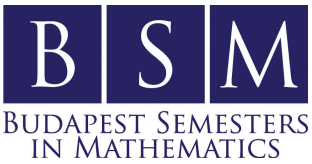

Introduction to number theory
by Péter Maga

Contents

Preface

These lecture notes are written to provide a text to my Introduction to Number Theory course at Budapest Semesters in Mathematics.

Chapter 1
The structure of integers

1.1 Introduction

We do not aim to build up arithmetic from axioms: we suppose that the set $\mathbf{N}$ of positive integers, the set $\mathbf{Z}$ of integers, the set $\mathbf{Q}$ of rationals, the set $\mathbf{R}$ of reals and the set $\mathbf{C}$ of complex numbers exist and the basic operations (addition, subtraction, multiplication, division and raising a positive number to powers) are performed as usual. Also, ordering of integers, rationals, reals and the absolute value of such numbers will be frequently used.

Definition 1.1.1 (divisibility)**.** Given integers a, b, we say $b \mid a$, if there exists an integer c such that $a = bc$.

Proposition 1.1.2. *If $a \mid b, d$, then for any integer c, $a \mid bc + d$.*

Proof. By definition, for some $u, v \in \mathbf{Z}$,

$$b = au, \qquad d = av.$$

Then

$$bc + d = auc + av = a(uc + v),$$

so the number $uc + v \in \mathbf{Z}$ multiplies a into $bc + d$. □

Definition 1.1.3 (units)**.** If $a \mid b$ for all $b \in \mathbf{Z}$, we say that a is a unit.

Proposition 1.1.4. *In $\mathbf{Z}$, the only two units are ± 1.*

Proof. Since for any $a \in \mathbf{Z}$, $a = 1 \cdot a = (-1) \cdot (-a)$, and $\pm a \in \mathbf{Z}$, ± 1 are indeed units. On the other hand, using $|xy| = |x||y|$ for any integers x, y, if a nonzero number $a \in \mathbf{Z}$ of absolute value at least 2 is multiplied by 0, it will give 0; while if it is multiplied by a nonzero integer, its absolute value will be at least 2 again, therefore it cannot be multiplied into ± 1. The number 0 is also not a unit, since its only multiple is 0. □

1.2 The fundamental theorem of arithmetic

In this section, we state and prove the fundamental theorem of arithmetic: the fact that any nonzero integer can be written – essentially uniquely – as the product of prime (irreducible) numbers. The heart of the matter is in fact that primes and irreducibles coincide among rational integers.

Proposition 1.2.1 (euclidean division)**.** *Given integers a, b, $b \neq 0$. Then there exist integers c, d satisfying $a = bc + d$ and $|d| < |b|$.*

Proof. Let $a \geqslant 0$, $b > 0$, the remaining cases are similar. Induct on a. For $a = 1$, the statement is trivial ($c = 1, d = 0$ if $b = 1$ and $c = 0, d = 1$ if $b > 1$). Now assume that the statement holds for any $0 \leqslant a' < a$. If $a < b$, then $c = 0, d = a$. If $a \geqslant b$, then $a - b = bc' + d'$ with $|d'| < |b|$ by induction, so $a = b(c' + 1) + d'$. □

Proposition 1.2.2. *Assume $a, b \in \mathbf{Z}$. Then there exists an integer $\gcd(a, b)$ satisfying $\gcd(a, b) \mid a, b$ and also that whenever $d \mid a, b$, $d \mid \gcd(a, b)$.*

Proof. If $b = 0$, then $\gcd(a, b) = a$ does the job. Otherwise, consider the sequence $(a, b, d_1, \ldots, d_n, 0)$, where each d_i is defined via the euclidean division $d_{i-2} = c_{i-1}d_{i-1} + d_i$ (with $d_{-1} = a, d_0 = b, d_{n+1} = 0$). It is clear that such a sequence of euclidean divisions terminates, since the absolute value decreases in each step. Set $\gcd(a, b) = d_n$. It is clear that $d_n \mid d_{n+1}, d_n$, and then by induction, $d_n \mid d_i, d_{i-1}$ implies $d_n \mid d_{i-2}$. Also, if $d \mid d_{i-2}, d_{i-1}$ (which holds for $i = 1$), then $d \mid d_i$, yielding $d \mid d_n = \gcd(a, b)$. □

Observe that $\gcd(a, b)$ is well-defined only up to sign.

Definition 1.2.3 (greatest common divisor)**.** The greatest common divisor of $a, b \in \mathbf{Z}$ is the nonnegative number which satisfies the conditions imposed on $\gcd(a, b)$ in Proposition 1.2.2.

Definition 1.2.4 (euclidean algorithm)**.** The sequence of euclidean divisions in the proof of Proposition 1.2.2 is called the euclidean algorithm.

Proposition 1.2.5. *Assume $a, b \in \mathbf{Z}$. Then $\gcd(a, b) = au + bv$ for some $u, v \in \mathbf{Z}$.*

Proof. If $b = 0$, the statement is trivial. Otherwise, we can create the same sequence $(a, b, d_1, \ldots, d_n, 0)$ as in the proof of Proposition 1.2.2. Clearly $d_{-1} = a, d_0 = b$ are integer combinations of a and b. Also, if d_{i-2}, d_{i-1} are integer combinations, then so is d_i. □

Definition 1.2.6 (prime numbers)**.** A nonzero integer p is said to be prime, if $p \nmid 1$, and whenever $p \mid ab$, $p \mid a$ or $p \mid b$.

Definition 1.2.7 (irreducible numbers)**.** A nonzero integer p is said to be irreducible, if $p \nmid 1$, and whenever $p = ab$, $a \mid 1$ or $b \mid 1$.

Proposition 1.2.8. *An integer p is prime if and only if it is irreducible.*

Proof. Assume p is prime, and let $p = ab$. Then $a, b \neq 0$. If $a \nmid 1$ and $b \nmid 1$, then $1 < |a|, |b| < p$. Therefore $p \nmid a, b$, which is a contradiction.

Assume p is irreducible, and $p \mid ab$. If $p \mid a$, we are done. If $p \nmid a$, then $\gcd(a, p) = 1$, since p is irreducible. Then there exist integers u, v satisfying $au + pv = 1$. Multiplying by b, we obtain $abu + pbv = b$, the left-hand side is divisible by p, so is the right-hand side. □

Theorem 1.2.9 (fundamental theorem of arithmetic)**.** *Every nonzero integer can be written as a product of prime (irreducible) numbers. The decomposition is unique, apart from factors dividing* 1*.*

Proof. First we prove the existence by induction on $|n|$. For $|n| = 1$, it is trivial. Assume that the statement holds for any n' with $|n'| < |n|$. If n is irreducible, we are done. If not, we can write it as a product $n = ab$ with $|a|, |b| < |n|$. We are done by induction.

Now we prove the uniqueness. Assume n has two decompositions $p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$. Here, p_1 divides the left-hand side, so it divides the right-hand side as well. Then, since it is a prime, it divides a factor of the right-hand side, say, q_1. Then $p_1 \mid q_1$, and also $q_1 \mid p_1$, since q_1 is irreducible. Dividing by them, we can complete the proof by induction. □

Definition 1.2.10 (canonical form)**.** If $n \in \mathbf{Z}$ satisfies

$$n = \pm p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}, \tag{1.2.1}$$

where $p_1, \ldots, p_r$ are distinct prime numbers and $\alpha_1, \ldots, \alpha_r \in \mathbf{N}$, then (1.2.1) is said to be its canonical form. By the fundamental theorem of arithmetic (Theorem 1.2.9), it is unique (apart from signs and the order of the prime powers).

Proposition 1.2.11. *A prime number p divides a number n if and only if it appears in its canonical form (1.2.1) of n.*

Proof. Obviously, if a prime p appears in the canonical form of n, it divides n. For the converse, we use the prime property: if p divides a product, then it divides at least one of the factors. Doing this successively, we obtain that p must equal one of the p_j's in (1.2.1). □

Occasionally, we consider an extended version of the canonical form, namely, we allow 0 exponents.

Proposition 1.2.12. *Let $n = \prod_{j=1}^{r} p_j^{\alpha_j}$ and $d = \prod_{j=1}^{r} p_j^{\beta_j}$ be extended canonical forms (i.e. the primes p_j are distinct, but some of the α_j's and β_j's can be zero). Then $d \mid n$ if and only if $\beta_j \leqslant \alpha_j$ for all $1 \leqslant j \leqslant r$.*

Proof. First assume $\beta_j \leqslant \alpha_j$ for all $1 \leqslant j \leqslant r$. Then simply

$$\frac{n}{d} = \prod_{j=1}^{r} p_j^{\alpha_j - \beta_j},$$

which is clearly an integer (as it is the product of certain integers).

For the converse, assume $m = n/d$ is an integer. Then

$$m = \frac{n}{d} = \prod_{j=1}^{r} p_j^{\alpha_j - \beta_j}.$$

Denote by I the set of indices $1 \leqslant i \leqslant r$ satisfying $\alpha_i < \beta_i$, or equivalently, $\alpha_i - \beta_i < 0$. Then multiplying by $p_i^{\beta_i - \alpha_i}$ for all $i \in I$, we obtain

$$m \prod_{i \in I} p_i^{\beta_i - \alpha_i} = \prod_{\substack{1 \leqslant j \leqslant r \\ j \notin I}} p_j^{\alpha_j - \beta_j}.$$

Here, for any $i \in I$, the left-hand side is divisible by p_i, while the right-hand side is not (by Proposition 1.2.11), therefore, $I = \emptyset$. □

Corollary 1.2.13. *If $a = \prod_{j=1}^{r} p_j^{\alpha_j}$, $b = \prod_{j=1}^{r} p_j^{\beta_j}$ are extended canonical forms (i.e. the primes p_j are distinct, but some of the α_j's and β_j's can be zero), then their greatest common divisor is*

$$\prod_{j=1}^{r} p_j^{\min(\alpha_j, \beta_j)}.$$

Proof. Apply Proposition 1.2.12 to all common divisors of a and b. □

Definition 1.2.14 (least common multiple)**.** If $a, b \in \mathbf{Z}$, then $\operatorname{lcm}(a, b)$ stands for the number satisfying the following properties: it is a multiple of both a and b, and whenever M is a multiplie of both a and b, then $\operatorname{lcm}(a, b) \mid M$. Again, it is clear that it is defined only up to sign, so by the least common multiple of a and b, we mean the nonnegative one.

Corollary 1.2.15. *The least common multiple exists, and when a, b are nonzero, then writing $a = \prod_{j=1}^{r} p_j^{\alpha_j}$, $b = \prod_{j=1}^{r} p_j^{\beta_j}$ for their extended canonical form, its value is*

$$\prod_{j=1}^{r} p_j^{\max(\alpha_j, \beta_j)}.$$

Proof. Apply Proposition 1.2.12 to all common multiples of a and b. □

Corollary 1.2.16. *If $a, b \in \mathbf{N}$, then*

$$a \cdot b = D \cdot m,$$

where D, m stand for the greatest common divisor and the least common multiple of a and b, respectively.

Proof. This follows obviously from the identity $\alpha_j + \beta_j = \min(\alpha_j, \beta_j) + \max(\alpha_j, \beta_j)$. □

Definition 1.2.17 (coprime integers)**.** Two integers a, b are said to be coprime, if $\gcd(a, b) = 1$.

Definition 1.2.18 (square-free numbers)**.** A nonzero integer is said to be square-free, if all the exponents in its canonical form (1.2.1) are 1.

Problem 1.2.1. Prove that $n \in \mathbf{N}$ is a kth power if and only if all the exponents in its canonical form (1.2.1) are divisible by k. (*Hint:* first assume that $n = \prod_{j=1}^{r} p_j^{\alpha_j}$ is a kth power. Consider the canonical form of $\sqrt[k]{n} = \prod_{j=1}^{r} p_j^{\beta_j}$. Show that $\alpha_j = k\beta_j$, so it must be divisible by k. Conversely, assume that $n = \prod_{j=1}^{r} p_j^{\alpha_j}$ with each α_j being divisible by k, say, $\alpha_j = k\beta_j$. Consider the number $\prod_{j=1}^{r} p_j^{\beta_j}$, and show its kth power is n.)

Problem 1.2.2. Prove that each nonzero rational number a can be written in canonical form:

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r},$$

where $p_1, \ldots, p_r$ are distinct prime numbers and $\alpha_1, \ldots, \alpha_r$ are nonzero integers. Prove this form is essentially unique (apart from signs and the order of prime powers). (*Hint:* write $a = b/c$, where b and c are coprime integers. Apply the fundamental theorem of arithmetic (Theorem 1.2.9) to b and c.)

Problem 1.2.3. Assume $n \geqslant 2$ is an integer, and $a \in \mathbf{N}$ is not the nth power of an integer. Prove that $\sqrt[n]{a}$ is irrational. (*Hint:* prove by contradiction as follows. Assume $\sqrt[n]{a} = p/q$ for some coprime integers $p, q \in \mathbf{N}$ (note that we can assume that both of them are positive). Raise this equation to the nth power, and multiply it by q^n. By picking a prime in the canonical form (1.2.1) of a which has exponent not divisible by n (use the statement of another problem in the problem section of Section 1.2 to see such a prime exists), show this contradicts the fundamental theorem of arithmetic (Theorem 1.2.9).)

Problem 1.2.4. Assume $a, b \geqslant 2$ are integers such that their canonical form contains the same prime numbers (possibly on different powers). Prove that there exists $n \in \mathbf{N}$ satisfying $a \mid b^n$ and $b \mid a^n$. (*Hint:* let $a = \prod_{j=1}^{r} p_j^{\alpha_j}$ and $b = \prod_{j=1}^{r} p_j^{\beta_j}$ are the canonical forms (1.2.1) with the same prime set (use the condition on a and b). Show then that $n = \max(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r)$ does the job.)

Problem 1.2.5.* Assume $\alpha \in \mathbf{N}$. Prove that there exist an integer $n \geqslant 2$ and a prime $p \geqslant 2$ such that

$$\sqrt[n]{p^\alpha n}$$

is an integer. Prove also that there are only finitely many such pair n, p.

1.3 Linear diophantine equations

By diophantine equations, we mean equations to be solved over the integers. In this section, we are going to consider the linear equation

$$ax + by = c, \tag{1.3.1}$$

where $a, b, c \in \mathbf{Z}$, and x, y are the indeterminates. To exclude trivialities, we assume from now on that none of a, b is zero.

Proposition 1.3.1. *The equation (1.3.1) has solutions if and only if* $\gcd(a, b) \mid c$. *When there are solutions, they can be described as follows. Set* x_0, y_0 *for any solution. Then the set of solutions is*

$$\left\{(x, y) = \left(x_0 + t \cdot \frac{b}{\gcd(a, b)}, y_0 - t \cdot \frac{a}{\gcd(a, b)}\right) : t \in \mathbf{Z}\right\}.$$

Proof. Since ax, by are both divisible by $\gcd(a, b)$ for any x, y, so is their sum, therefore if $c \nmid \gcd(a, b)$, there is no solution.

Now assume $c \mid \gcd(a, b)$. By Proposition 1.2.5, for well-chosen $u, v \in \mathbf{Z}$,

$$au + bv = \gcd(a, b).$$

Then multiplying by $c/\gcd(a, b)$, and setting $x = uc/\gcd(a, b)$, $y = vc/\gcd(a, b)$,

$$ax + by = c.$$

Obviously, if (x_0, y_0) is any solution, then for any $t \in \mathbf{Z}$,

$$a\left(x_0 + t \cdot \frac{b}{\gcd(a,b)}\right) + b\left(y_0 - t \cdot \frac{a}{\gcd(a,b)}\right) = ax_0 + by_0 = c,$$

so we are left with proving that there are no other solutions.

Assume (x_1, y_1) is a solution. Now let

$$t = (x_1 - x_0)\gcd(a,b)b^{-1} = (y_0 - y_1)\gcd(a,b)a^{-1},$$

showing that $t \in \mathbf{Q}$. Write $t = m/n$ in its simplest form, i.e. $\gcd(m,n) = 1$. By contradiction, assume $n > 1$, and let then p be a prime divisor of n. Clearly p does not divide both of $a/\gcd(a,b)$ and $b/\gcd(a,b)$, assume $p \nmid a/\gcd(a,b)$ (in the other case, the contradiction follows verbatim). Then consider

$$n(y_0 - y_1) = ma/\gcd(a,b).$$

Here, the left-hand side is divisible by p, the right is not, a contradiction. □

Problem 1.3.1. We have a 7-liter and a 11-liter jug. How can we weigh out 1 liter of tap water? (*Hint:* apply the euclidean division and write it in practical terms.)

Problem 1.3.2. In Nekeresdország (this is a country in Hungarian fairy tales) 7-headed and 12-headed dragons live (these are species in the fauna of Hungarian fairy tales). Altogether, there are 1000 heads of dragons. How many dragons of the two species live in Nekeresdország? Give all possibilities. (*Hint:* apply Proposition 1.3.1.)

1.4 Residue classes

Definition 1.4.1 (congruence)**.** Given $m \in \mathbf{Z}$, we say that $a \equiv b \bmod m$ (in words: a is congruent to b modulo m) if $m \mid (a - b)$.

Proposition 1.4.2 (remainders)**.** *Given $m \in \mathbf{Z} \setminus \{0\}$ and $a \in \mathbf{Z}$, there exist $0 \leqslant b < |m|$ and $-|m|/2 < c \leqslant |m|/2$ satisfying $a \equiv b \equiv c \bmod m$.* □

Proposition 1.4.3. *Given $m \in \mathbf{Z}$. Being congruent modulo m is an equivalence relation, by which we mean that $a \equiv a \bmod m$ (reflexivity), $a \equiv b \bmod m$ implies $b \equiv a \bmod m$ (symmetry), $a \equiv b \bmod m$ and $b \equiv c \bmod m$ imply $a \equiv c \bmod m$ (transitivity).* □

Definition 1.4.4 (residue classes)**.** Let $m \in \mathbf{Z}$. Then the equivalence classes defined via modulo m congruency are said to be modulo m residue classes.

Proposition 1.4.5. *Let $m \in \mathbf{Z} \setminus \{0\}$. The number of residue classes modulo m is $|m|$.* □

Proposition 1.4.6. *Let $m \in \mathbf{Z} \setminus \{0\}$. The modulo m residue classes form a commutative ring, where addition, multiplication and taking additive inverse are the usual addition, multiplication and taking additive inverse, all reduced modulo m. The residue class of 1 is the multiplicative unit.*

Proof. Let a, b be arbitrary representatives of two residue classes. Then for any $k, l \in \mathbf{Z}$, we have

$$\begin{aligned}
(a + km) + (b + lm) &= (a + b) + (k + l)m \equiv a + b \bmod m,\\
(a + km) \cdot (b + lm) &= ab + (kb + la)m + klm^2 \equiv ab \bmod m,\\
-(a + km) &= -a - km \equiv -a \bmod m,
\end{aligned}$$

showing that the operations can be performed via any representatives. Then obviously the residue class of 1 is a multiplicative unit. □

Theorem 1.4.7 (Chinese remainder theorem)**.** *Assume $m, n \in \mathbf{N}$ satisfy $\gcd(m,n) = 1$. Then for any $a, b \in \mathbf{Z}$, there exists a unique residue class c modulo mn satisfying $c \equiv a \bmod m$, $c \equiv b \bmod n$.*

Proof. Define the function $f : x \bmod mn \mapsto (x \bmod m, x \bmod n)$. There are mn residue classes modulo mn, and the number of possible values of this function is also mn. It suffices to prove that f is a bijection, which holds if and only if it is a surjection.

