University of
Cambridge

Mathematics Tripos

Part II

Number Theory

Michaelmas, 2018

Lectures by
A. Scholl

Notes by
Qiangru Kuang

Contents

0 Introduction

Number theory is the study of $\mathbb{Z}$ and $\mathbb{Q}$. It differs from other areas of mathematics of being an experimental science. We list three conjectures:

1. congruent number problem: suppose $N \geq 1$ is an integer. Does there exist a right angle triangle whose sides are rational whose area is N? This is equivalent to find $a, b, c \in \mathbb{Q}$ positive such that $a^2 + b^2 = c^2, ab = 2N$.

   We expect if N is of the form $8n + 5, 8n + 6$ or $8n + 7$ then there exist such a, b, c. It turns out to be equivalen to an unsolved problem about elliptic curves, i.e. Birch-Swinnerton-Dyer conjecutre.

2. twin prime conjecture: do there exist infinitely many primes p such that $p + 2$ is prime? By a result of Chen in the 1950s, there exist infinitely many p such that $p + 2$ is either prime or is the product of two primes. In 2014 it is proven that there exist infinitely many primes p such that $\{p + 2, p + 4, \dots, p + 246\}$ contains at least one prime.

3. let $\pi(x) = \#\{\text{primes } p \leq x\}$, the prime counting function. Define $\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$ which grow asymptotically as $\frac{x}{\log x}$. Then prime number theory asserts that $\frac{\pi(x)}{\mathrm{li}(x)} \to 1$ as $x \to \infty$. The question: is it true that $|\pi(x) - \mathrm{li}(x)| \leq \sqrt{x} \log x$? It turns out it would follow from Riemann Hypothesis.

Number theory is related to algebra, geometry and many other aspects of mathematics. However in this course, we will focus on elementary number theory. But that doesn't mean we won't be able to prove results with great importance or implication. In fact, by the end of the course, we will be able to prove Tchebychev's theorem: there exist $c_1 > c_2 > 0$ such that

$$c_2 \frac{2}{\log x} < \pi(x) < c_1 \frac{x}{\log x}$$

for all $x > 2$, which is an approximation to the prime number theorem.

1 Euclid's algorithm and factoring

Proposition 1.1 (division algorithm)**.** *Given $a, b \in \mathbb{Z}, b > 0$, then there exist $q, r \in \mathbb{Z}$ with $a = bq + r$ and $0 \leq r < b$.*

Proof. Let $S = \{a - nb : n \in \mathbb{Z}\}$. Then S contains some nonnegative integers. Let r be the least element of S, which is nonnegative. Then claim $r < b$: if not, $a - (n+1)b = r - b \in S$ and $0 \leq r - b$. So $a = nb + r, 0 \leq r < b$. □

Notation. If $r = 0$, i.e. $a = bq$ for some $q \in \mathbb{Z}$, write $b \mid a$, read as "b is a divisor of a" or "b divides a". Otherwise write $b \nmid a$.

Let $a_1, \dots, a_n \in \mathbb{Z}$, not all zero. Let

$$I = \{\lambda_1 a_1 + \dots + \lambda_n a_n : \lambda_i \in \mathbb{Z}\}.$$

Note that I is an ideal of $\mathbb{Z}$.

Lemma 1.2. *There exists a unique $d \in \mathbb{Z}, d > 0$ such that $I = \{md : m \in \mathbb{Z}\} = d\mathbb{Z}$.*

Proof. Uniqueness is obvious. For existence, let d be the least positive element of I. Then $d\mathbb{Z} \subseteq I$. If $a \in I$, write $a = dq + r, 0 \leq r < d$. Then $r = a - dq \in I$ so by minimality of d, $r = 0$, i.e. $a = dq \in d\mathbb{Z}$. □

Remark. $a_i \in I$ so for all a_i, $d \mid a_i$. On the other hand, if $e \mid a_i$ for all i then e divides $d = \lambda_1 a_1 + \dots \lambda_n a_n$ for some λ_i's.

Notation (greatest commmon divisor)**.** Write $d = (a_1, \dots, a_n) = \gcd(a_1, \dots, a_n)$, the *greatest common divisor* of $\{a_i\}$, justified by the previous remark.

Corollary 1.3. *Let $a, b, c \in \mathbb{Z}$, a, b not both 0. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $(a, b) \mid c$. Especially, $(a, b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

This "algorithm" is not very constructive since to find the GCD, we have to write down infinitely many numbers. So how to compute $\gcd(a, b)$? Assume $a > b > 0$. Write

$$a = q_1 b + r_1, 0 \leq r_1 < b.$$

If $r_1 = 0$ then stop, and $\gcd(a, b) = b$. Otherwise write

$$b = q_2 r_1 + r_2, 0 \leq r_2 < r_1.$$

If $r_2 = 0$ then stop. Iterate by

$$\begin{aligned} r_1 &= q_3 r_2 + r_3, 0 \leq r_3 < r_2, \\ &\vdots \\ r_{k-1} &= q_k r_{k-1} + r_k, r_k \neq 0 \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

It has to terminate as $r_1 > r_2 > \dots \geq 0$. Claim that $(a, b) = r_k$: indeed $r_1 = a - q_1 b$ so $(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{k-1}, r_k) = r_k$.

