{Z}$. Write $\mathbb{Z}/n\mathbb{Z}$ for the set of equivalence classes $\{ a + n\mathbb{Z} \}$, where $a + n\mathbb{Z} = b + n\mathbb{Z} \iff a \equiv b \pmod{n}$. It is easy to see that the operations of addition and multiplication in $\{ a + n\mathbb{Z} \}$ are well defined. [In other words, $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring.]

Lemma 2.1. Let $a \in \mathbb{Z}$. The following are equivalent:

i. $(a, n) = 1$

ii. $\exists b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{n}$

iii. (The equivalence class of) a is a generator of the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proof.

i. $\Rightarrow$ ii. If $(a, n) = 1$, $\exists b, c \in \mathbb{Z}$ with $ab + nc = 1$ so $ab \equiv 1 \pmod{n}$

ii. $\Rightarrow$ i. $ab \equiv 1 \pmod{n} \iff ab + kn = 1$, for some $k \in \mathbb{Z} \implies (a, n) = 1$

ii. $\Leftrightarrow$ iii. $ab \equiv 1 \pmod{n}$ for some $b \iff 1$ belongs to the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by $a \iff$ the subgroup generated by a is $\mathbb{Z}/n\mathbb{Z}$

□

Notation. For $n > 1$, we write $(\mathbb{Z}/n\mathbb{Z})^*$ to denote the set of units (invertible elements) of $\mathbb{Z}/n\mathbb{Z}$. By lemma 2.1, this is the set of classes $a + n\mathbb{Z}$ where $(a, n) = 1$. We can then define $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = \# \{ a \in \mathbb{Z} \mid 1 \leq a \leq n, \ (a, n) = 1 \}$, the **Euler ϕ-function**.

Remark. For $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ every non-zero element has an inverse under X $\iff$ n is prime $\iff$ $\phi(n) = n - 1$.

Theorem (Euler-Fermat Theorem)**.** If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof. $(n > 1)$ Apply Lagrange's theorem to the group $G = (\mathbb{Z}/n\mathbb{Z})^*$ which has order $\phi(n)$. Then $a \in \mathbb{Z}$ with $(a, n) = 1$ defines an element of G whose order divides $\phi(n)$. So $a^{\phi(n)} \equiv 1 \pmod{n}$. □

This has an important special case, called Fermat's Little Theorem.

Theorem (Fermat's Little Theorem)**.** If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Proof. Trivial if $p \mid q$. If not, $(a, p) = 1$ so $a^{\phi(p)} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$ □