To see this, take $u, v \in \mathbf{Z}$ satisfying $mu + nv = 1$. Then take the number $c = mub + nva$. Then

$$c \equiv nva \equiv mua + nva \equiv a \bmod m, \qquad c \equiv mub \equiv mub + nvb \equiv b \bmod n.$$

The proof is complete. □

Corollary 1.4.8. *Assume $m_1, \ldots, m_n$ satisfy $\gcd(m_i, m_j) = 1$ for all $1 \leqslant i < j \leqslant n$. Then for any $a_1, \ldots, a_n \in \mathbf{Z}$, there exists a unique residue class c modulo $m_1 \cdot \ldots \cdot m_n$ satisfying $c \equiv a_i \bmod m_i$ for each $1 \leqslant i \leqslant n$.* □

Problem 1.4.1. Prove that a square modulo 3 can be only 0 or 1. Prove that a square modulo 4 can only be 0 or 1. (*Hint:* as for modulo 3, square $3m$, $3m + 1$ and $3m + 2$; as for modulo 4, square $2m$ and $2m + 1$.)

Problem 1.4.2. Prove that a cube modulo 7 can be only 0, 1 or 6. (*Hint:* compute the cube of $7m, 7m + 1 \ldots, 7m + 6$.)

Problem 1.4.3. Prove that the sum of twelve consecutive square numbers cannot be a square. (*Hint:* calculate modulo 4: observe that among 12 square numbers, exactly 6 are odd, therefore they are 1 modulo 4, the even ones are divisible by 4. Conclude that the sum of twelve consecutive squares is 2 modulo 4, which cannot happen with a square number. Alternatively, you can calculate modulo 3.)

Problem 1.4.4. Let $a_1, \ldots, a_{10}$ and $b_1, \ldots, b_{10}$ be the numbers $1, \ldots, 10$ in some (not necessarily different) sequences. Prove that $a_1 + b_1, \ldots, a_{10} + b_{10}$ cannot be distinct modulo 10. (*Hint:* let $c_1 = a_1 + b_1, \ldots, c_{10} = a_{10} + b_{10}$. Assume by contradiction that $c_1, \ldots, c_{10}$ are distinct modulo 10. Then prove that $c_1 + \ldots + c_{10} \equiv 5 \bmod 10$, and that $c_1 + \ldots + c_{10} = (a_1 + b_1) + \ldots + (a_{10} + b_{10}) \equiv 0 \bmod 10$. Conclude the contradiction.)

Problem 1.4.5.* Let $n \in \mathbf{N}$ be fixed. Prove that given n integers, we can choose a few of them such that their sum is divisible by n.

1.5 Number-theoretic functions

A function defined on the positive integers is said to be a number-theoretic function. In what follows, we always assume that the functions take complex values. First we introduce some of the most important number-theoretic functions. The summations in the definitions always run through positive numbers. The first class is about the divisors.

Definition 1.5.1 (power sum of divisors)**.** Define

$$\tau_s(n) = \sum_{d|n} d^s.$$

Two important special cases are $s = 0$ (the number of divisors) and $s = 1$ (the sum of divisors). The second class is about the number of prime and prime power divisors.

Definition 1.5.2. Define

$$\omega(n) = \sum_{\substack{p|n \\ p \text{ prime}}} 1, \qquad \Omega(n) = \sum_{\substack{p^k|n \\ p \text{ prime},\ k \in \mathbf{N}}} 1.$$

Two further examples are of extreme importance in number theory.

Definition 1.5.3 (Euler's number of coprime residue classes function)**.** Define

$$\varphi(n) = \sum_{\substack{d \leqslant n \\ \gcd(d,n)=1}} 1.$$

Definition 1.5.4 (Möbius function)**.** Define

$$\mu(n) = \begin{cases} 0, & \text{if } n \text{ is not square-free,} \\ (-1)^{\omega(n)}, & \text{otherwise.} \end{cases}$$

Definition 1.5.5 (multiplicative functions)**.** A number-theoretic function f is said to be multiplicative, if for $\gcd(m,n)=1$, $f(mn)=f(m)f(n)$. Furthermore, it is totally multiplicative, if $f(mn)=f(m)f(n)$ for all $m,n \in \mathbf{N}$.

Definition 1.5.6 (additive functions)**.** A number-theoretic function f is said to be additive, if for $\gcd(m,n)=1$, $f(mn)=f(m)+f(n)$. Furthermore, it is totally additive, if $f(mn)=f(m)+f(n)$ for all $m,n \in \mathbf{N}$.

Example 1.5.7. The function ω is additive. The function Ω is totally additive. □

Example 1.5.8. The function μ is multiplicative. □

Proposition 1.5.9. *Assume $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. Then*

$$\varphi(n) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

Proof. Assume n has prime factors $p_1, \ldots, p_r$. From the set $\{1, \ldots, n\}$, sift out the numbers that are divisble by some of $p_1, \ldots, p_r$. That is, by the inclusion-exclusion principle,

$$\varphi(n) = n + \sum_{j=1}^{r} (-1)^j \sum_{1 \leqslant i_1 < \ldots < i_j \leqslant r} \frac{n}{p_{i_1} \cdot \ldots \cdot p_{i_j}} = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

The proof is complete. □

Corollary 1.5.10. *The function φ is multiplicative.* □

Definition 1.5.11 (convolution)**.** Given two number-theoretic functions f, g, their convolution is defined as

$$(f * g)(n) = \sum_{d|n} f(d) g(n/d).$$

Proposition 1.5.12. *Number-theoretic functions with respect to convolution and pointwise addition form a ring. The ring is commutative with unit element*

$$\delta_1(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$$

If $f(1) \neq 0$, then there exists g satisfying $f * g = \delta_1$.

Proof. The ring-properties are all straight-forward calculations except for the associativity of convolution. This goes as follows:

$$((f*g)*h)(n) = \sum_{d|n} (f*g)(d) h(n/d) = \sum_{d'|d} \sum_{d|n} f(d') g(d/d') h(n/d) = \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3),$$

and the same calculation shows that this equals $(f * (g * h))(n)$.

An easy calculation shows that δ_1 is indeed a unit-element. Assume $f(1) \neq 0$, then its inverse g can be defined recursively. Let $g(1) = f(1)^{-1}$, and whenever g is defined for each $k < n$, set

$$g(n) = -\left(\sum_{1 \neq d | n} f(d) g(n/d) \right) f(1)^{-1}.$$

Obviously $f * g = \delta_1$. □

Proposition 1.5.13. *The convolution of multiplicative functions is multiplicative.*

Proof. Assume f and g are multiplicative, and m, n are coprime integers. Then

$$(f * g)(mn) = \sum_{d|mn} f(d)g(mn/d).$$

Here, each $d \mid mn$ can be uniquely written as a product $d = d_m d_n$ with $d_m \mid m$ and $d_n \mid n$, since m and n are coprime. So the above equals

$$\sum_{\substack{d_m|m \\ d_n|n}} f(d_m d_n)g(mn/d_m d_n) = \sum_{d_m|m} f(d_m)g(m/d_m) \sum_{d_n|n} f(d_n)g(d_n/n) = (f * g)(m)(f * g)(n).$$

The proof is complete. □

Introduce the function

$$\mathrm{id}^s(n) = n^s.$$

Obviously id^s is (totally) multiplicative for each $s \in \mathbf{C}$. Two important examples are id^0 (the constant 1) and id^1 (the identity).

Corollary 1.5.14. *The function τ_s is multiplicative for each $s \in \mathbf{C}$.*

Proof. We have $\tau_s = \mathrm{id}^s * \mathrm{id}^0$. □

Proposition 1.5.15. *We have $\mu * \mathrm{id}^0 = \delta_1$. In other words,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Since $\mu, \mathrm{id}^0, \delta_1$ are all multiplicative, it suffices to prove $(\mu * \mathrm{id}^0)(p^k) = 0$ for primes p and $k \in \mathbf{N}$ and $(\mu * \mathrm{id}^0)(1) = 1$. The latter is obvious, the former is a straight-forward calculation. □

Proposition 1.5.16. *We have $\mu * \mathrm{id}^1 = \varphi$.*

Proof. Since $\mu, \mathrm{id}^1, \varphi$ are all multiplicative, it suffices to prove $(\mu * \mathrm{id}^1)(p^k) = \varphi(p^k)$ for primes p and $k \in \mathbf{N}$ and $(\mu * \mathrm{id}^1)(1) = \varphi(1)$. The latter is obvious, the former is a straight-forward calculation. □

Corollary 1.5.17. *We have $\varphi * \mathrm{id}^0 = \mathrm{id}^1$. In other words,*

$$\sum_{d|n} \varphi(d) = n$$

for each integer n.

Proof. Since δ_1 is the unit element in the ring of convolutions,

$$\mathrm{id}^1 = \delta_1 * \mathrm{id}^1 = \mu * \mathrm{id}^0 * \mathrm{id}^1 = \mathrm{id}^0 * \mu * \mathrm{id}^1 = \mathrm{id}^0 * \varphi.$$

The proof is complete. □

Problem 1.5.1. For a number given in canonical form (1.2.1) $n = \prod_{j=1}^r p_j^{\alpha_j}$, compute $\omega(n)$, $\Omega(n)$, $\tau_0(n)$. (*Hint:* compute them for prime powers and apply additivity, multiplicativity).

Problem 1.5.2. Prove that for any $n \in \mathbf{N}$, $\tau_0(n) \leqslant 2\sqrt{n}$. (*Hint:* use the fact that divisors of n come in pairs (if $a \mid n$, then its divisor pair is n/a), and that in each pair, the smaller number is at most $\sqrt{n}$.)

Problem 1.5.3. Prove that for any $\varepsilon > 0$, $\tau_0(n) \ll_\varepsilon n^\varepsilon$ for $n \in \mathbf{N}$. (*Hint:* prove first the statement for prime powers, then use multiplicativity.)

Problem 1.5.4. Which integers n satisfy the equation $\tau_0(n) + \varphi(n) = \tau_1(n)$? (*Hint:* show that a number $2 \leqslant j \leqslant n$ cannot be simultaneously coprime to n and a divisor of n. Conclude that $\tau_0(n) + \varphi(n) \leqslant n + 1$. Observe that for $n \geqslant 2$, n certainly has at least two divisors: n and 1, implying $\tau_1(n) \geqslant n + 1$ for $n \geqslant 2$. When do we have equality?)

Problem 1.5.5.* Prove that for any $\varepsilon > 0$, $\varphi(n) \gg_\varepsilon n^{1-\varepsilon}$ for $n \in \mathbf{N}$.

1.6 Multiplicative groups

Given $m \in \mathbf{N}$, we denote by $\mathbf{Z}_m$ the set of residue classes modulo m. This is a ring with respect to modulo m addition and multiplication. Assume $\gcd(a, m) = 1$.

Proposition 1.6.1. *The function $x \mapsto xa : \mathbf{Z}_m \to \mathbf{Z}_m$ is a bijection.*

Proof. Since $\mathbf{Z}_m$ is finite, it suffices to show that the function is surjective. By $\gcd(a, m) = 1$ and Proposition 1.2.5, for some $u, v \in \mathbf{Z}$, $au + mv = 1$. Now for any $b \in \mathbf{Z}_m$, setting $x \equiv ub \bmod m$, we see that

$$aub + mvb \equiv b \bmod m,$$

and the proof is complete. □

Corollary 1.6.2. *The coprime residue classes form a group. (This is the unit group of $\mathbf{Z}_m$ and will be denoted by $\mathbf{Z}_m^\times$ from now on.)* □

Corollary 1.6.3. *If p is a prime, the residue classes modulo p form a field (denoted by $\mathbf{F}_p$ from now on).* □

Now we prove a basic theorem of group theory.

Theorem 1.6.4 (Lagrange)**.** *Assume G is a finite group and H is a subgroup of G. Then $|H| \mid |G|$.*

Proof. Introduce the following relation on the pair of elements of G: $x \sim y$, if for some $h \in H$, $xh = y$. This is an equivalence relation: $1 \in H$ implies $x \sim x$; if $xh \sim y$ for some $h \in H$, then $yh^{-1} = x$ and $h^{-1} \in H$; if $x \sim y \sim z$, then for some $h_1, h_2 \in H$, $xh_1 = y$, $yh_2 = z$, then $x(h_1h_2) = z$ and $h_1h_2 \in H$, yielding $x \sim z$. Then G is partitioned into equivalence classes, and we claim that each equivalence class has the same number of elements as H (this clearly implies the statement). Take any equivalence class C, let x be a representative of it. Then take the function $f(h) = xh$ for $h \in H$, obviously $f(H) \subseteq C$. Also, for any $y \in C$, there is h satisfying $xh = y$, then $f(h) = y$, thus $f(H) = C$. Then f surjects H onto C, it suffices to see that it also injects H into C. Assume that for h, h', $f(h) = f(h')$. Then $xh = xh'$, so multiplying by x^{-1} on the left, $h = h'$. □

Definition 1.6.5. The (multiplicative) order of an element $a \in \mathbf{Z}_m^\times$ is the least positive number k such that $a^k \equiv 1 \bmod m$. In other words, the order of a is the order of the subgroup generated by a.

Proposition 1.6.6. *Given $a \in \mathbf{Z}_m^\times$, let its order be k. Then $a^l \equiv 1 \bmod m$ if and only if l is a multiple of k.*

Proof. If $l = nk$, then

$$a^l \equiv a^{nk} \equiv (a^k)^n \equiv 1^n \equiv 1 \bmod m.$$

Conversely, assume $a^l \equiv 1 \bmod m$. By the definition of the order, $l \geqslant k$. By Proposition 1.4.2, for some $0 \leqslant l' < k$ and some integer $n \in \mathbf{N}$, $l - nk = l'$. Then

$$a^{l'} \equiv a^l a^{-nk} \equiv 1 \cdot 1 \equiv 1 \bmod m,$$

and by the minimality of k, we have then $l' = 0$, which implies $l = nk$. □

Then Lagrange's theorem (Theorem 1.6.4) has the following consequences.

Corollary 1.6.7. *Assume $m \in \mathbf{N}$ and a is coprime to m. Then the order of a (modulo m) divides $\varphi(m)$.* □

Corollary 1.6.8 (Euler-Fermat)**.** *Assume $m \in \mathbf{N}$. Then*

$$a^{\varphi(m)} \equiv 1 \bmod m$$

for any a coprime to m. □

Corollary 1.6.9 (Fermat). *Assume p is a prime. Then*

$$a^p \equiv a \bmod p$$

for any $a \in \mathbf{Z}$. □

The aim of this section is to describe the group $\mathbf{Z}_m^\times$. Assume $m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. By the Chinese remainder theorem (Corollary 1.4.8),

$$\mathbf{Z}_m^\times \cong \mathbf{Z}_{p_1^{\alpha_1}}^\times \times \ldots \times \mathbf{Z}_{p_r^{\alpha_r}}^\times,$$

so we are left to describe the multiplicative group $\mathbf{Z}_{p^\alpha}^\times$, which has $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ elements.

Proposition 1.6.10. *If p is a prime, $\mathbf{Z}_p^\times$ is cyclic.*

Proof. For $n \in \mathbf{N}$, introduce the nth cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{\omega \in \mathbf{C} \\ \omega \text{ is a primitive } n\text{th root of unity}}} (x - \omega).$$

A priori, this is a polynomial in $\mathbf{C}[x]$. It is easy to see that $x^n - 1$ is divisible by $\prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ in $\mathbf{C}[x]$, and that

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}.$$

Since the leading coefficient of $x^n - 1$ is 1, induction shows that each $\Phi_n(x)$ is of integer coefficients and leading coefficient 1. Recalling $\sum_{d|n} \varphi(d) = n$, it also follows by induction that $\deg \Phi_n = \varphi(n)$.

From this point on, we work in $\mathbf{F}_p$ (the above argument shows that cyclotomic polynomials make sense in $\mathbf{F}_p$). By the Euler-Fermat theorem (Corollary 1.6.8), each $a \in \mathbf{Z}_p^\times$ is a root of the polynomial $x^{p-1} - 1$, therefore, each $a \in \mathbf{Z}_p^\times$ is a root of some cyclotomic polynomial Φ_d (with $d \mid (p-1)$). Since each Φ_d (with $d \mid (p-1)$) has at most $\deg \Phi_d = \varphi(d)$ roots, and altogether they have $p - 1$, each of them must have $\varphi(d)$ roots, and there is no common root of any two of them. Then take a root a of Φ_{p-1}. Assume by contradiction that it has order $d < p - 1$. Then $a^d - 1 \equiv 0 \bmod p$, so a is a root of some $\Phi_{d'}$ with $d' \leqslant d$, which is a contradiction. □

Proposition 1.6.11. *If $\alpha \leqslant 2$, the group $\mathbf{Z}_{2^\alpha}^\times$ is cyclic. If $\alpha \geqslant 3$, the group $\mathbf{Z}_{2^\alpha}^\times$ is generated by the order 2 element -1 and the order $2^{\alpha-2}$ element 5.*

Proof. The case $\alpha \leqslant 2$ is obvious. Let $\alpha \geqslant 3$.

We claim $\mathbf{Z}_{2^\alpha}^\times$ is not cyclic. For $\alpha = 3$, this is clear, since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$. If $\alpha > 3$, assume by contradiction that $g \in \mathbf{Z}_{2^\alpha}^\times$ generates $\mathbf{Z}_{2^\alpha}^\times$. Then g (reduced modulo 8) generates $\mathbf{Z}_8^\times$, a contradiction.

Now we prove that the order of 5 is $2^{\alpha-2}$. Since $|\mathbf{Z}_{2^\alpha}^\times| = 2^{\alpha-1}$, the order of 5 is a 2-power, and it is less than $2^{\alpha-1}$, since $\mathbf{Z}_{2^\alpha}^\times$ is not cyclic. So it suffices to prove that $5^{2^{\alpha-3}} \not\equiv 1 \bmod 2^\alpha$. We claim that for each $k \geqslant 0$,

$$5^{2^k} = l_k 2^{k+2} + 1$$

with some odd number l_k. By induction, for $k = 0$, $l_k = 1$ does the job; and if it holds for k, then

$$5^{2^{k+1}} = (5^{2^k})^2 = l_k^2 2^{2(k+2)} + l_k 2^{k+3} + 1 = (l_k^2 2^{k+1} + l_k) 2^{k+3} + 1,$$

and $l_k^2 2^{k+1} + l_k$ is odd, since l_k is odd. Now applying this with $k = \alpha - 3$, we obtain $5^{2^{\alpha-3}} = \text{odd} \cdot 2^{\alpha-1} + 1$, which is clearly not 1 modulo 2^α.