This is know as *Euclid's algorithm*, which, besides being constructive, is very efficient.

Remark. We know $(a, b) = d = ra + sb$ for some $r, s \in \mathbb{Z}$. Euclid's algorithm also can find r and s. (table of extended Euclid's algorithm)

$'$[prime, composite] Recall $n > 1$ is (a) *prime* if its only positive divisors are 1 and n. Otherwise say that n is *composite*.

> **Lemma 1.4.** *Let p be prime and $a, b \in \mathbb{Z}$ with $p \mid ab$. Then either $p \mid a$ or $p \mid b$.*

Proof. Suppose $p \nmid a$, Then $(p, a) \mid p$ so $(p, a) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Then $b = (ab)x + p(by)$ is divisible by p. □

> **Theorem 1.5** (Fundamental Theorem of Arithmetic)**.** *Every integer larger than* 1 *can be written as a product of primes. The expression is unique up to order.*

Proof. Existence is easy by induction on n. For uniqueness, suppose

$$n = p_1 \dots p_r = q_1 \dots q_s$$

where p_i's and q_i's prime. Then $p_1 \mid q_1 \dots q_s$ so by the above lemma $p_1 = q_i$ for some i. Reorder and assume $p_1 = q_1$ so

$$\frac{n}{p1} = p_2 \dots p_r = q_2 \dots q_s.$$

Proceed by induction. □

Remark. If

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, b = \prod_{i=1}^{k} p_i^{\beta_i}$$

where p_i's are distinct primes, then clearly

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

where $\gamma(i) = \min(\alpha_i, \beta_i)$. However, this is *not* an efficient way to calculate GCDs — Euclid's algorithm is much better.

> **Definition.** An algorithm with input an integer $N > 0$ is *polynomial-time* if it completes after $\leq c(\log N)^b$ "elementary operations" (for example, add or multiply digits in some fixed base) for some constants $b, c > 0$ (independent of N).

Example. Addition and multiplication (in the usual way) and computing GCDs using Euclid's algorithm are obviously polynomial time. It is perhaps slighly surprising that primality testing is also polynomial time.

On the other hand, factoring N, by naïve way to test divisibility by numbers up to $\sqrt{N}$, takes $\sqrt{N}$ time. Later in the course, we will discuss better factoring algorithms (but *not* polynomial-time), practial for N up to 200 decimal digits. Is there a polynomial-time algorithm for factoring? It is an unsolved problem and is generally believed to be no.

Theorem 1.6 (Euclid)**.** *There are infinitely many primes.*

Proof. IA Numbers and Sets. □

2 Congruences

Diophantine equaitions, i.e. polynomial equations in $\mathbb{Z}$ whose solutions are also in $\mathbb{Z}$, such as $x^n + y^n = z^n$, are often difficult to solve. If $f(x, y, \dots) = 0$ then for every n, $f(x, y, \dots) = 0 \pmod{n}$ so it is useful to study the congruence first.

Fix integer $n \geq 1$ (the *modulus*, and usually $n > 1$), recall that given $a, b \in \mathbb{Z}$, $a = b \pmod{n}$ ("a is congruent to $b \mod n$") if $n \mid a - b$. This defines an equivalence on $\mathbb{Z}$. The equivalence classes are the sets $a + n\mathbb{Z}$ (taking, say, $a = 0, \dots, n - 1$). Write $\mathbb{Z}/n\mathbb{Z}$ for the set of equivalence classes. Then addition and multiplication are well-defined.

Lemma 2.1. *Let $a \in \mathbb{Z}$. Then TFAE:*

1. $(a, n) = 1$,
2. *there exists $x \in \mathbb{Z}$ such that $ax = 1 \pmod{n}$,*
3. *(the equivalence class of) a is a generator of the group $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Proof.

- $1 \iff 2$: $(a, n) = 1$ if and only if there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$, if and only if $ax = 1 \pmod{n}$.
- $2 \iff 3$: $ax = 1 \pmod{n}$ if and only if in the group $(\mathbb{Z}/n\mathbb{Z}, +)$, 1 is a multiple of a, if and only if a is a generator of the group.

□

Notation. For $n > 1$, $(\mathbb{Z}/n\mathbb{Z})^* =$ set of elements of $\mathbb{Z}/n\mathbb{Z}$ with an inverse under multiplication, i.e. *units* of $\mathbb{Z}/n\mathbb{Z}$.

By the lemma above,

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a + n\mathbb{Z} : (a, n) = 1\}$$

and define

Definition (Euler's φ-function)**.**

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = \#\{a \in \mathbb{Z} : 1 \leq a \leq n : (a, n) = 1\}$$

where $\#S$ is the number of elements of S.

We put $\varphi(1) = 1$.

Theorem 2.2 (Fermat-Euler)**.** *If $(a, n) = 1$ then $a^{\varphi(n)} = 1 \pmod{n}$. Especially when $n = p$ a prime, for all $a \in \mathbb{Z}$, $a^p = a \pmod{p}$.*

Proof. $\varphi(n) = \#G$ where $G = ((\mathbb{Z}/n\mathbb{Z})^*, \times)$. By Lagrange's theorem, the order of a in G divides $\varphi(n)$. □

Index