We are left to prove that -1 is not a power of 5 modulo 2^α, which is clear from the fact that $5 \equiv 1 \bmod 4$, thus any power of 5 is 1 modulo 4 but -1 is not. □

Proposition 1.6.12. *If $p > 2$, the group $\mathbf{Z}_{p^\alpha}^\times$ is cyclic.*

Proof. Assume a is coprime to p, and that $k \geqslant 0$ is an integer. Then we claim

$$(a+p)^{(p-1)p^k} = a^{(p-1)p^k} + \text{term divisible by } p^{k+1}, \text{ not by } p^{k+2}.$$

We prove by induction. For $k = 0$,

$$(a+p)^{p-1} = a^{p-1} + \text{term divisible by } p, \text{ not by } p^2,$$

since in the binomial expansion, the single term not divisible by p is a^{p-1}, and the single term divisible by p, and not by p^2 is $\binom{p-1}{1}a^{p-2}p$. If the statement holds for k, then for $k+1$,

$$(a+p)^{(p-1)p^{k+1}} = \left((a+p)^{(p-1)p^k}\right)^p = \left(a^{(p-1)p^k} + \text{term divisible by } p^{k+1}, \text{ not by } p^{k+2}\right)^p.$$

In the binomial expansion, only those terms are not divisible by p^{k+3}, which contain 'term divisible by p^{k+1}, not by p^{k+2}' on at most power 1: if the power is at least 3, then the number of factors p is at least $3k+3 \geqslant k+3$; if the power is 2, then by $p > 2$, the binomial coefficient $\binom{p}{2}$ contributes one more p, then $2k+3 \geqslant k+3$. Now the statement is obvious: the modulo p part is $a^{(p-1)p^{k+1}}$, and apart from this, the binomial coefficient $\binom{p}{1}$ contributes one (and only one) more factor p to the term containing 'term divisible by p^{k+1}, not by p^{k+2}' on power 1.

Now we prove that $\mathbf{Z}_{p^\alpha}^\times$ is cyclic for $p > 2$. We proceed by induction on α. For $\alpha = 1$, we have already proved the statement. If it is true for $\alpha \geqslant 1$, then take a, a generator of $\mathbf{Z}_{p^\alpha}^\times$. If a is a generator of $\mathbf{Z}_{p^{\alpha+1}}^\times$, then we are done. If not, consider $b = a + p$. The order of b divides $(p-1)p^\alpha$, but by Fermat's theorem (Corollary 1.6.9), it cannot be a power of p (noting that $a, b \not\equiv 1 \bmod p$, since otherwise, each power of a would be 1 modulo p, but a is a generator of $\mathbf{Z}_{p^\alpha}^\times$), so it must be of the form $(p-1)p^k$ with some $0 \leqslant k \leqslant \alpha$. Therefore, it is enough to show that $b^{(p-1)p^{\alpha-1}} \not\equiv 1 \bmod p^{\alpha+1}$. Using that $a^{(p-1)p^{\alpha-1}} \equiv 1 \bmod p^{\alpha+1}$ (by our assumption, a does not generate the whole group, so its order must be a proper divisor of $(p-1)p^\alpha$, and it also cannot be a power of p), the above claim with $k = \alpha - 1$ completes the proof. □

Whenever $\mathbf{Z}_m^\times$ is cyclic, any generator of $\mathbf{Z}_m^\times$ is called a primitive root modulo m.

Problem 1.6.1. Let p be an odd prime and $\alpha \in \mathbf{N}$. Prove that if the odd integer a is a primitive root modulo p^α, then a is a primitive root modulo $2p^\alpha$ as well. (*Hint:* compute the order of a modulo p^α, further $\varphi(p^\alpha)$ and $\varphi(p^{2\alpha})$).

Problem 1.6.2. For which $m \in \mathbf{N}$ does $m \mid (ab-1)$ imply $m \mid (a-b)$? (*Hint:* observe that the condition $m \mid (ab-1)$ means that the group $\mathbf{Z}_m^\times$ is an elementary 2-group (the square of each element is 2). Use the structure theorems about $\mathbf{Z}_m^\times$.)

Problem 1.6.3. Determine the prime numbers p which satisfy $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$. (*Hint:* consider first the cases $p = 2, 3$. For $p > 3$, multiply $2^{p-2} + 3^{p-2} + 6^{p-2} - 1$ by 6 (which is coprime to p), and use Euler-Fermat (Corollary 1.6.8).)

Problem 1.6.4. Prove Wilson's theorem: for any prime number p, $(p-1)! \equiv -1 \bmod p$. (*Hint:* couple the numbers $1, \ldots, p-1$ as follows: let the pair of a number be its multiplicative inverse modulo p. Prove that only 1 and $p-1$ do not have a multiplicative inverse different from themselves. Then $(p-1)! \equiv 1 \cdot (p-1) \cdot$ 'pairs' mod p, and in each pair, the product is 1 modulo p.)

Problem 1.6.5.* Prove that for any $m \in \mathbf{N}$, the sequence $2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots$ modulo m is constant from a certain point on.

1.7 The law of quadratic reciprocity

Definition 1.7.1 (Legendre symbol)**.** Let p be a prime, and assume $a \in \mathbf{Z}$. Then define the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if } p \nmid a \text{ and } a \text{ is a square modulo } p, \\ -1, & \text{if } p \nmid a \text{ and } a \text{ is not a square modulo } p. \end{cases}$$

When $\left(\frac{a}{p}\right) = 1$, a is said to be a quadratic residue modulo p, while if $\left(\frac{a}{p}\right) = -1$, a is said to be a quadratic non-residue modulo p. Note that when $p \mid a$, then a is neither a quadratic residue, nor a quadratic non-residue modulo p.

Proposition 1.7.2. *Assume $p > 2$ is a prime and $a \in \mathbf{Z}$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof. The statement is clear for $\left(\frac{a}{p}\right) = 0$. If $\left(\frac{a}{p}\right) = 1$, then for some b modulo p,

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$$

by Euler-Fermat (Corollary 1.6.8). Also, for any $a \in \mathbf{Z}_p^\times$,

$$a^{\frac{p-1}{2}} \in \{\pm 1\} \bmod p.$$

Indeed, set c for the left-hand side. Then $c^2 \equiv 1 \bmod p$ by Euler-Fermat (Corollary 1.6.8), hence $c \in \{\pm 1\}$.

Now observe that the polynomial $x^{\frac{p-1}{2}} - 1$ has at most $(p-1)/2$ roots modulo p, which means that it suffices to prove that the number of the quadratic residues is $(p-1)/2$. Assume a is a quadratic residue, say, it is the square of b modulo p. Then the equation $x^2 - a \equiv 0 \bmod p$ has exactly two solutions: b and $-b$ (they cannot coincide since p is odd). This means that $x \mapsto x^2$ from $\mathbf{Z}_p^\times$ to quadratic residues is a two-folded cover, yielding that the latter set has cardinality $(p-1)/2$. □

Corollary 1.7.3. *We have*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

for any residue classes a, b modulo p. □

Proposition 1.7.4. *Assume p is an odd prime and a is an integer satisfying $\gcd(a,p) = 1$. Consider the modulo p residue classes $a, 2a, \ldots, \frac{p-1}{2}a$. Assume that exactly v of them is congruent to a number bigger than $p/2$ but less than p modulo p. Then*

$$\left(\frac{a}{p}\right) = (-1)^v.$$

Also, if a is odd, then

$$v \equiv \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \ldots + \left\lfloor \frac{\frac{p-1}{2}a}{p} \right\rfloor \bmod 2.$$

Proof. For each $1 \leqslant j \leqslant (p-1)/2$, set $1 \leqslant b_j \leqslant (p-1)/2$ satisfying either $ja \equiv b_j \bmod p$ or $ja \equiv p - b_j \bmod p$. We claim that if $i \neq j$, then $b_i \neq b_j$. This is clear if ia and ja are both either in the interval $[1, (p-1/2)]$ or in $[(p+1)/2, p-1]$ modulo p. Otherwise, let, say $ia \equiv b_i \bmod p$, $ja \equiv p - b_j \bmod p$. Then if $b_i \equiv b_j \bmod p$, this implies $i + j \equiv 0 \bmod p$ which is clearly excluded by $1 \leqslant i, j \leqslant (p-1)/2$. Then the b_j's run through the interval $[1, (p-1)/2]$. Therefore

$$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a \equiv \prod_j (b_j \text{ or } p - b_j) \equiv \left(\frac{p-1}{2}\right)! (-1)^v \bmod p,$$

and using that a is invertible modulo p, the first claim is proved.

As for the second claim, observe that its right hand-side can be written as

$$\frac{a - (b_1 \text{ or } p - b_1)}{p} + \frac{2a - (b_2 \text{ or } p - b_2)}{p} + \ldots + \frac{\frac{p-1}{2}a - (b_{(p-1)/2} \text{ or } p - b_{(p-1)/2})}{p},$$

in each term, we write b_j or $p - b_j$ according to that whether ja is in $[1, (p-1)/2]$ or in $[(p+1)/2, p-1]$. Now observe that we are interested in this only modulo 2, so we may change the signs as we wish. Then the above (modulo 2) is

$$\frac{pv}{p} + \frac{a-1}{p} \sum_{j=1}^{(p-1)/2} j \equiv v \bmod 2,$$

using again that the set of b_j's is exactly $\{1, \ldots, (p-1)/2\}$. □

Corollary 1.7.5. *The number* 2 *is a quadratic residue modulo* p *if* $p \equiv \pm 1 \bmod 8$ *and it is a quadratic non-residue if* $p \equiv \pm 3 \bmod 8$. □

Theorem 1.7.6 (quadratic reciprocity)**.** *Assume* p *and* q *are odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof. In the positive quarterplane (i.e. points (x, y) with $x, y > 0$), draw a line l from the origin of slope q/p. Now count the integer points of positive coordinates in the rectangle with vertices $(0, 0)$, $((p-1)/2, 0)$, $((p-1)/2, (q-1)/2)$, $(0, (q-1)/2)$. On the one hand, it is trivially $(p-1)(q-1)/4$. On the other hand, there are

$$\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \ldots + \left\lfloor \frac{\frac{p-1}{2}q}{p} \right\rfloor$$

and

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \ldots + \left\lfloor \frac{\frac{q-1}{2}p}{q} \right\rfloor$$

such integer points below and above l, respectively. Then Proposition 1.7.4 completes the proof. □

Definition 1.7.7 (Jacobi symbol)**.** For any positive integer m, consider its canonical form (1.2.1) $m = \prod_{j=1}^{r} p_j^{\alpha_j}$. Then for $a \in \mathbf{Z}$, set

$$\left(\frac{a}{m}\right) = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{\alpha_j}.$$

Corollary 1.7.8. *We have*

$$\left(\frac{a}{m}\right)\left(\frac{a}{n}\right) = \left(\frac{a}{mn}\right)$$

for any $m, n \in \mathbf{N}$. □

Problem 1.7.1. Assume $p, q \equiv 1 \bmod 4$ are primes. Prove that

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

(*Hint:* Apply Theorem 1.7.6.)

Problem 1.7.2. Assume $p > 2$ is a prime and a, b are quadratic non-residues modulo p. Show ab is a quadratic residue modulo p. (*Hint:* Using Corollary 1.7.3, prove that the product of a quadratic non-residue and a quadratic residue is a quadratic non-residue. Apply that there are as many quadratic residues as non-residues.)

Problem 1.7.3. Prove that if m is the product of at least two distinct prime numbers, then there exists $a \in \mathbf{N}$ coprime to m such that

$$\left(\frac{a}{m}\right) = 1,$$

yet a is not a square modulo m. (*Hint:* Let $m = p_1 \cdot \ldots \cdot p_r$, where p_j's are distinct prime numbers. Take residue classes $a_1 \bmod p_1, \ldots, a_r \bmod p_r$ such that $a_1 \bmod p_1$ and $a_2 \bmod p_2$ are quadratic non-residues, while $a_j \bmod p_j$ are quadratic residues for $3 \leqslant j \leqslant r$. Apply Corollary 1.4.8 to find $a \bmod m$ which satisfies $a \equiv a_j \bmod p_j$ for each $1 \leqslant j \leqslant r$. Prove that a is not a square modulo m by contradiction, and that

$$\left(\frac{a}{m}\right) = 1$$

by Corollary 1.7.8.)

Problem 1.7.4. Let $p > 2$ be a prime. Prove that for any number $a \in \mathbf{N}$ coprime to $2p$,

$$\left(\frac{a}{2p}\right) = 1$$

if and only if a is a square modulo $2p$. (*Hint:* if a is a square modulo $2p$, then show it is a square modulo p as well, so

$$\left(\frac{a}{p}\right) = 1.$$

Prove also

$$\left(\frac{a}{2}\right) = 1$$

for any a coprime to 2. Use Corollary 1.7.8. As for the converse, assume

$$\left(\frac{a}{2p}\right) = 1.$$

Derive then

$$\left(\frac{a}{p}\right) = \left(\frac{a}{2}\right) = 1.$$

So $a \equiv b^2 \equiv (p-b)^2 \bmod p$ for some b. Out of b and $p-b$, choose the odd one, and show its square is a modulo $2p$.)

Problem 1.7.5.* For any prime $p > 2$, denote by $l(p)$ the smallest positive number which is a quadratic non-residue modulo p. Prove that

$$l(p) \leqslant \sqrt{p} + 1.$$

Chapter 2
Various introductory topics

2.1 Prime number theory

Theorem 2.1.1. *There are infinitely many prime numbers.*

Proof. By contradiction, assume that there are finitely many prime numbers, set $\mathcal{P} = \{2, 3, \dots, p\}$ for the finite set of primes. Let $A = \prod_{a\in\mathcal{P}} a + 1$. Then $A \geqslant 2$, so A has a prime divisor q by the fundamental theorem of arithmetic (Theorem 1.2.9). Then q divides both $A - 1$ (as it is listed in $\mathcal{P}$) and A, hence also divides their difference 1, which is a contradiction. □

Theorem 2.1.2. *The reciprocal sum of prime numbers is infinity.*

Proof. Let $2 = p_1 < p_2 < \dots$ be the increasing sequence of primes. By contradiction, assume

$$\sum_{k=1}^{\infty} \frac{1}{p_k} < \infty.$$

Then, for some $N \in \mathbf{N}$,

$$\sum_{k=N+1}^{\infty} \frac{1}{p_k} < 1/3.$$

For any integer $A \in \mathbf{N}$, divide the set $\{1, \dots, A\}$ into disjoint subsets A_1 and A_2, where

$$A_1 = \{1 \leqslant a \leqslant A : a \text{ has a prime divisor bigger than } p_N\},$$
$$A_2 = \{1 \leqslant a \leqslant A : a \text{ has no prime divisor bigger than } p_N\}.$$

First,

$$\#A_1 \leqslant \sum_{k=N+1}^{\infty} \left\lfloor \frac{A}{p_k} \right\rfloor \leqslant A \sum_{k=N+1}^{\infty} \frac{1}{p_k} < A/3.$$

We claim that any positive integer n can be written as the product of a square and a square-free number, as it follows from the canonical form (1.2.1) of n:

$$n = \prod_{j=1}^{r} p_j^{\alpha_j} = \prod_{j=1}^{r} p_j^{2\lfloor \alpha_j/2 \rfloor} \cdot \prod_{j=1}^{r} p_j^{\alpha_j - 2\lfloor \alpha_j/2 \rfloor},$$

and here the first factor is a square and the second one is square-free.

With this fact in our toolbox, write each number $a \in A_2$ as $a = a_1^2 a_2$, where a_2 is square-free. Since $1 \leqslant a_1^2 \leqslant A$, there are at most $\sqrt{A}$ choices for a_1. Also, there are at most 2^N choices for a_2, since

$$a_2 = \prod_{j=1}^{N} p_j^{0 \text{ or } 1}.$$

Altogether,

$$\#A_2 \leqslant \sqrt{A}2^N,$$

which is less than $A/3$, if A is large enough. Altogether, this is a contradiction, since each number between 1 and A must be in either A_1 or A_2. □

The following beautiful (and useful) theorem of Dirichlet states that any arithmetic progression contains infinitely many primes, if there is no obvious obstacle.

Theorem 2.1.3 (Dirichlet)**.** *If q and a are coprime integers, then there are infinitely many prime numbers p satisfying $p \equiv a \bmod q$.*

Proof omitted.

For any number $x \geqslant 2$, denote by $\pi(x)$ the number of primes not exceeding x. Now we are going to prove some estimates on $\pi(x)$ going back to Chebyshev. We will need the following fact about the product of primes up to x.

Proposition 2.1.4. *For any $x \geqslant 2$, we have*

$$\prod_{\substack{p \leqslant x \\ p \text{ prime}}} p < 4^x.$$

Proof. It suffices to prove for $x \geqslant 2$ integers. We prove by induction. The statement is true for $x \leqslant 10$. Now let $x > 10$ and assume the estimate holds for any integer smaller than x. If x is even, then x is not a prime, therefore the product of primes up to x is the same as up to $x-1$, that is,

$$\prod_{\substack{p \leqslant x \\ p \text{ prime}}} p = \prod_{\substack{p \leqslant x-1 \\ p \text{ prime}}} p < 4^{x-1} < 4^x.$$

If x is odd, then set $x = 2m+1$, and then

$$\prod_{\substack{p \leqslant 2m+1 \\ p \text{ prime}}} p = \prod_{\substack{p \leqslant m+1 \\ p \text{ prime}}} p \prod_{\substack{m+2 \leqslant p \leqslant 2m+1 \\ p \text{ prime}}} p < 4^{m+1}\binom{2m+1}{m+1} \leqslant 4^{m+1}2^{2m} = 4^{2m+1},$$

using that

$$\prod_{\substack{m+2 \leqslant p \leqslant 2m+1 \\ p \text{ prime}}} p \mid \binom{2m+1}{m+1},$$

since when simplifying $(2m+1)!/((m+1)!m!)$, primes exceeding $m+1$ do not cancel; and also that $\binom{2m+1}{m+1} \leqslant 2^{2m}$, which follows from $\sum_{j=0}^{2m+1}\binom{2m+1}{j} = 2^{2m+1}$ and $\binom{2m+1}{m} = \binom{2m+1}{m+1}$. □

Theorem 2.1.5 (Chebyshev)**.** *There exist positive constants c_1, c_2 such that for all $x \geqslant 2$,*

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

Proof. First we prove the upper bound. As in the proof of Proposition 2.1.4,

$$\prod_{\substack{n < p \leqslant 2n \\ p \text{ prime}}} p < 4^n.$$

since $\binom{2n}{n}$ is divisible by each prime greater then n not exceeding $2n$. Then, since each prime on the left-hand side is at least n,

$$\#\{\text{primes between } n \text{ and } 2n\} < \log_n(4^n) = \log 4 \cdot \frac{n}{\log n}.$$

Applying this between $x/2$ and x, then between $x/4$ and $x/2$, and so on, until we arrive below $\sqrt{x}$, we have

$$\#\{\text{primes between } \sqrt{x} \text{ and } x\} < \log 4 \cdot \frac{x(1/2+1/4+1/8+\ldots)}{\log \sqrt{x}} + 2 \cdot \frac{\log x}{\log 2},$$

where the last term is to take care of the integer parts at each halving. Estimating the number of primes below $\sqrt{x}$ by $\sqrt{x}$, and noting that if x is large enough, $\sqrt{x} + 2\log x/\log 2 < x/\log x$, we are done.

As for the lower bound, consider the canonical form (1.2.1) of the binomial coefficient

$$\binom{2n}{n} = \prod_{\substack{p \leqslant \sqrt{2n} \\ p \text{ prime}}} p^{\alpha_p} \prod_{\substack{\sqrt{2n} < p \leqslant 2n/3 \\ p \text{ prime}}} p^{\alpha_p} \prod_{\substack{2n/3 < p \leqslant n \\ p \text{ prime}}} p^{\alpha_p} \prod_{\substack{n < p \leqslant 2n \\ p \text{ prime}}} p^{\alpha_p}.$$

For any prime p,

$$\alpha_p = \sum_{j=1}^{\infty} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leqslant \log_p(2n).$$

Therefore, the first factor above satisfies

$$\prod_{\substack{p \leqslant \sqrt{2n} \\ p \text{ prime}}} p^{\alpha_p} \leqslant (2n)^{\sqrt{2n}}.$$

In the second factor, we apply Proposition 2.1.4, and conclude

$$\prod_{\substack{\sqrt{2n} < p \leqslant 2n/3 \\ p \text{ prime}}} p^{\alpha_p} \leqslant 4^{2n/3}.$$

In the third factor, each $\alpha_p = 0$, therefore

$$\prod_{\substack{2n/3 < p \leqslant n \\ p \text{ prime}}} p^{\alpha_p} = 1.$$

Applying $\binom{2n}{n} \geqslant 4^n/(2n+1)$, we obtain

$$\prod_{\substack{n < p \leqslant 2n \\ p \text{ prime}}} p^{\alpha_p} \geqslant 4^{n - \log_4(2n+1) - \sqrt{2n}\log_4(2n) - 2n/3} > 4^{n/4},$$

if n is large enough. Since each prime in the product is at most $2n$,

$$\#\{\text{primes between } n \text{ and } 2n\} > \log 4 \cdot \frac{n/4}{\log(2n)},$$

which clearly implies the statement. □

In fact, we have a much stronger result on the number of primes not exceeding x.

Theorem 2.1.6 (prime number theorem)**.** *We have*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Proof omitted.

Problem 2.1.1. Prove that for any n, there are n consecutive composite (neither prime nor unit) numbers. (*Hint:* assume $n \geqslant 2$, and consider the numbers $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$. Show that all of them are composite.)

Problem 2.1.2. Prove that there are infinitely many prime numbers which are congruent to -1 modulo 4. Note that this is the case $q = 4$, $a = 3$ in Dirichlet's theorem. (*Hint:* imitate the proof of the infinitude

of primes. Observe that there are such prime numbers: $3, 7, 11 \equiv -1 \bmod 4$. Assume that there are finitely many, let their set be $\mathcal{P}$, and consider the number $A = 4\prod_{a\in\mathcal{P}} a - 1$. Show it must be at least 2, so it has at least one prime divisor. On the other hand, observe it is odd, so 2 cannot be among its prime divisors. Also prove that all its prime divisors cannot be simultaneously congruent to 1 modulo 4: to see this, prove that the product of numbers congruent to 1 modulo 4 is still 1 modulo 4; and that $A \equiv -1 \bmod 4$. Conclude that A has a prime divisor congruent to -1 modulo 4 and show it is coprime to all elements of $\mathcal{P}$, therefore cannot be listed in $\mathcal{P}$, a contradiction.)

Problem 2.1.3. Prove that there are infinitely many prime numbers which are congruent to -1 modulo 3. This is another case, namely $q = 3$, $a = 2$ in Dirichlet's theorem. (*Hint:* imitate the proof of the infinitude of primes. Observe that there are such prime numbers: $5, 11, 17 \equiv -1 \bmod 6$. Assume that there are finitely many, let their set be $\mathcal{P}$, and consider the number $A = 3\prod_{a\in\mathcal{P}} a - 1$. Show it must be at least 2, so it has at least one prime divisor. On the other hand, observe that 3 cannot be among its prime divisors. Also prove that all its prime divisors cannot be simultaneously congruent to 1 modulo 3: to see this, prove that the product of numbers congruent to 1 modulo 3 is still 1 modulo 3; and that $A \equiv -1 \bmod 3$. Conclude that A has a prime divisor congruent to -1 modulo 3 and show it is coprime to all elements of $\mathcal{P}$, therefore cannot be listed in $\mathcal{P}$, a contradiction.)

Problem 2.1.4. Prove that there is no (nonconstant) infinite arithmetic progression consisting of prime numbers. (*Hint:* prove by contradiction, assume there is such an arithmetic progession. We may assume the first term $a_0 = p$ and the difference d are both positive. Give another element of the sequence $(a_0 + nd)_{n\in\mathbf{N}}$ which is divisible by p and greater than p, concluding the contradiction.)

Problem 2.1.5.* Prove that

$$\lim_{x\to\infty} \prod_{\substack{p<x \\ p \text{ prime}}} \frac{p}{p-1} = \infty.$$

2.2 Open problems about primes

Definition 2.2.1 (Mersenne primes)**.** A prime number p is said to be a Mersenne prime, if $p = 2^n - 1$ for some $n \in \mathbf{N}$.

Proposition 2.2.2. *If $p = 2^n - 1$ is a Mersenne prime, then the exponent n is a prime number.*

Proof. If $n = ab$ for some $1 < a, b < n$, then

$$2^n - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1),$$

and here, both factors are bigger than 1. □

Open problem 2.2.3. *Are there infinitely many Mersenne primes?*

Definition 2.2.4 (perfect numbers)**.** A number n is said to be a perfect number, it it satisfies $\tau_1(n) = 2n$.

Example 2.2.5. The numbers 6 and 28 are perfect.

Proposition 2.2.6. *An even number n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ for some Mersenne prime $2^p - 1$.*

Proof. Assume first $2^p - 1$ is a Mersenne prime. Then

$$\tau_1(n) = \tau_1(2^{p-1})\tau_1(2^p - 1) = (1 + 2 + \ldots + 2^{p-1})(1 + 2^p - 1) = (2^p - 1)2^p = 2n.$$

As for the converse, write the perfect even number n in the form $n = 2^k t$, where $k \in \mathbf{N}$ and t is an odd number. Then

$$2^{k+1}t = \tau_1(n) = \tau_1(t)(2^{k+1} - 1).$$

Then $2^{k+1} - 1$ divides $2^{k+1}t$, and since it is odd, it divides t. Set then $t' = t/(2^{k+1} - 1)$. Substituting this back, we obtain

$$2^{k+1}t' = \tau_1(t).$$

Here, the left hand-side is $t+t'$, while the right hand-side is at least $t+t'$ (since t, t' are different divisors of t), and they equal if and only if there is no further divisor of t. This can happen only if t is a prime, $t'=1$. Then $t = 2^{k+1}-1$ for $k \in \mathbf{N}$, a Mersenne prime. □

Open problem 2.2.7. *Do odd perfect numbers exist?*

Open problem 2.2.8. *Are there infinitely many perfect numbers?*

Remark 2.2.9. If the answer to Open problem 2.2.7 is negative, then this is equivalent to Open problem 2.2.3.

Definition 2.2.10 (Fermat numbers)**.** For $n \in \mathbf{N} \cup \{0\}$, the nth Fermat number is defined as $2^{2^n}+1$.

The reason of considering only powers of 2 in the exponent is the following.

Proposition 2.2.11. *If m is not a power of 2, then 2^m+1 is not a prime.*

Proof. Assume $1 \leqslant t < m$ is an odd divisor of m. Then

$$2^m+1 = (2^{m/t}+1)(2^{(m/t)(t-1)} - 2^{(m/t)(t-2)} + \ldots - 2^{m/t} + 1),$$

so $2^{m/t}+1$ is a proper divisor of 2^m+1 (it is smaller than 2^m+1 and bigger than 1). □

Proposition 2.2.12. *For different positive integers m, n, the mth and nth Fermat numbers are coprime.*

Proof. Denote by F_k the kth Fermat number. Assuming $m > n$, we have, by induction,

$$F_m = 2 + \prod_{j=0}^{m-1} F_j.$$

Indeed, $F_1 = 5$, $F_0 = 3$, so $F_1 = 2 + F_0$; then for any m, multiplying

$$2^{2^m} - 1 = F_m - 2 = \prod_{j=0}^{m-1} F_j$$

by $F_m = 2^{2^m}+1$,

$$2^{2^{m+1}} - 1 = F_{m+1} - 2 = \prod_{j=0}^{m} F_j,$$

we obtain the induction step.

Therefore any common divisor d of F_m and F_n divides 2. Since all Fermat numbers are odd, d must be ± 1. □

Definition 2.2.13 (Fermat primes)**.** A Fermat prime is a Fermat number which is further a prime.

The most remarkable fact about Fermat primes was proved by Gauss.

Theorem 2.2.14 (Gauss)**.** *For a given $n \in \mathbf{N}$, a regular n-gon is constructible if and only if the canonical form (1.2.1) looks as follows:*

$$n = 2^k \cdot p_1 \cdot \ldots \cdot p_r,$$

where $k \in \mathbf{N} \cup \{0\}$, and $p_1, \ldots, p_r$ are distinct Fermat primes.

Proof omitted.

Open problem 2.2.15. *Are there infinitely many Fermat primes?*

What about primes close to each other?

Open problem 2.2.16. *Are there infinitely many primes p such that $p+2$ is also a prime?*

This topic became extremely hot in 2013, we only mention the two greatest breakthroughs.

Theorem 2.2.17 (Zhang)**.** *If $h > 70000000$, then there exist infinitely many numbers $n \in \mathbf{N}$ such that the interval $[n, n+h]$ contains at least two primes.*

Proof omitted.

Theorem 2.2.18 (Maynard)**.** *For any $k \in \mathbf{N}$, there exists $h(k) \in \mathbf{N}$ such that for infinitely many $n \in \mathbf{N}$, the interval $[n, n+h(k)]$ contains at least k primes.*

Proof omitted.

Another easy-to-ask, hard-to-attack topic is due to Goldbach and Euler.

Open problem 2.2.19 (Goldbach's conjecture)**.** *Every even number bigger than 2 is representable as the sum of two prime numbers.*

A beautiful result, also from 2013, is the solution for three prime numbers.

Theorem 2.2.20 (Helfgott)**.** *Every odd number bigger than 5 is representable as the sum of three prime numbers.*

Proof omitted.

Dirichlet's theorem (Theorem 2.1.3) can be reformulated as follows: if a polynomial $ax + b \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Z}$ (by this we mean that if we write it as the product of two polynomials, one of them is the constant ± 1), then it is a prime for infinitely many $x \in \mathbf{Z}$. For higher-degree polynomials, very little is known.

Open problem 2.2.21. *Is it true that $n^2 + 1$ is a prime for infinitely many $n \in \mathbf{N}$?*

Problem 2.2.1. Prove that there are no infinitely many triplets of primes, i.e. only finitely many primes p satisfy that $p + 2, p + 4$ are also primes. (*Hint:* considering everything modulo 3, prove that one of $p, p + 2, p + 4$ is divisible by 3.)

Problem 2.2.2. Prove that there exists a quadratic polynomial $f \in \mathbf{Z}[x]$ such that f is irreducible over $\mathbf{Z}$ (by this we mean that if we write it as the product of two polynomials, one of them is the constant ± 1) and $f(x)$ is prime only for finitely many $x \in \mathbf{Z}$. (*Hint:* prove that $x^2 + x + c$ is always even, if c is even, and we can choose $2 \mid c$ such that $x^2 + x + c$ is irreducible over $\mathbf{Z}$.)

2.3 Number theory in cryptography

In this section, we describe a real-life application of number theory, namely, the RSA cryptosystem.

Assume Alice wants to send a message to Bob which is unreadable for everyone else. The basic idea – first without any number theory – is the following. Bob chooses a function C which encodes numbers:

$$x \text{ (the original message, a number)} \longmapsto C(x) \text{ (the encoded message, another number).}$$

Bob makes C public, but keeps C^{-1} in secret. Alice can easily encode her message x by applying C to it, and sends only $C(x)$ to Bob. Now Bob, who knows not only C, but also C^{-1}, can easily recover x: takes the encoded message $C(x)$, and applies C^{-1}, getting $C^{-1}(C(x)) = x$.

Is it plausible to have such functions, namely, whose inverse cannot be easily computed? The answer is yes. Assume you have only an English-Hungarian dictionary (C: encode English words in Hungarian), and you want to translate from Hungarian to English (this would be C^{-1}, the decryption procedure): although decryption can be done, it takes much more time than the ecryption. Note that in practice, our aim is not to make an undecryptable encryption: if our encoding can be inverted only in 10 million years even for the fastest computers, it does the job.

And here number theory enters the picture. Given two primes p, q (where p has, say, 500, q has, say, 600 digits in base 10), their product $N = pq$ can be computed essentially in no time (with computers, of course). However, if we give only N, according to the current state of computer science, it is hopeless to get p, q in a reasonable time.

Bob also takes a number e coprime to $\varphi(N)$, and computes its multiplicative inverse f modulo $\varphi(N)$. For him, this is easy to do, since $\varphi(N) = (p-1)(q-1)$, and then the equation

$$ef - \varphi(N)v = 1$$

can be solved fast using the euclidean algorithm (we will return to this in the problem section).

And now we give Bob's cryptosystem.

- **Public part:** N, e. Bob makes this public.
- **Secret part:** $p, q, \varphi(N), f$. Bob keeps this in secret.
- **Encrypting:** Bob publishes the following: "If you want to send me a message $1 \leqslant x \leqslant N-1$, take $x^e \bmod N$, and send it to me."
- **Decrypting:** For an incoming message y, Bob takes $y^f \bmod N$ and says: "Okay, they wanted to send me the message $y^f \bmod N$."

How does this work? It is a simple consequence of Euler-Fermat (Corollary 1.6.8):

$$y^f \equiv (x^e)^f \equiv x^{ef} \equiv x^{\varphi(N)v+1} \equiv (x^{\varphi(N)})^v \cdot x \equiv x \bmod N,$$

so Bob gets x back. Well, at least if the original message x is coprime to N, but this happens with extremely high probability (something like $1 - 10^{-500}$), so the risk is very low.

When we talk about algorithms and their cost in time, a fast algorithm is an algorithm which terminates in polynomial many steps, where polynomial means a polynomial of $\log n$, if n is the input – in other words, a polynomial in the number of digits (no matter in which base). (If the input is more than one number, say, $n_1, \dots, n_k$, polynomial means a polynomial in $\max(\log n_1, \dots, \log n_k)$.)

Problem 2.3.1. Prove that addition, subtraction, multiplication and euclidean division can be computed in polynomial time. (*Hint:* recall how you did these basic operations in elementary school – via the digits.)

Problem 2.3.2. Prove that gcd can be computed in polynomial time. (*Hint:* apply the euclidean algorithm, and show that the remainder can be halved in each euclidean division (Proposition 1.4.2). Prove also that a polynomial of a polynomial is still a polynomial, so euclidean division (which takes polynomial time to do) can be nested as a 'step' in the computation of gcd.)

Problem 2.3.3. Assume $N = pq$, where p, q are primes as in RSA. Prove that if there is an algorithm computing $\varphi(N)$ in polynomial time, then there is an algorithm to compute p, q in polynomial time. (*Hint:* prove that $p + q$ can be computed directly from $N, \varphi(N)$. Use also $pq = N$.)

Problem 2.3.4. Assume $N = pq$, where p, q are primes as in RSA. Prove that if there is an algorithm computing the multiplicative inverse $\bmod \varphi(N)$ of any e coprime to $\varphi(N)$, then there is an algorithm to compute $\varphi(N)$ in polynomial time. (*Hint*: prove that there exists a prime $e \ll (\log N)^k$ for some $k \in \mathbf{N}$ which is coprime to $\varphi(N)$ (use Proposition 2.1.4 and/or Theorem 2.1.5 to see this). Using the algorithm for the multiplicative inverse, find such a prime e. Computing its multiplicative inverse f, show that there are at most $\ll (\log N)^k$ choices for $\varphi(N)$. For each choice, compute p, q and make a reality check.)

Problem 2.3.5.* Given N as in RSA. Prove that if $1 \leqslant x, e \leqslant N-1$, then $x^e \bmod N$ can be computed in polynomial time.

2.4 The mean value of number-theoretic functions

Experience shows that the behaviour of number-theoretic functions is somewhat chaotic. However, when averaged over a large interval, they become more regular. We have already seen an example for this phenomenon: the number of prime numbers up to x is close to $x/\log x$ (Theorem 2.1.5 and Theorem 2.1.6).

Proposition 2.4.1. *For $x \geqslant 2$, $\sum_{n \leqslant x} \tau_0(n) = x \log x + O(x)$.*

Proof. For any d, the number of multiples of d up to x is $\lfloor x/d \rfloor = x/d + O(1)$. We can rewrite the counting on the divisors as a counting on the multiples as follows:

$$\sum_{n\leqslant x} \tau_0(n) = \sum_{n\leqslant x}\sum_{d|n} 1 = \sum_{d\leqslant x}\sum_{n\leqslant x/d} 1 = \sum_{d\leqslant x} \left\lfloor \frac{x}{d} \right\rfloor.$$

Therefore

$$\sum_{n\leqslant x} \tau_0(n) = \sum_{d\leqslant x} \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d\leqslant x} \left(\frac{x}{d} + O(1) \right) = x \sum_{d\leqslant x} \frac{1}{d} + O(x) = x(\log x + O(1)) + O(x) = x\log x + O(x),$$

and the proof is complete. □

In fact, a sharper result can be proved using Dirichlet's hyperbola method.

Proposition 2.4.2. *For $x \geqslant 2$, $\sum_{n\leqslant x} \tau_0(n) = x\log x + (2\gamma - 1)x + o(x)$, where*

$$\gamma = \lim_{T\to\infty} \left(\sum_{n\leqslant T} \frac{1}{n} - \log T \right).$$

Proof. Fixing x, in the positive quarterplane (i.e. points (y, z) with $y, z > 0$), draw the hyperbola

$$H_x = \{(y, z) : y, z > 0, yz = x\}.$$

Obviously, $\sum_{n\leqslant x} \tau_0(n)$ equals the number of integer points in the positive quarterplane below H_x. Now to any integer point (y, z) with $y > \sqrt{x}$, associate the point (z, y). So the number of integer points below H_x equals

$$2\sum_{d\leqslant\sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor - \lfloor\sqrt{x}\rfloor^2,$$

where in the last term, we subtracted the points (y, z) with $y, z \leqslant \sqrt{x}$ (counted twice in the first term). Then the above equals

$$2x(\log\sqrt{x} + \gamma + o(1)) + O(\sqrt{x}) - x + O(\sqrt{x}) = x\log x + (2\gamma - 1)x + o(x),$$

and the proof is complete. □

Proposition 2.4.3. *For any $x \geqslant 2$, $\sum_{n\leqslant x} |\mu(n)| = 6/\pi^2 \cdot x + o(x)$.*

Remark 2.4.4. Note that $|\mu(n)|$ is 1 if and only if n is square-free, otherwise it is zero.

Proof. Introduce the function

$$s(n) = \sum_{d^2|n} \mu(d).$$

One can easily check that

$$s(n) = \begin{cases} 1, & \text{if } n \text{ is square-free,} \\ 0, & \text{otherwise.} \end{cases}$$

Indeed, if n is square-free, the only nonzero term is $\mu(1) = 1$, while if $n = \prod_{j=1}^{r} p_j^{\alpha_j}$ with $\alpha_1 > 1$, then

$$s(n) = \sum_{0\leqslant\beta_1\leqslant\alpha_1/2} \dots \sum_{0\leqslant\beta_r\leqslant\alpha_r/2} \mu(p_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}) = (1 + \mu(p_1)) \sum_{0\leqslant\beta_2\leqslant\alpha_2/2} \mu(p_2^{\beta_2})\cdot\ldots\cdot \sum_{0\leqslant\beta_r\leqslant\alpha_r/2} \mu(p_r^{\beta_r}) = 0.$$

Now

$$\sum_{n\leqslant x} |\mu(n)| = \sum_{n\leqslant x}\sum_{d^2|n} \mu(d) = \sum_{d\leqslant x} \mu(d) \sum_{n:d^2|n} 1 = \sum_{d\leqslant x} \mu(d) \left\lfloor \frac{x}{d^2} \right\rfloor = x \sum_{d\leqslant\sqrt{x}} \frac{\mu(d)}{d^2} + O(\sqrt{x}).$$

Here,

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sum_{n=1}^{\infty} \frac{1}{n^2} = \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{d|m} \mu(d) = 1,$$

since $\sum_{d|m}\mu(d)$ vanishes unless $m=1$ by Proposition 1.5.15. This implies

$$\sum_{d\leqslant\sqrt{x}}\frac{\mu(d)}{d^2}=\left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right)^{-1}+o(1).$$

Using now $\sum_{n=1}^{\infty}n^{-2}=\pi^2/6$,

$$\sum_{n\leqslant x}|\mu(n)|=\left(\frac{6}{\pi^2}+o(1)\right)x+O(\sqrt{x}),$$

and the proof is complete. □

Problem 2.4.1. Prove that there are arbitrarily deep valleys in the sequence $\tau_0(n)$, i.e. for any $N\in\mathbf{N}$, there exists $n\in\mathbf{N}$ such that $\tau_0(n-1)-\tau(n)>N$ and $\tau_0(n+1)-\tau_0(n)>N$. (*Hint:* combine Dirichlet's theorem (Theorem 2.1.3) with the Chinese remainder theorem (Corollary 1.4.8) as follows. Let $P=p^{N+2}$ and $Q=q^{N+2}$ for different prime numbers p,q. Show there exists a residue class a mod PQ such that $a\equiv 1 \bmod P$, $a\equiv -1 \bmod Q$ and $\gcd(a,PQ)=1$. Prove that a prime number $n\equiv a \bmod PQ$ satisfies $\tau_0(n-1)-\tau(n)>N$ and $\tau_0(n+1)-\tau_0(n)>N$, and show that such a prime number n exists.)

Problem 2.4.2. Prove that there are arbitrarily high mountains in the sequence $\tau_0(n)$, i.e. for any $N\in\mathbf{N}$, there exists $n\in\mathbf{N}$ such that $\tau_0(n)-\tau_0(n-1)>N$ and $\tau_0(n)-\tau_0(n+1)>N$. (*Hint:* for some $x\geqslant 10$, set A for the product of primes up to x. Show that both $A-1$ and $A+1$ has much less divisors than A if x is large enough as follows. Choose x to be so large that the first prime number bigger than x is greater than the product of the first $N+2$ primes. Then prove that

$$\Omega(A\pm 1)+N+1\leqslant\Omega(A)$$

using that each prime divisor of $A-1$ or $A+1$ exceeds x. Show then that $\tau_0(A)=2^{\Omega(A)}=2^{\pi(A)}$, while $\tau(A\pm 1)\leqslant 2^{\Omega(A\pm 1)}\leqslant 2^{\pi(A)-N-1}$.)

Problem 2.4.3. Prove that $\omega(n)\ll\log n$ for $n\in\mathbf{N}$. (*Hint:* show that it suffices to show for square-free numbers $n\in\mathbf{N}$ and prove the statement for them by giving a lower bound on n in terms of $\omega(n)$.)

Problem 2.4.4. Prove that there exists $c>0$ such that for infinitely many n,

$$\tau_0(n)>n^{\frac{c}{\log\log n}}.$$

(*Hint:* for any $x\geqslant 10$, let n be the product of the primes not exceeding x. Compute $\tau_0(n)$ and apply Theorem 2.1.5 to relate x and n.)

Problem 2.4.5.** Prove that if f is a multiplicative number-theoretic function which is further monotone increasing, then it is totally multiplicative, and further $f=\mathrm{id}^s$ for some $s\geqslant 0$.

2.5 Approximation of irrational numbers

The aim of this section is to prove Dirichlet's approximation of irrational numbers.

Theorem 2.5.1 (Dirichlet's approximation – first form)**.** *For any $\alpha\in\mathbf{R}\setminus\mathbf{Q}$, and any $Q\in\mathbf{N}$, there exist integers $p\in\mathbf{Z}$ and $\mathbf{N}\ni q\leqslant Q$ such that*

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{qQ}.$$

Proof. Consider the numbers $\{\alpha\},\{2\alpha\},\dots,\{Q\alpha\}$. These are Q numbers, each of them is in one of the Q intervals $(0,1/Q),(1/Q,2/Q),\dots,((Q-1)/Q,1)$. If any of them, say, $\{q\alpha\}$ is in $(0,1/Q)$ or in $((Q-1)/Q,1)$, then for some $p\in\mathbf{Z}$,

$$|q\alpha-p|<\frac{1}{Q},$$

and the statement follows. If not, then by the pigeonhole principle, for some $q_1 > q_2$, $\{q_1\alpha\}, \{q_2\alpha\}$ are in the same interval $(i/Q, (i+1)/Q)$ for some $1 \leqslant i \leqslant Q-2$. Then for some $p \in \mathbf{Z}$,

$$|q_1\alpha - q_2\alpha - p| < \frac{1}{Q},$$

and the statement follows with $q = q_1 - q_2$. □

Corollary 2.5.2 (Dirichlet's approximation – second form)**.** *For any $\alpha \in \mathbf{R} \setminus \mathbf{Q}$, there exist infinitely many pairs of integers $p \in \mathbf{Z}$, $q \in \mathbf{N}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Proof. Set $Q = 1$, and apply Theorem 2.5.1 to find the first pair. Assume we have already found some pairs, say, $(p_1, q_1), \ldots, (p_n, q_n)$. Then choose Q such that

$$\left|\alpha - \frac{p_1}{q_1}\right|, \ldots, \left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{Q}.$$

Then apply again Theorem 2.5.1, it gives a further pair (p, q). It is not already listed, since

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ} \leqslant \frac{1}{Q} < \left|\alpha - \frac{p_1}{q_1}\right|, \ldots, \left|\alpha - \frac{p_n}{q_n}\right|.$$

The proof is complete. □

Definition 2.5.3 (Liouville numbers)**.** An irrational number α is said to be Liouville, if for any $n \in \mathbf{N}$, there exist infinitely many pairs $p \in \mathbf{Z}$, $q \in \mathbf{N}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Problem 2.5.1. Prove directly that for $n \in \mathbf{N}$, $\sqrt{n^2+1}$ can be approximated with a rational number of denominator $2n$ such that the error is less than n^{-2}. (*Hint:* compute the square of $n + 1/(2n)$.)

Problem 2.5.2. Prove that for any $\varepsilon > 0$, there exists an irrational number α such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

holds only for finitely many pairs $p \in \mathbf{Z}$, $q \in \mathbf{N}$. (*Hint:* in the interval $[0, 1]$, for any fraction p/q, draw an interval $I_{p/q}$ of radius $q^{-2-\varepsilon}$ centered at p/q. Show the lengths of these intervals sum up to $\leqslant 2q^{-1-\varepsilon}$. Using that

$$\sum_{q=1}^{\infty} \frac{1}{q^{1+\varepsilon}} < \infty,$$

show that if Q is large enough,

$$\bigcup_{q=Q}^{\infty} \bigcup_{p=0}^{q} I_{p/q} \subsetneqq [0, 1].$$

Take $\alpha \in [0, 1]$ not contained in the left-hand side here.)

Problem 2.5.3. Prove that there are continuum many Liouville numbers. (*Hint:* take an increasing sequence $a_1, a_2, \ldots$ of positive integers satisfying, for any $n \in \mathbf{N}$, that $a_{n+1} > 2a_n^n$ and that a_{n+1} is a multiple of a_n and $n!$. Take the numbers

$$\sum_{n=1}^{\infty} \frac{0 \text{ or } 1}{a_n}.$$

Show that each of them is approximated by its partial sums (as required in the definition of Liouville numbers) and that those containing infinitely many 1's are irrational.)

Problem 2.5.4. Assume $\alpha \in \mathbf{R}$. Prove that if $p_1, p_2 \in \mathbf{Z}$, $q_1, q_2 \in \mathbf{N}$ satisfy

$$\left|\alpha - \frac{p_1}{q_1}\right|, \left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{2q_1q_2},$$

then $p_1/q_1 = p_2/q_2$. (*Hint:* prove that if $p_1/q_1 \neq p_2/q_2$, then their difference is at least $1/(q_1q_2)$.)

2.6 Pell's equation

In this section, we are going to consider Pell's equation, and describe its solutions. Let $d > 0$ be an integer, which is not a square. Then Pell's equation is

$$x^2 - dy^2 = 1. \tag{2.6.1}$$

The trivial solutions are $x = \pm 1$, $y = 0$, our aim is to find nontrivial ones.

Proposition 2.6.1. *There are infinitely many nontrivial solutions of* (2.6.1).

Proof. By Dirichlet's approximation theorem (Corollary 2.5.2), there are infinitely many rational numbers x_n/y_n ($x_n, y_n \to \infty$) satisfying

$$\left| \frac{x_n}{y_n} - \sqrt{d} \right| < \frac{1}{y_n^2}.$$

Fix such an infinite sequence of x_n/y_n. Then

$$|x_n - \sqrt{d} y_n| < \frac{1}{y_n}.$$

Moreover, $x_n < \sqrt{d} y_n + 1$, which implies that

$$x_n + \sqrt{d} y_n < T y_n$$

for some real number T (depending only on d). Therefore,

$$\left| x_n^2 - d y_n^2 \right| < T$$

for all n. Since $|x_n^2 - dy_n^2|$ is an integer, there exists $t \in \mathbf{Z}$ such that $x_n^2 - dy_n^2 = t$ for infinitely many n. In an appropriate infinite subsequent, we may assume that $x_n^2 - dy_n^2 = t$ for all n and also that (x_n) and (y_n) are both constant modulo t. Then

$$\frac{x_m \pm \sqrt{d} y_m}{x_n \pm \sqrt{d} y_n} = \frac{x_m \pm \sqrt{d} y_m}{x_n \pm \sqrt{d} y_n} \cdot \frac{x_n \mp \sqrt{d} y_n}{x_n \mp \sqrt{d} y_n} = \frac{x_m x_n - d y_m y_n \pm \sqrt{d}(-x_m y_n + x_n y_m)}{x_n^2 - d y_n^2} = X_{m,n} \pm \sqrt{d} Y_{m,n}, \tag{2.6.2}$$

where $X_{m,n}, Y_{m,n} \in \mathbf{Z}$, since the denominator is t, and in the numerator, both $x_m x_n - d y_m y_n$ and $-x_m y_n + x_n y_m$ are 0 modulo t. Now

$$X_{m,n}^2 - d Y_{m,n}^2 = \frac{(x_m + \sqrt{d} y_m)(x_m - \sqrt{d} y_m)}{(x_n + \sqrt{d} y_n)(x_n - \sqrt{d} y_n)} = \frac{x_m^2 - d y_m^2}{x_n^2 - d y_n^2} = \frac{t^2}{t^2} = 1.$$

We are left to guarantee that $Y_{m,n} \neq 0$, in other words, the solution is nontrivial. Fix n, and tend to infinity by m. Then $x_m + \sqrt{d} y_m$ tends to infinity, so does $X_{m,n} + \sqrt{d} Y_{m,n}$, which implies $X_{m,n}, Y_{m,n} \to \infty$. □

For a given d, choose the solution (x_1, y_1) such that $x_1, y_1 > 0$ and x_1 is minimal among these (then so is y_1, or equivalently, $x_1 + \sqrt{d} y_1$ is minimal). We prove that this solution generates all other solutions in some sense.

Proposition 2.6.2. *If (x, y) is a solution such that $x, y > 0$, then for some $n \in \mathbf{N}$,*

$$x + \sqrt{d} y = (x_1 + \sqrt{d} y_1)^n.$$

Remark 2.6.3. It is easy to see that such numbers are solutions. If $x + \sqrt{d} y = (x_1 + \sqrt{d} y_1)^n$, then $x - \sqrt{d} y = (x_1 - \sqrt{d} y_1)^n$, which implies

$$x^2 - d y^2 = (x + \sqrt{d} y)(x - \sqrt{d} y) = (x_1 + \sqrt{d} y_1)^n (x_1 - \sqrt{d} y_1)^n = (x_1^2 - d y_1^2)^n = 1.$$

Remark 2.6.4. This means that we can compute all solutions: take $x_1 + \sqrt{d} y_1$, then raise to positive powers and separate their 'integer' and '$\sqrt{d}$' parts, they give x and y, respectively.

Proof. For a positive solution x, y, take the largest number $n \in \mathbf{N}$ such that

$$x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n \leqslant x + \sqrt{d}y.$$

Then for the reciprocals,

$$x_n - \sqrt{d}y_n = (x_1 - \sqrt{d}y_1)^n \geqslant x - \sqrt{d}y.$$

This implies

$$x_n - \sqrt{d}y_n \geqslant x - \sqrt{d}y > 0,$$

and dividing the left-hand side by y_n, and the middle expression by y, and using $y_n \leqslant y$ (which follows easily from $x_n + \sqrt{d}y_n \leqslant x + \sqrt{d}y$ and $x_n^2 - dy_n^2 = x^2 - dy^2$), we obtain

$$\frac{x_n}{y_n} \geqslant \frac{x}{y}.$$

Now repeating the computation in (2.6.2), we obtain

$$\frac{x + \sqrt{d}y}{x_n + \sqrt{d}y_n} = xx_n - dyy_n + \sqrt{d}(-xy_n + x_n y) = X + \sqrt{d}Y.$$

Since $x - \sqrt{d}y, x_n - \sqrt{d}y_n > 0$, we have $x > \sqrt{d}y, x_n > \sqrt{d}y_n$, then $X = xx_n - dyy_n > 0$. Also by $x_n/y_n \geqslant x/y$, $Y = -xy_n + x_n y \geqslant 0$. Therefore (X, Y) is a nonnegative solution. By the maximal choice of n, $X + \sqrt{d}Y < x_1 + \sqrt{d}y_1$. Then by the minimality of (x_1, y_1), $X = 1$, $Y = 0$, implying $x + \sqrt{d}y = x_n + \sqrt{d}y_n$. □

Now we are going to get rid of the positivity condition. First let y be arbitrary, and assume $x > 0$. If $y > 0$, then $x + \sqrt{d}y = (x_1 + \sqrt{d}y_1)^n$ for some $n \in \mathbf{N}$. If $y = 0$, then x must be 1, so $x + \sqrt{d}y = (x_1 + \sqrt{d}y_1)^0$. Finally, if $y < 0$, then $(x, -y)$ is also a solution with $-y > 0$, therefore it is of the form $x + \sqrt{d}(-y) = (x_1 + \sqrt{d}y_1)^n$ for some $n \in \mathbf{N}$; then taking reciprocals, we get $x + \sqrt{d}y = (x_1 + \sqrt{d}y_1)^{-n}$. Altogether, the solutions in the case $x > 0$ can be described as follows: all solutions (x, y) with $x > 0$ are given via $x + \sqrt{d}y = (x_1 + \sqrt{d}y_1)^n$ as n runs through $\mathbf{Z}$.

Finally, observe that if (x, y) is a solution, then so is $(-x, -y)$, so taking negatives, we may assume that $x > 0$ (there is trivially no solution with $x = 0$).

We summarize these results as follows.

Theorem 2.6.5. *The solutions of (2.6.1) can be described as follows. There exists a solution (x_1, y_1) such that $x_1, y_1 > 0$ and $x_1 + \sqrt{d}y_1$ is minimal among these. Then the solutions (x, y) are exactly the pairs of integers that satisfy*

$$x + \sqrt{d}y = \pm(x_1 + \sqrt{d}y_1)^n$$

for some $n \in \mathbf{Z}$. □

Problem 2.6.1. For a fixed $k \in \mathbf{Z}$, consider the more general Pell equation

$$x^2 - dy^2 = k.$$

Prove that if it has a solution, it has infinitely many. (*Hint:* take a solution of the equation

$$x^2 - dy^2 = k,$$

and multiply it by the infinitely many solutions (as in (2.6.2)) of

$$x^2 - dy^2 = 1.$$

Show they give rise to infinitely many solutions of

$$x^2 - dy^2 = k.)$$

Problem 2.6.2. The set $(a, b, c) \in \mathbf{N}^3$ is said to be a pythagorean triple, if $a^2 + b^2 = c^2$, and it is a primitive pythagorean triple, if it further satisfies $\gcd(a, b, c) = 1$. Prove that for any pythagorean

triple (a, b, c), there is a unique primitive pythagorean triple (a', b', c') and a unique $d \in \mathbf{N}$ such that $a = da'$, $b = db'$, $c = dc'$. (*Hint:* set $d = \gcd(a, b, c)$ and $(a', b', c') = (a/d, b/d, c/d)$. Prove that (a', b', c') is pythagorean and satisfies $\gcd(a', b', c') = 1$. As for uniqueness, observe that if (a, b, c) is a multiple of another pythagorean triple (a', b', c'), then $(a', b', c') = (a/d, b/d, c/d)$ for some $d \in \mathbf{N}$, therefore, d must be a common divisor of a, b and c. Use that among the divisors, there is a largest one, which is a multiple of all other divisors; we have seen this for two numbers: for three numbers, read this out from their canonical form (1.2.1). Conclude d is well-defined from (a, b, c) to obtain a primitive pythagorean triple $(a/d, b/d, c/d)$.)

Problem 2.6.3. Prove that the primitive pythagorean triples are parametrized as follows: $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$, where (m, n) runs through those pairs of integers that are coprime and satisfy that one of them is even, the other one is odd. Check that these are indeed primitive pythagorean triples. (*Hint:* showing that $a^2 + b^2 = c^2$ for numbers of the given form is straight-forward. To see they are coprime, assume that an odd prime p divides a, b, c, then show it divides m, n, a contradiction. Prove that $2 \nmid \gcd(a, b, c)$ follows from the different parity of m and n. As for the parametrization, assume (a, b, c) is a given primitive pythagorean triple. Without loss of generality, assume a, c are odd (considering the pythagorean equation modulo 4, prove that c is odd and that exactly one of a and b is odd, the other is even). Then write $(b/2)^2 = ((c - a)/2)((c + a)/2)$, and prove that the two factors on the right-hand side are coprime. Using also that their product is a square, conclude $(c - a)/2$ and $(c + a)/2$ are both squares. Setting $n^2 = (c - a)/2$, $m^2 = (c + a)/2$ prove that $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$, that $\gcd(m, n) = 1$, and also that exactly one of m and n is even, the other one is odd.)

Problem 2.6.4. Prove that $n \in \mathbf{N}$ can be written as the difference of two square numbers if and only if $n \not\equiv 2 \bmod 4$. (*Hint:* write the equation $n = x^2 - y^2$ in the form $n = (x - y)(x + y)$. Prove that $x - y$ and $x + y$ share the same parity, which excludes the solvability when $n \equiv 2 \bmod 4$. On the other hand, when $n \not\equiv 2 \bmod 4$, write it as the product of two numbers of the same parity ($n = ab$, say) and solve the linear system $a = x - y, b = x + y$. Prove that the resulting x, y are both integers and $n = x^2 - y^2$.)

2.7 Number theory of polynomials

In this section, we will work abstractly to some extent, on the one hand, making life more complicated. On the other hand, this has the benefit that our results are applicable among much more general circumstances. Along this principle, let K be any field.

The object we will examine is the polynomial ring $K(x)$ in one variable x. We will see that this object resembles a lot to $\mathbf{Z}$ from the structural point of view, namely, a considerable amount of Section 1.2 can be translated to the language of polynomials. What we are going to understand is the following.

Dictionary

notion	in $\mathbf{Z}$	in $K[x]$
units	± 1	$K^\times$
norm	absolute value	degree
euclidean algorithm	euclidean algorithm	euclidean algorithm
primes/irreducibles	prime numbers	irreducible polynomials
residue classes	residue classes	residue classes

Definition 2.7.1 (divisibility)**.** Given polynomials $p(x), q(x) \in K[x]$, we say $q(x) \mid p(x)$, if there exists a polynomial $r[x]$ such that $p(x) = q(x)r(x)$.

Proposition 2.7.2. *If $p(x) \mid q(x), s(x)$, then for any polynomial $r(x) \in K(x)$, $p(x) \mid q(x)r(x) + s(x)$.*

Proof. By definition, for some $u(x), v(x)$,

$$q(x) = p(x)u(x), \qquad s(x) = p(x)v(x).$$

Then

$$q(x)r(x) + s(x) = p(x)u(x)r(x) + p(x)v(x) = p(x)(u(x)r(x) + v(x)),$$

so the polynomial $u(x)r(x) + v(x) \in K[x]$ multiplies $p(x)$ into $q(x)r(x) + s(x)$. □

Definition 2.7.3 (units)**.** If $p(x) \mid q(x)$ for all $q(x) \in K[x]$, we say that $p(x)$ is a unit.

Proposition 2.7.4. *In $K[x]$, the only units are the nonzero constant polynomials $c \in K^\times$.*

Proof. First we prove that the nonzero constants $c \in K^\times$ are units. Indeed, take any polynomial $p(x)$, we have $p(x) = c \cdot c^{-1}p(x)$, so the polynomial $c^{-1}p(x) \in K[x]$ multiplies c into $p(x)$.

For the converse, recall that if $p(x), q(x)$ are nonzero polynomials, then

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$$

holds for the degrees. Since the degree is a nonnegative integer, this means that a polynomial $p(x)$ of positive degree cannot divide a nonzero constant polynomial, say 1 (if we multiply $p(x)$ by 0, we get 0; if we multiply $p(x)$ by nonzero, we get something of degree not less than that of $p(x)$). The polynomial 0 is also not a unit, since its only multiple is 0. □

Proposition 2.7.5 (euclidean division)**.** *Given polynomials $p(x), q(x) \in K[x]$, $q(x) \neq 0$. Then there exist polynomials $r(x), s(x)$ satisfying $p(x) = q(x)r(x) + s(x)$ and either $s(x) = 0$ or $\deg s(x) < \deg q(x)$.*

Proof. Fix $0 \neq q(x) = b_k x^k + \ldots + b_1 x + b_0 \in K[x]$ with $\deg q(x) = k$ (i.e. $b_k \neq 0$). If $p(x) = 0$, then $r(x) = s(x) = 0$ does the job.

For $p(x) \neq 0$, we prove by induction on $\deg p(x)$. If $\deg p(x) = 0$, then $r(x) = 0$, $s(x) = p(x)$ does the job for $\deg q(x) > 0$ and $r(x) = p(x)/q(x)$, $s(x) = 0$ does the job for $\deg q(x) = 0$ (this time $q(x)$ is a nonzero constant so it makes sense to divide $p(x)$ by it).

Assume $\deg p(x) = n > 0$ and that the statement holds for 0 and any polynomial of lower degree in place of $p(x)$. Let $p(x) = a_n x^n + \ldots + a_1 x + a_0$ with $a_n \neq 0$. If $n < k$, then $r(x) = 0$, $s(x) = p(x)$ does the job. In the other case $n \geqslant k$, set $t(x) = (a_n/b_k)x^{n-k} \in K[x]$. We have

$$\begin{aligned} p(x) - t(x)q(x) &= a_n x^n + \ldots + a_1 x + a_0 - \left(a_n x^n + \frac{a_n}{b_k} b_{k-1} x^{n-1} + \ldots + \frac{a_n}{b_k} b_1 x^{n-k+1} + \frac{a_n}{b_k} b_0 x^{n-k} \right) \\ &= c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 = u(x), \end{aligned}$$

for $c_{n-1}, \ldots, c_0 \in K$. If $u(x) = 0$, then $r(x) = t(x)$, $s(x) = 0$ does the job. If $u(x) \neq 0$, clearly $\deg u(x) \leqslant n - 1$, so for some $v(x), w(x) \in K[x]$ satisfying $\deg w(x) < \deg q(x)$ or $w(x) = 0$, and $u(x) = q(x)v(x) + w(x)$ by the induction hypothesis. Then

$$p(x) = q(x)t(x) + u(x) = q(x)t(x) + q(x)v(x) + w(x) = q(x)(t(x) + v(x)) + w(x),$$

so $r(x) = t(x) + v(x)$, $s(x) = w(x)$ does the job. □

Then we may define, for any polynomials $p(x), q(x)$, their gcd, analogously to that in Proposition 1.2.2 (in this case, instead of absolute value, we consider the degree of the remainders, which form a decreasing sequence of nonnegative integers, hence terminates); then define primes and irreducibles as in Definitions 1.2.6, 1.2.7; via integer combinations (Proposition 1.2.5), we can prove that primes and irreducibles are the same (Proposition 1.2.8); and finally conclude the fundamental theorem of arithmetic in $K[x]$ the same way as in Theorem 1.2.9.

Definition 2.7.6 (irreducible polynomials)**.** A nonzero, nonconstant polynomial is said to be an irreducible polynomial, if it cannot be written as the product of two polynomials of lower degree.

Remark 2.7.7. These are the same as prime polynomials (those which divide a product only if they divide one of the factors), recall Proposition 1.2.8.

Theorem 2.7.8. *Every nonzero polynomial in $K[x]$ can be written as a product of irreducible polynomials. The decomposition is unique, apart from constant polynomials.*

Proof. Follow the pattern of Section 1.2 as described above. □

Also, it makes sense to speak about residue classes.

Definition 2.7.9 (congruence)**.** Given $p(x) \in K[x]$, we say that $q(x) \equiv r(x) \bmod p(x)$ (in words: $q(x)$ is congruent to $r(x)$ modulo $p(x)$) if $p(x) \mid (q(x) - r(x))$.

This is an equivalence relation, and the residue classes form a ring just like in Proposition 1.4.6, which is denoted by $K[x]/p(x)$.

Proposition 2.7.10 (remainders)**.** *Given $0 \neq p(x) \in K[x]$ and $q(x) \in K[x]$, there exists $r(x) \in K[x]$ satisfying $q(x) \equiv r(x) \bmod p(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg p(x)$.*

Proof. Clear from Proposition 2.7.5. □

Proposition 2.7.11. *Assume $0 \neq p(x) \in K[x]$. Then $K[x]/p(x)$ is a field if and only if $p(x)$ is irreducible.*

Proof. If $p(x)$ is not irreducible, then for some polynomials $q(x), r(x)$ of lower degree than $p(x)$, $p(x) = q(x)r(x)$, i.e. $q(x)r(x) \equiv 0 \bmod p(x)$. Then $q(x), r(x)$ are not invertible in $K[x]/p(x)$, and since they are nonzero, this means $K(x)/p(x)$ is not a field.

Conversely, assume $p(x)$ is irreducible. We have to prove that any $q(x) \not\equiv 0 \bmod p(x)$ has a multiplicative inverse modulo $p(x)$. Since $q(x) \not\equiv 0 \bmod p(x)$, $p(x) \nmid q(x)$. Using that $p(x)$ is irreducible, this means that $\gcd(p(x), q(x)) = 1$. Then by integer combinations (the version of Proposition 1.2.5 to polynomials) means that for some $u(x), v(x) \in K[x]$,

$$p(x)u(x) + q(x)v(x) = 1.$$

Then clearly

$$q(x)v(x) \equiv 1 \bmod p(x),$$

so $v(x)$ is the multiplicative inverse of $q(x)$ modulo $p(x)$. □

Now we turn to an other important topic in the number theory of polynomials, namely, we are going to investigate the polynomials in $\mathbf{Z}[x]$. Since $\mathbf{Z}$ is not a field, it is not covered by our above results.

Definition 2.7.12 (primitive polynomial)**.** A polynomial $p(x) \in \mathbf{Z}[x]$ is primitive, if it is nonzero, and

$$p(x) = a_n x^n + \ldots + a_1 x + a_0$$

satisfies $\gcd(a_n, \ldots, a_0) = 1$.

Proposition 2.7.13 (Gauss)**.** *The product of two primitive polynomials is a primitive polynomial.*

Proof. Assume $u(x) = a_n x^n + \ldots + a_1 x + a_0$ and $v(x) = b_k x^k + \ldots + b_1 x + b_0$ are both primitive polynomials.

Fixing any prime $p \in \mathbf{Z}$, it suffices to show that there is a coefficient of $(uv)(x)$, which is not divisible by p (then taking this for all primes, we obtain that the gcd of all coefficients is 1). Let $a_{n'}$ and $b_{k'}$ be the highest degree coefficients in $u(x), v(x)$, respectively, which are not divisible by p (there are such coefficients, since $u(x), v(x)$ are primitive). Now compute the coefficient of $x^{n'+k'}$ in $(uv)(x)$:

$$a_n b_{n'+k'-n} + a_{n-1} b_{n'+k'-n+1} + \ldots + a_{n'} b_{k'} + \ldots + a_{n'+k'-k+1} b_{k-1} + a_{n'+k'-k} b_k,$$

where the a_i's and b_j's are defined to be zero for $i > n$, $j > k$. In this sum, by the maximal choice of n', k' for $p \nmid a_{n'}, b_{k'}$, each term is divisible by p except for $a_{n'} b_{k'}$. □

Proposition 2.7.14. *Any polynomial $0 \neq p(x) \in \mathbf{Q}(x)$ can be written as $p(x) = c \cdot q(x)$ where $c \in \mathbf{Q}^\times$ and $q(x) \in \mathbf{Z}[x]$ is primitive. The pair $c, q(x)$ is unique up to signs.*

Proof. Write $p(x)$ as

$$\frac{a_n}{b_n} x^n + \ldots + \frac{a_1}{b_1} x + \frac{a_0}{b_0},$$

where the a's are integers, the b's are nonzero integers, and for each $0 \leqslant j \leqslant n$, $\gcd(a_j, b_j) = 1$. Set then $B = b_n \cdot \ldots \cdot b_0$

$$\begin{aligned} p(x) =& \frac{1}{B}(Ba_n x^n + \ldots + Ba_1 x + Ba_0) \\ =& \frac{\gcd(Ba_n, \ldots, Ba_0)}{B} \\ & \cdot \left(\frac{Ba_n}{\gcd(Ba_n, \ldots, Ba_0)} x^n + \ldots + \frac{Ba_1}{\gcd(Ba_n, \ldots, Ba_0)} x + \frac{Ba_0}{\gcd(Ba_n, \ldots, Ba_0)} \right), \end{aligned}$$

and this is of the desired form.

As for the uniqueness, assume $c_1 q_1(x) = c_2 q_2(x)$ where $c_1, c_2 \in \mathbf{Q}^\times$ and $q_1(x), q_2(x)$ are both primitive. Dividing by c_2, then writing $c_1/c_2 = d_1/d_2$ with $d_1, d_2 \in \mathbf{Z}$ and $\gcd(d_1, d_2) = 1$, we have

$$\frac{d_1}{d_2} q_1(x) = q_2(x).$$

This means, by the primitivity of q_1, that $d_2 = \pm 1$ (if it were divisible by a prime, $d_1 q_1(x)/d_2$ would be a noninteger polynomial). Therefore $c_2 \mid c_1$, and the same way, $c_1 \mid c_2$. Then $c_1 = \pm c_2$, $q_1(x) = \pm q_2(x)$. □

Proposition 2.7.15. *Assume $p(x) \in \mathbf{Z}[x]$ is irreducible in $\mathbf{Z}[x]$. Then it is irreducible also in $\mathbf{Q}[x]$.*

Proof. Clearly $p(x)$ is primitive (otherwise we could factor a prime out of it, which contradicts its irreducibility).

Now assume $p(x) = q(x)r(x)$ for some polynomials $q(x), r(x) \in \mathbf{Q}[x]$. Then by Proposition 2.7.14, for some $q', r' \in \mathbf{Q}^\times$, and primitive polynomials $Q(x), R(x) \in \mathbf{Z}[x]$,

$$p(x) = q' r' Q(x) R(x).$$

By Proposition 2.7.13, $Q(x)R(x)$ is primitive, and then by the essential uniqueness in Proposition 2.7.14, we have $Q(x)R(x) = \pm p(x)$, $q'r' = \pm 1$. Now since $p(x)$ is irreducible in $\mathbf{Z}[x]$, either $Q(x)$ or $R(x)$ equals $\pm p(x)$. Then either $q(x)$ or $r(x)$ differs from $p(x)$ only by a constant factor.

Since this argument holds for any factorization $p(x) = q(x)r(x)$ in $\mathbf{Q}[x]$, the proof is complete. □

Proposition 2.7.16. *Assume $p(x) \in \mathbf{Z}[x]$ is irreducible in $\mathbf{Z}[x]$. Then it is a prime in $\mathbf{Z}[x]$, i.e. whenever $p(x) \mid u(x)v(x)$ with $u(x), v(x) \in \mathbf{Z}[x]$, $p(x) \mid u(x)$ or $p(x) \mid v(x)$.*

Proof. We may assume that $u(x)v(x) \neq 0$. Considering everything in $\mathbf{Q}[x]$, $p(x) \mid u(x)v(x)$ in $\mathbf{Q}[x]$, and applying Proposition 2.7.15 and Remark 2.7.7, we see that $p(x)$ divides at least one of $u(x)$ and $v(x)$ in $\mathbf{Q}(x)$. Assume it is $u(x)$, then applying Proposition 2.7.14, we obtain

$$\frac{u(x)}{p(x)} = c \cdot q(x)$$

where $c \in \mathbf{Q}^\times$, and $q(x) \in \mathbf{Z}[x]$ is primitive. Multiplying, we obtain

$$u(x) = c \cdot p(x) q(x).$$

Here, $p(x)q(x)$ is primitive by Proposition 2.7.13. Now since $u(x) \in \mathbf{Z}[x]$, $c \in \mathbf{Z}$. Then $u(x)/p(x) \in \mathbf{Z}[x]$. □

This means that we have the analogue of Proposition 1.2.8, so the fundamental theorem of arithmetic holds.

Theorem 2.7.17. *Every nonzero polynomial in $\mathbf{Z}[x]$ can be written as a product of irreducible polynomials. The decomposition is unique, apart from the constant polynomials ± 1.*

Proof. Follow the pattern of Section 1.2 as described above. □

Remark 2.7.18. Observe that we have no euclidean algorithm and there is no analogue for Proposition 1.2.5: for example, the greatest common divisor of 2 and x is 1, but no matter how we choose $u(x), v(x) \in \mathbf{Z}[x]$,

$$2u(x) + xv(x) \neq 1.$$

Remark 2.7.19. The method described here in fact proves that if R is a ring with unique factorization, then $R[x]$ has also unique factorization. A nice consequence of this is the fact that for any field K, the polynomial ring $K[x_1, \ldots, x_n]$ in many variables has unique factorization. Also, $\mathbf{Z}[x_1, \ldots, x_n]$ has unique factorization.

2.8 Algebraic and transcendental numbers

Assume $\mathbf{Q} \subseteq K \subseteq \mathbf{C}$ is a field, which is a little more special situation than the one covered in Section 2.7.

Definition 2.8.1 (algebraic number, minimal polynomial)**.** We say that a number $\alpha \in \mathbf{C}$ is algebraic over K if it is a root of a nonzero polynomial in $K[x]$, i.e.

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$$

for some $a_n, \ldots, a_1, a_0 \in K$ which are not all zero. If the degree n of the polynomial is chosen to be minimal, we say it is the minimal polynomial of α over K.

Remark 2.8.2. Note that the minimal polynomial is well-defined only modulo a nonzero constant factor, i.e. if $p(x)$ is such a polynomial, then for any $a \in K^\times$, $(ap)(x)$ is also such a polynomial.

Proposition 2.8.3. *The minimal polynomial $p(x)$ of α is irreducible.*

Proof. Assume by contradiction that $p(x) = q(x)r(x)$ where, $q(x), r(x) \in K[x]$ are of lower degree than $p(x)$. Clearly

$$0 = p(\alpha) = q(\alpha)r(\alpha),$$

so at least one of $q(\alpha)$ and $r(\alpha)$ is zero. This contradicts the minimal choice of $p(x)$ in degree. □

Proposition 2.8.4. *If a number $\alpha \in \mathbf{C}$ is algebraic, the field generated by α (over K) is finite-dimensional over K as a vector space. If a field F is finite-dimensional over K as a vector space, then all of its elements are algebraic.*

Proof. For the first statement, denote by F the field generated by the algebraic number α. Assume its minimal polynomial is

$$p(x) = a_n x^n + \ldots + a_1 x + a_0.$$

Set

$$S = K[x]/p(x) = \left\{\lambda_{n-1}x^{n-1} + \ldots + \lambda_1 x + \lambda_0 : \lambda_{n-1}, \ldots, \lambda_0 \in K\right\},$$

the equation on the right is meant under the identification of each polynomial in $K[x]$ and its residue modulo $p(x)$ (recall Proposition 2.7.10). Let now S' be the image of S under $x \mapsto \alpha$. This is an isomorphism of rings, since $p(\alpha) = 0$.

We claim that $F = S'$. Clearly $S' \subseteq F$, since all elements listed as residue classes modulo $p(x)$ in the definition of S are generated by x, which gives altogether S' after $x \mapsto \alpha$. Now it suffices to prove that S' is a field, which follows from Proposition 2.7.11 applied to S.

For the second statement, assume F is finite-dimensional over K, and let $\alpha \in F$ be arbitrary. Then $1, \alpha, \alpha^2, \ldots$ are not linearly independent, implying that there exist $a_n, \ldots, a_1, a_0 \in K$ such that

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0.$$

Then α is algebraic by definition. □

Theorem 2.8.5. *Algebraic numbers form a field.*

Proof. If α is algebraic, then for some $a_n, \ldots, a_1, a_0 \in K$ not all zero, we have

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0.$$

Then

$$(-1)^n a_n(-\alpha)^n + (-1)^{n-1}a_{n-1}(-\alpha)^{n-1} + \ldots + (-1)a_1\alpha + a_0 = 0$$

and when $\alpha \neq 0$, also

$$a_n + a_{n-1}\alpha^{-1} + \ldots + a_1\alpha^{-(n-1)} + a_0\alpha^n = 0$$

together show that $-\alpha$ and $1/\alpha$ (provided that $\alpha \neq 0$) are algebraic.

So we are left to prove that the sum and the product of two algebraic numbers are algebraic. Assume that $K \subseteq E \subseteq F \subseteq \mathbf{C}$ are fields, and that $\alpha_1, \ldots, \alpha_k \in E$ form a K-basis of E as a vector space, and that

$\beta_1, \ldots, \beta_l$ form an E-basis of F as a vector space. Then we claim that $(\alpha_i\beta_j)_{1\leqslant i\leqslant k, 1\leqslant j\leqslant l}$ is a K-basis of F as a vector space.

Let $\xi \in F$ be arbitrary. Then

$$\xi = \lambda_1\beta_1 + \ldots + \lambda_l\beta_l, \qquad \lambda_1, \ldots, \lambda_l \in E$$

since the β_j's form a basis of F over E as a vector space. Now write each λ_j (for $1 \leqslant j \leqslant l$) as

$$\lambda_j = \mu_{1,j}\alpha_1 + \ldots + \mu_{k,j}\alpha_k, \qquad \mu_{1,j}, \ldots, \mu_{k,j} \in K,$$

which can be done, as the α_i's form a basis of E over K. Obviously,

$$\xi = (\mu_{1,1}\alpha_1 + \ldots + \mu_{k,1}\alpha_k)\beta_1 + \ldots + (\mu_{1,l}\alpha_1 + \ldots + \mu_{k,l}\alpha_k)\beta_l = \sum_{\substack{1\leqslant i\leqslant k\\ 1\leqslant j\leqslant l}} \mu_{i,j}\alpha_i\beta_j,$$

which shows that $\alpha_i\beta_j$'s indeed form a generating set of F over K as a vector space.

To see it is a basis, assume

$$\sum_{\substack{1\leqslant i\leqslant k\\ 1\leqslant j\leqslant l}} \mu_{i,j}\alpha_i\beta_j = 0, \qquad \mu_{i,j} \in K.$$

Setting

$$\lambda_j = \mu_{1,j}\alpha_1 + \ldots + \mu_{k,j}\alpha_k, \qquad \mu_{1,j}, \ldots, \mu_{k,j} \in K$$

for each $1 \leqslant j \leqslant l$, this means

$$\lambda_1\beta_1 + \ldots + \lambda_l\beta_l = 0, \qquad \lambda_1, \ldots, \lambda_l \in E.$$

Now since β_j's form a basis of F over E as a vector space, each λ_j must be 0. Then since α_i's form a basis of E over K as a vector space, each $\mu_{i,j}$ must be 0.

Now assume α, β are algebraic. Setting E for the field generated by α over K, and F for the field generated by β over E, Proposition 2.8.4 implies that E is finite-dimensional over K, and F is finite-dimensional over E (both as vector spaces). What we have proved now is that then F is finite-dimensional over K as a vector space. Applying again Proposition 2.8.4 we see that each element of F is algebraic over K. In particular, since $\alpha + \beta, \alpha\beta \in F$, they are algebraic. □

Definition 2.8.6 (transcendental numbers)**.** A number $\alpha \in \mathbf{C}$ is said to be transcendental over K if it has no minimal polynomial.

In view of Proposition 2.8.4, this amounts to say that the field generated by α is infinite-dimensional over K as a vector space. For the rest of this section, set $K = \mathbf{Q}$. Are there then transcendental numbers at all?

Theorem 2.8.7. *There are continuum many transcendental numbers.*

Proof. The number of polynomials in $\mathbf{Q}[x]$ is countable. Each of them has finitely many roots, therefore the number of algebraic numbers is countable. On the other hand, the cardinality of $\mathbf{C}$ (also of $\mathbf{R}$) is continuum, which is bigger than countable, therefore continuum many elements in $\mathbf{C}$ (also in $\mathbf{R}$) are transcendental. □

Historically, the question on the existence of transcendental numbers arose before the set theory of Cantor, so this was not the way how mathematicians first answered it. What we are going to prove is that Liouville numbers are transcendental, and we know it is relatively easy to construct Liouville numbers (we have seen this in the problem section of Section 2.5).

Theorem 2.8.8 (Liouville)**.** *Every Liouville number is transcendental.*

Proof. Assume α is Liouville, and by contradiction that

$$a_N\alpha^N + \ldots + a_1\alpha + a_0 = 0$$

for a nonzero polynomial $f(x) = a_N x^N + \ldots + a_1 x + a_0$ of integer coefficients, which is irreducible over $\mathbf{Q}$. Since α is Liouville, we may take rational numbers p_n/q_n with $q_n \to \infty$ satisfying

$$\alpha - \frac{p_n}{q_n} = o(q_n^{-N}).$$

For any $1 \leqslant j \leqslant N$, we have

$$\alpha^j - \left(\frac{p_n}{q_n}\right)^j = \left(\alpha - \frac{p_n}{q_n}\right)\left(\alpha^{j-1} + \alpha^{j-2}\frac{p_n}{q_n} + \ldots + \alpha\left(\frac{p_n}{q_n}\right)^{j-2} + \left(\frac{p_n}{q_n}\right)^{j-1}\right) = o(q_n^{-N}).$$

Then

$$f\left(\frac{p_n}{q_n}\right) = f(\alpha) + \sum_{j=0}^{N} a_j \left(\left(\frac{p_n}{q_n}\right)^j - \alpha^j\right) = o(q_n^{-N}).$$

Multiplying this by q_n^N, we obtain

$$a_N p_n^N + a_{N-1} p_n^{N-1} q_n + \ldots + a_1 p_n q_n^{N-1} + a_0 q_n^N = o(1).$$

Here, the left-hand side is an integer, so it must be zero, if n is large enough. Then, by its irreducibility, the degree of $f(x)$ is 1, which contradicts that α is irrational. □

Remark 2.8.9. One can define the degree of an algebraic number as the degree of its minimal polynomial. The proof of Theorem 2.8.8 in fact shows that an algebraic number of degree N cannot be approximated by rational numbers p_n/q_n such that

$$\alpha - \frac{p_n}{q_n} = o(q_n^{-N}).$$

Theorem 2.8.10 (Hermite)**.** *The number e is transcendental.*

Proof omitted.

Theorem 2.8.11 (Lindemann)**.** *The number π is transcendental.*

Proof omitted.

Problem 2.8.1. Give a polynomial $p(x) \in \mathbf{Q}[x]$ such that $p(\sqrt{2} + \sqrt{3}) = 0$. (*Hint:* consider the polynomial

$$p(x) = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}).$$

Prove that $p(x) \in \mathbf{Q}[x]$ and that $p(\sqrt{2} + \sqrt{3}) = 0$.)

Problem 2.8.2. Assume $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$ has a rational root p/q with $\gcd(p, q) = 1$. Prove that $p \mid a_0, q \mid a_n$. (*Hint:* write

$$f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + \ldots + a_1\frac{p}{q} + a_0 = 0.$$

Multiply both sides by q^n and conclude $q \mid a_n p^n$, $p \mid a_0 q^n$. Use the assumption $\gcd(p, q) = 1$.)

Chapter 3
Quadratic forms

3.1 Sum of two squares

In this section, we are going to answer the question which integers are represented as the sum of two squares, in other words, for which n can one solve the diophantine equation

$$x^2 + y^2 = n.$$

For a better understanding, we introduce the ring of gaussian integers, namely

$$\mathbf{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbf{Z}\}.$$

One can easily check that gaussian integers form a ring.

Definition 3.1.1 (divisibility)**.** For $\alpha, \beta \in \mathbf{Z}[\sqrt{-1}]$, we say thet $\beta \mid \alpha$, if there exists some $\gamma \in \mathbf{Z}[i]$ such that $\alpha = \beta\gamma$.

Definition 3.1.2 (conjugate of gaussians)**.** The conjugate of a gaussian integer $a + b\sqrt{-1}$ is defined as

$$a + b\sqrt{-1} = a - b\sqrt{-1}.$$

Definition 3.1.3 (norm of gaussians)**.** The norm of a gaussian integer $\alpha = a + b\sqrt{-1}$ is defined as

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2.$$

Two important facts is that we often think about gaussian integers as they are embedded into $\mathbf{C}$ via the identification $\sqrt{-1} \mapsto i$; and that $\mathbf{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} : a, b \in \mathbf{Q}\}$ (or $\mathbf{Q}(i)$, when embedded) is the field of fractions for $\mathbf{Z}[\sqrt{-1}]$. Note that norm and conjugation can be extended to $\mathbf{Q}(\sqrt{-1})$, and further, in the complex embedding, $N(\cdot) = |\cdot|^2$, where $|\cdot|$ is the complex absolute value.

Proposition 3.1.4. *We have $N(\alpha)N(\beta) = N(\alpha\beta)$ for any numbers $\alpha, \beta \in \mathbf{Q}(\sqrt{-1})$.*

Proof. This can be seen in the complex embedding (via $N(\cdot) = |\cdot|^2$), or also from the following calculation:

$$N(a+b\sqrt{-1})N(c+d\sqrt{-1}) = (a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2 = N((ac-bd)+(ad+bc)\sqrt{-1}),$$

and observe that $(ac - bd) + (ad + bc)\sqrt{-1} = (a + b\sqrt{-1})(c + d\sqrt{-1})$. □

Proposition 3.1.5 (euclidean division)**.** *Given gaussian integers α, β, $\beta \neq 0$. Then there exist gaussian integers γ, δ satisfying $\alpha = \beta\gamma + \delta$ and $N(\delta) < N(\beta)$.*

Proof. Use the complex embedding, and consider the fraction $\alpha/\beta \in \mathbf{C}$. It is in some unit square in the lattice generated by 1 and i. The longest distance in the unit square is $\sqrt{2}$, so there is some $\gamma \in \mathbf{Z}[\sqrt{-1}]$ such that $|\alpha/\beta - \gamma| < 1$. Let $\delta = \alpha - \beta\gamma$. It is easy to check that $N(\delta) < N(\beta)$. □

Then we may define, for any gaussian integers α, β, their gcd, analogously to that in Proposition 1.2.2 (in this case, instead of absolute value, we consider the norm of the remainders, which form a decreasing sequence of natural numbers, hence terminates); then define primes and irreducibles as in Definitions 1.2.6, 1.2.7; via integer combinations (Proposition 1.2.5), we can prove that primes and irreducibles are the same (Proposition 1.2.8); and finally conclude the fundamental theorem of arithmetic among gaussian integers the same way as in Theorem 1.2.9.

Theorem 3.1.6. *Every nonzero gaussian integer can be written as a product of gaussian prime (irreducible) numbers. The decomposition is unique, apart from factors dividing* 1.

Proof. Follow the pattern of Section 1.2 as described above. □

The importance of gaussian integers in our problem can be understood via considering the norm function: obviously, a positive integer n can be written as the sum of two squares if and only if it is the norm of a gaussian integer. Indeed, if $n = a^2 + b^2$ with $a, b \in \mathbf{Z}$, then $n = N(a + b\sqrt{-1})$ and $a + b\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}]$; while if $n = N(a + b\sqrt{-1})$ with $a + b\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}]$, then $n = a^2 + b^2$ and $a, b \in \mathbf{Z}$.

Proposition 3.1.7. *If two numbes can be written as the sum of two squares then so is their product.*

Proof. By our observation, being the sum of two squares is equivalent to being a norm of a gaussian integer. The product of norms of two gaussian integers is the norm of the product of the gaussian integers themselves (which is a gaussian integer again) by Proposition 3.1.4. The proof is complete then by using again the equivalence of being a norm and being the sum of two squares.

Alternatively, if $m = x_1^2 + x_2^2$ and $n = y_1^2 + y_2^2$, then

$$mn = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

Note that the two proofs are connected by taking the complex numbers $\alpha = x_1 + y_1 i$, $\beta = x_2 + y_2 i$, when $m = |\alpha|^2 = x_1^2 + y_1^2$ and $n = |\beta|^2 = x_2^2 + y_2^2$. Then $|\alpha|^2|\beta|^2 = |\alpha\beta|^2$, and $\alpha\beta = (x_1y_1 - x_2y_2) + (x_1y_2 + x_2y_1)i$. □

Proposition 3.1.8. *If $p \equiv -1 \bmod 4$, and $a^2 + b^2 \equiv 0 \bmod p$, then $a, b \equiv 0 \bmod p$.*

Proof. Assume $b \not\equiv 0 \bmod p$. Then divide by b modulo p,

$$\left(\frac{a}{b}\right)^2 \equiv -1 \bmod p, \qquad \left(\frac{a}{b}\right)^4 \equiv 1 \bmod p.$$

Then the order of a/b modulo p divides 4 by Proposition 1.6.6. If this order were 1 or 2, then $(a/b)^2$ would be 1 modulo p, which is a contradiction, since $p > 2$, $-1 \not\equiv 1 \bmod p$. Altogether, the order of a/b is 4. On the other hand $p = 4k + 3$ for some $k \geqslant 0$. Therefore, the order of $\mathbf{Z}_p^\times$ is $4k + 2$, which is not divisible by 4, the order of a/b. Altogether this contradicts Lagrange's theorem (Theorem 1.6.4), therefore $b \not\equiv 0 \bmod p$ leads to a contradiction.

Then $b \equiv 0 \bmod p$, which implies $a \equiv 0 \bmod p$. □

Assume then $n = a^2 + b^2$ is divisible by $p \equiv -1 \bmod 4$. Then $p \mid a, b$. Therefore n is divisible by p^2, and $n/p^2 = (a/p)^2 + (b/p)^2$. This division by p^2 can be continued, if n/p^2 is still divisible by p. Altogether this yields that if n is the sum of two squares, then in its canonical form (1.2.1), each prime congruent to -1 modulo 4 occurs with even exponent.

Record the following trivial representations as the sum of two squares: $2 = 1^2 + 1^2$; and $p^2 = p^2 + 0^2$ for $p \equiv -1 \bmod 4$.

Proposition 3.1.9. *If $p \equiv 1 \bmod 4$, then -1 is a quadratic residue modulo p.*

Proof. By Proposition 1.6.10, there is a primitive root g modulo p. Then $g^{p-1} \equiv 1 \bmod p$, but $g^{(p-1)/2} \not\equiv 1 \bmod p$, therefore $g^{(p-1)/2} \equiv -1 \bmod p$. Consider then $a \equiv g^{(p-1)/4}$, then $a^2 \equiv g^{(p-1)/2} \equiv -1 \bmod p$. Altogether, we found a residue class a modulo p such that $a^2 \equiv -1 \bmod p$. □

Proposition 3.1.10. *If $p \equiv 1 \bmod 4$, then it can be represented as the sum of two squares.*

Proof. Combining 3.1.9 and Proposition 1.4.2, take an integer a satisfying $a^2+1 \equiv 0 \bmod p$ and $|a| < p/2$. Then considering the gaussian integer $\alpha = a + \sqrt{-1}$,

$$N(\alpha) = N(\overline{\alpha}) = a^2 + 1,$$

which, on the one hand, is divisible by p, and on the other hand, is at most $p^2/4 + 1 < p^2$. This means that $p \mid N(\alpha) = \alpha\overline{\alpha}$, but $p \nmid \alpha, \overline{\alpha}$ (because $N(p) = p^2$, $0 \neq N(\alpha), N(\overline{(\alpha)}) < p^2$). Altogether, p is not a prime in $\mathbf{Z}[i]$. Then it is not irreducible, so $p = \beta\gamma$, where none of β and γ is a unit. Now if any β or γ were of norm 1, then it would be any of $\pm 1, \pm\sqrt{-1}$, but these are units, a contradiction, altogether implying $N(\beta) = N(\gamma) = p$. Now p is a norm of a gaussian integer, hence it is the sum of two squares. □

Let us summarize: we proved that for n being representable as the sum of two squares, it must have each prime divisor being congruent to -1 modulo 4 on even power. Then we proved that 2, primes congruent to 1 modulo 4 and squares of primes congruent to -1 modulo 4 are all representable as the sum of two squares. Altogether, via Proposition 3.1.7, we arrive at the main result of this section (noting the trivial $1 = 1^2 + 0^2$).

Theorem 3.1.11. *A positive integer can be written as the sum of two squares if and only if in its canonical form (1.2.1), each prime congruent to -1 modulo 4 occurs with even exponent.* □

Problem 3.1.1. Prove that there are infinitely many prime numbers which are congruent to 1 modulo 4. Note that this is the case $q = 4$, $a = 1$ in Dirichlet's theorem. (*Hint:* prove that for $n \in \mathbf{N}$ the number $n^2 + 1$ has no prime divisor congruent to -1 modulo 4 (use Proposition 3.1.8 to see this). Now follow the earlier pattern: there are prime numbers $\equiv 1 \bmod 4$, e.g. $5, 13, 17$. Assume there are finitely many and denote their set by $\mathcal{P}$. Consider $A = (2\prod_{p\in\mathcal{P}} p)^2 + 1$, and show that each of its prime divisors is not 2, not $\equiv -1 \bmod 4$, so it must be $\equiv 1 \bmod 4$, hence listed in $\mathcal{P}$. On the other hand, A is coprime to everything listed in $\mathcal{P}$, a contradiction.)

Problem 3.1.2. Prove that there are infinitely many prime numbers which are congruent to 1 modulo 3. Note that this is the case $q = 3$, $a = 1$ in Dirichlet's theorem. (*Hint:* prove that for $n \in \mathbf{N}$ the number $n^2 + n + 1$ has no prime divisor congruent to -1 modulo 3 (modify the proof of Proposition 3.1.8 to see this). Now follow the earlier pattern: there are prime numbers $\equiv 1 \bmod 3$, e.g. $7, 13, 19$. Assume there are finitely many and denote their set by $\mathcal{P}$. Consider $A = (3\prod_{p\in\mathcal{P}} p)^2 + 3\prod_{p\in\mathcal{P}} p + 1$, and show that each of its prime divisors is not 3, not $\equiv -1 \bmod 3$, so it must be $\equiv 1 \bmod 3$, hence listed in $\mathcal{P}$. On the other hand, A is coprime to everything listed in $\mathcal{P}$, a contradiction.)

Problem 3.1.3.* Prove that for infinitely many $n \in \mathbf{N}$ such that $n^2 + 1$ has a prime divisor greater than $2n$.

Problem 3.1.4.* State and prove the fundamental theorem of arithmetic in the ring $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$.

3.2 Sum of four squares

In this section, in place of two squares, we use four, and prove that every positive integer can be written as the sum of four squares. As in the case of two squares, we start by a reduction step.

Proposition 3.2.1. *If two numbes can be written as the sum of four squares then so is their product.*

Proof. Let $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $n = y_1^2 + y_2^2 + y_3^2 + y_4^2$. Then one can easily check that

$$\begin{aligned} mn = &(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \\ &(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ &(x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + \\ &(x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned} \tag{3.2.1}$$

The proof is complete. □

In the case of two squares, we used complex numbers, which is a two-dimensional real algebra. This time, we will use a four-dimensional algebra, the quaternions.

Definition 3.2.2 (quaternions)**.** Introduce the symbols i, j, k, and let $\mathbf{H}$ be the algebra (a vector space which is further a ring) over $\mathbf{R}$ of basis $\{1, i, j, k\}$. That is, as a set,

$$\mathbf{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbf{R}\},$$

and addition is performed coordinatewise:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k.$$

As for multiplication, let $i^2 = j^2 = k^2 = -1$, and $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$, i.e.

$$\begin{aligned}(a + bi + cj + dk)(a' + b'i + c'j + d'k) =& (aa' - bb' - cc' - dd') \\ &+ (ab' + ba' + cd' - d'c)i \\ &+ (ac' + ca' - bd' + db')j \\ &+ (ad' + da' + bc' - cb')k.\end{aligned} \tag{3.2.2}$$

Then $\mathbf{H}$ is an associative algebra over $\mathbf{R}$. Unlike complex numbers, $\mathbf{H}$ is not commutative, consider for example $ij \neq ji$. However, if $r \in \mathbf{R}$, then for any $\alpha \in \mathbf{H}$, $r\alpha = \alpha r$, that is, $\mathbf{R}$ is in the center of $\mathbf{H}$ (in fact, one can easily check that $\mathbf{R}$ is the center of $\mathbf{H}$).

Definition 3.2.3 (conjugation)**.** For $\alpha = a + bi + cj + dk \in \mathbf{H}$, let its conjugate be $\overline{\alpha} = a - bi - cj - dk$.

Definition 3.2.4 (norm)**.** For $\alpha = a+bi+cj+dk \in \mathbf{H}$, let its norm be $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2+c^2+d^2 \in \mathbf{R}$.

Proposition 3.2.5. *For $\alpha, \beta \in \mathbf{H}$,*

$$\overline{\alpha} \cdot \overline{\beta} = \overline{\beta\alpha},$$

and

$$N(\alpha)N(\beta) = N(\alpha\beta).$$

Proof. The first statement is a simple calculation from (3.2.2). As for the second one,

$$N(\alpha)N(\beta) = \alpha\overline{\alpha}N(\beta) = \alpha N(\beta)\overline{\alpha} = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha\beta\overline{\alpha\beta} = N(\alpha\beta),$$

where we used that $N(\beta)$ is a real number, hence it commutes with $\overline{\alpha}$, and also the first statement. □

On this point, we see a profound source of the identity in Proposition 3.2.1. If $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $y = y_1^2 + y_2^2 + y_3^2 + y_4^2$, then consider the quaternions $\alpha = x_1 + x_2 i + x_3 j + x_4 k$, $\beta = y_1 + y_2 i + y_3 j + y_4 k$ with $N(\alpha) = m$ and $N(\beta) = n$. Now $N(mn)$ is the sum of four squares, and the expressions under the square in (3.2.1) are the real, i-, j- and k-part of $\alpha\beta$, respectively.

An important subring of $\mathbf{H}$ is the ring of so-called Hurwitz quaternions, namely

$$\mathcal{O} = \{a + bi + cj + dk \in \mathbf{H} : \text{either } a, b, c, d \in \mathbf{Z} \text{ or } a - 1/2, b - 1/2, c - 1/2, d - 1/2 \in \mathbf{Z}\}.$$

A crucial property of $\mathcal{O}$ is that $N(\mathcal{O}) \subseteq \mathbf{Z}$.

Proposition 3.2.6. *Every right ideal of $\mathcal{O}$ is principal.*

Proof. Assume I is a right ideal in $\mathcal{O}$. If $I = 0$, then it is obviously principal. If $I \neq 0$, then obviously there is an element $0 \neq \beta \in I$ of smallest norm. We claim that $\beta\mathcal{O} = I$. Assume not, and take an element $\alpha \in I \setminus \beta\mathcal{O}$. Take the quaternion $\gamma = \beta^{-1}\alpha \notin \mathcal{O}$.

We claim that there is a Hurwitz quaternion $\beta' \in \mathcal{O}$ such that $N(\beta' - \gamma) < 1$. To see this, first consider the point $\gamma = a + bi + cj + dk$ and the lattice $\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$, and choose $a' + b'i + c'j + d'k$ such that $|a - a'|, |b - b'|, |c - c'|, |d - d'| \leqslant 1/2$. Then the distance of γ and $a' + b'i + c'j + d'k$ is at most $\sqrt{4 \cdot 1/4} = 1$. In fact, it is strictly smaller than 1 (when we are done, as $\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k \subset \mathcal{O}$), since when $|a - a'| = |b - b'| = |c - c'| = |d - d'| = 1/4$, then $\gamma \in \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k + (1 + i + j + k)/2 \subset \mathcal{O}$, which is excluded.

Set then $\alpha' = \beta(\beta' - \gamma) = \beta(\beta' - \beta^{-1}\alpha) = \beta\beta' - \alpha$. First, $N(\alpha') = N(\beta)N(\beta' - \gamma) < N(\beta)$. Second, $\alpha' = \beta\beta' - \alpha \in I$, which contradicts the minimal choice (in norm) of β. □

Our next aim is to prove that any prime number is representable as the sum of four squares. Obviously, $2 = 1^2 + 1^2 + 0^2 + 0^2$, so from now on, fix a prime $p \geqslant 3$.

Proposition 3.2.7. *There exist integers $0 \leqslant x, y < p/2$ such that $x^2 + y^2 + 1 \equiv 0 \bmod p$.*

Proof. As x runs through the set $\{0, 1, \ldots, (p-1)/2\}$, x^2 runs through a set X of cardinality $(p+1)/2$ (since $x \mapsto x^2$ on $\mathbf{F}_p$ is injective apart from $x^2 \equiv (-x)^2 \bmod p$). The same way, as y runs through the set $-y^2 - 1$ runs through a set Y of cardinality $(p+1)/2$. Since $\mathbf{F}_p$ has p elements, by the pigeonhole principle, $X \cap Y \neq \emptyset$, that is, for well-chosen x, y, $x^2 \equiv -y^2 - 1 \bmod p$, that is, $x^2 + y^2 + 1 \equiv 0 \bmod p$. Obviously, if any of x and y is bigger than $p/2$, it can be replaced with its negative modulo p. □

Proposition 3.2.8. *There exists a Hurwitz quaternion $\beta = a + bi + cj + dk \in \mathcal{O}$ such that $N(\beta) = a^2 + b^2 + c^2 + d^2 = p$.*

Proof. Take $0 \leqslant x, y < p/2$ such that $x^2 + y^2 + 1 \equiv 0 \bmod p$, and consider the Hurwitz quaternion $\alpha = 1 + xi + yj$. Then $N(\alpha) = \alpha\overline{\alpha} = x^2 + y^2 + 1$, which is divisible by p. Consider the right ideal $I = p\mathcal{O} + \alpha\mathcal{O}$. Then $I = \beta\mathcal{O}$ for some $\beta \in \mathcal{O}$. Now $N(\beta) \mid N(p) = p^2$ and $N(\beta) \mid N(\alpha) < 2p^2/4 + 1 < p^2$. Therefore, $N(\beta)$ can be 1 or p.

If $N(\beta) = 1$, for some $\gamma, \delta \in \mathcal{O}$,

$$\beta = p\gamma + \alpha\delta.$$

Multiplying both sides by its conjugate, we obtain

$$1 = p^2 N(\gamma) + p(\gamma\overline{\alpha\delta} + \alpha\delta\overline{\gamma}) + N(\alpha)N(\delta).$$

Here, each side is an integer, but the right-hand side is divisible by p, while the left is not, a contradiction.

Therefore $N(\beta) = p$, that is, if $\beta = a + bi + cj + dk$, then $p = N(\beta) = a^2 + b^2 + c^2 + d^2$. □

Altogether, we represented p as a norm, the only problem is that it is over the Hurwitz quaternions. With the notation of the proof of Proposition 3.2.8, fix $\beta = a + bi + cj + dk$. If $a, b, c, d \in \mathbf{Z}$, then we are done, $p = a^2 + b^2 + c^2 + d^2$, where a, b, c, d are integers. Now assume we are in the opposite case, that is, a, b, c, d with $a, b, c, d \in \mathbf{Z} + 1/2$. Choose then $\omega = \pm 1/2 \pm i/2 \pm j/2 \pm k/2$ such that $\tau = \omega + \beta$ has even integer coordinates. Then $N(\omega) = 1$, and

$$p = \beta\overline{\beta} = (\tau - \omega)(\overline{\tau} - \overline{\omega}) = (\tau\overline{\omega} - 1)(\omega\overline{\tau} - 1) = N(\tau\overline{\omega} - 1).$$

Here, since τ has even coordinates, $\tau\overline{\omega} - 1$ has integer coordinates and its norm is still p.

Altogether, using Proposition 3.2.1, we obtain the main result of this section (noting the trivial $1 = 1^2 + 0^2 + 0^2 + 0^2$).

Theorem 3.2.9. *Every positive integer can be represented as the sum of four squares.* □

3.3 The geometry of numbers and two applications

In this section, we are going to give new proofs to the theorems on the sum of two (Theorem 3.1.11) and four squares (Theorem 3.2.9). In view of Proposition 3.1.7 and Proposition 3.2.1 (and the obvious representations of 1 and 2), it suffices to prove that prime numbers congruent to 1 modulo 4 are representable as the sum of two squares, and every odd prime number is representable as the sum of four squares. Our tool will be the following basic, yet powerful observation about the geometry of numbers.

Theorem 3.3.1 (Minkowski)**.** *Let Λ be a lattice in the d-dimensional euclidean space. Assume B is a compact, convex set which is further centrally symmetric with respect to the origin. If*

$$\mathrm{vol}(B) > 2^d \mathrm{covol}(\Lambda),$$

then $B \cap \Lambda$ contains a point other than the origin.

Proof. Fix P, a fundamental parallelepiped for the doubled lattice 2Λ, and let $f : B \to P$ be the map which sends each point of B to its equivalent in P (this is nothing else but cutting B by hyperplanes which are 2Λ-translates of the hyperfaces of P). Since

$$\mathrm{vol}(B) > 2^d \mathrm{covol}(\Lambda) = \mathrm{covol}(2\Lambda) = \mathrm{vol}(P),$$

f cannot be injective, that is, $f(a) = f(b)$ for some elements $a \neq b$ of B. Then for some $0 \neq \lambda \in 2\Lambda$, $a = b + \lambda$. By the central symmetry of B, this implies $-b \in B$, and then by the convexity of B,

$$B \ni \frac{1}{2}a + \frac{1}{2}(-b) = \frac{a-b}{2} = \frac{\lambda}{2} \in \Lambda.$$

The proof is complete. □

Another proof of Proposition 3.1.10. By Proposition 3.1.9, there exists an integer a such that $a^2 + 1$ is divisible by p. Consider the lattice

$$\Lambda = \mathbf{Z}(p, 0) + \mathbf{Z}(a, 1) \subseteq \mathbf{Z}^2 \subset \mathbf{R}^2.$$

Then

$$\mathrm{covol}(\Lambda) = \left| \det \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix} \right| = p.$$

Now let B be the ball centered at the origin of radius r satisfying

$$\frac{2}{\sqrt{\pi}}\sqrt{p} < r < \sqrt{2p},$$

which is possible, since $2/\sqrt{\pi} < \sqrt{2}$. By our lower bound on r and Theorem 3.3.1, there exists $(0, 0) \neq (b, c) \in B \cap \Lambda$. Since $(b, c) = \Lambda$, for some $k, l \in \mathbf{Z}$,

$$(b, c) = k(p, 0) + l(a, 1),$$

implying

$$b^2 + c^2 = (kp + la)^2 + l^2 \equiv l(a^2 + 1) \equiv 0 \bmod p,$$

by the choice of a. Also, since $(b, c) \in B \setminus \{(0, 0)\}$

$$0 < b^2 + c^2 \leqslant r^2 < 2p,$$

by the choice of r. Therefore, $b^2 + c^2 = p$, and the proof is complete. □

Proposition 3.3.2. *If $p > 2$ is a prime, then it can be represented as the sum of four squares.*

Proof. The proof is similar to the one above. First fix integers a, b satisfying that $a^2 + b^2 + 1$ is divisible by p (the existence of such integers follows from Proposition 3.2.7). Now consider the lattice

$$\Lambda = \mathbf{Z}(p, 0, 0, 0) + \mathbf{Z}(0, p, 0, 0) + \mathbf{Z}(a, b, 1, 0) + \mathbf{Z}(-b, a, 0, 1) \subseteq \mathbf{Z}^4 \subset \mathbf{R}^4.$$

This time,

$$\mathrm{covol}(\Lambda) = \left| \det \begin{pmatrix} p & 0 & a & -b \\ 0 & p & b & a \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right| = p^2$$

Let then B be the ball centered at the origin of radius r satisfying

$$\frac{2\sqrt[4]{2}}{\sqrt{\pi}}\sqrt{p} < r < \sqrt{2p},$$

which is possible, since $2\sqrt[4]{2}/\sqrt{\pi} < \sqrt{2}$. Using the fact that the 4-dimensional ball of radius R has volume $\pi^2 R^4/2$, by our lower bound on r and Theorem 3.3.1, there exists $(0, 0, 0, 0) \neq (c, d, e, f) \in B \cap \Lambda$. Since $(c, d, e, f) = \Lambda$, for some $k, l, m, n \in \mathbf{Z}$,

$$(c, d, e, f) = k(p, 0, 0, 0) + l(0, p, 0, 0) + m(a, b, 1, 0) + n(-b, a, 0, 1),$$

implying

$$c^2+d^2+e^2+f^2=(kp+ma-nb)^2+(lp+mb+na)^2+m^2+n^2\equiv(m^2+n^2)(a^2+b^2+1)\equiv 0 \bmod p,$$

by the choice of a, b. Also, since $(c,d,e,f)\in B\setminus\{(0,0,0,0)\}$

$$0<c^2+d^2+e^2+f^2\leqslant r^2<2p,$$

by the choice of r. Therefore, $c^2+d^2+e^2+f^2=p$, and the proof is complete. □

3.4 Minkowski's reduction theory

For $n\in\mathbf{N}$, denote by $\mathcal{P}_n$ the set of symmetric, positive definite $n\times n$ matrices over $\mathbf{R}$, i.e.

$$\mathcal{P}_n=\{A\in \mathrm{Mat}^{n\times n}(\mathbf{R}) : A^t=A \text{ and } x^tAx>0 \text{ for all nonzero } x\in\mathbf{R}^n\}.$$

On $\mathcal{P}_n$, $\mathrm{GL}_n(\mathbf{R})$ acts via the base change: for $g\in\mathrm{GL}_n(\mathbf{R})$ and $A\in\mathcal{P}_n$, $A\bullet g=g^tAg$, this is symmetric and positive definite again by the simple calculations

$$(A\bullet g)^t=(g^tAg)^t=g^tA^t(g^t)^t=g^tAg=A\bullet g,\qquad x^t(A\bullet g)x=x^tg^tAgx=(gx)^tA(gx),$$

and noting that $x\in\mathbf{R}^n$ is nonzero if and only if $gx\in\mathbf{R}^n$ is nonzero (since g is invertible).

For arithmetic, we will restrict to vectors of integer coordinates, i.e. to $x\in\mathbf{Z}^n$, and the group acting on them, i.e. $\mathrm{GL}_n(\mathbf{Z})$.

Definition 3.4.1. We say that $A,B\in\mathcal{P}_n$ are equivalent quadratic forms (over $\mathrm{GL}_n(\mathbf{Z})$), if for some $\gamma\in\mathrm{GL}_n(\mathbf{Z})$, $A\bullet\gamma=B$.

Proposition 3.4.2. *If $A,B\in\mathcal{P}_n$ are equivalent, then* $\det A=\det B$.

Proof. By definition, for some $\gamma\in\mathrm{GL}_n(\mathbf{Z})$, $\gamma^tA\gamma=B$, therefore $\det B=\det A(\det\gamma)^2$. As $\det\gamma=\pm1$, the proof is complete. □

Given a quadratic form represented by some matrix A, we would like to find another matrix which is equivalent to it and has a simpler form in some sense.

Theorem 3.4.3 (Hermite)**.** *For any $A\in\mathcal{P}_n$, we have*

$$0<m(A)=\min_{x\in\mathbf{Z}^n\setminus\{0\}}x^tAx\leqslant\left(\frac{4}{3}\right)^{(n-1)/2}(\det A)^{1/n}.$$

Proof. First, we know from linear algebra that for some orthogonal real matrix K, K^tAK is diagonal with positive entries (eigenvalues) $\rho_1\geqslant\ldots\geqslant\rho_n>0$. Then for any $x\in\mathbf{R}^n$,

$$x^tAx=(x^tK^{-t})(K^tAK)(K^{-1}x)\geqslant\rho_n\|K^{-1}x\|^2=\rho_n\|x\|^2.$$

This implies, on the one hand, that for any nonzero $x\in\mathbf{Z}^n$, $x^tAx\geqslant\rho_n$, as $\|x\|\geqslant1$ for vectors of integer coordinates. On the other hand, it implies that the minimum $m(A)$ exists. Indeed, set $e_1=(1,0,\ldots,0)^t$, and consider the integer vectors x satisfying $x^tAx\leqslant e_1^tAe_1$. For such vectors, as computed above, if $x^tAx\geqslant\rho_n\|x\|^2$, so $\|x\|^2\leqslant(e_1^tAe_1)\rho_n^{-1}$, hence only finitely many vectors x satisfy $x^tAx\leqslant e_1^tAe_1$, among them, there is a minimal positive value of x^tAx.

We prove the last statement by induction, it is obviously true for $n=1$. Now let $n\geqslant2$, assume the statement is true up to $n-1$, and let $A\in\mathcal{P}_n$. Set then $a_1=m(A)$, and let $x=(x_1,\ldots,x_n)^t\in\mathbf{Z}^n$ with $x^tAx=a_1$. Obviously, $\gcd(x_1,\ldots,x_n)=1$ (if it were bigger, say, $d>1$, then x/d would still be an integer vector, and $(x/d)^tA(x/d)=m(A)/d^2$, a contradiction). Now there is an integer matrix $\gamma\in\mathrm{GL}_n(\mathbf{Z})$ such that its first column is x, and then the matrix $B=\gamma^tA\gamma$ (which is equivalent to A) has upper-left entry a_1.

We have, for any integer vector $b \in \mathbf{R}^{n-1}$ and any matrix $A_1 \in \mathbf{R}^{n-1}$,

$$\begin{pmatrix} 1 & 0 \\ b & \mathrm{id}_{n-1} \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & A_1 \end{pmatrix} \begin{pmatrix} 1 & b^t \\ 0 & \mathrm{id}_{n-1} \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ ba_1 & A_1 \end{pmatrix} \begin{pmatrix} 1 & b^t \\ 0 & \mathrm{id}_{n-1} \end{pmatrix} = \begin{pmatrix} a_1 & a_1 b^t \\ ba_1 & ba_1 b^t + A_1, \end{pmatrix}$$

meaning that this is B for a well-chosen integer vector $b \in \mathbf{R}^{n-1}$ and a well-chosen matrix $A_1 \in \mathcal{P}_{n-1}$ (a_1 is already fixed, choose b adjusting to the upper-right block, then the bottom-left block is automatic from symmetry, finally adjust A_1 to the bottom-right block; the positivity of A_1 follows from the fact that $\left(\begin{smallmatrix} a_1 & 0 \\ 0 & A_1 \end{smallmatrix}\right)$ is equivalent to A). Now for any vector $y \in \mathbf{Z}^n$, we may decompose it as $(y_1, y_2) \in \mathbf{Z} \times \mathbf{Z}^{n-1}$, and then

$$\begin{aligned} y^t B y &= \begin{pmatrix} y_1 & y_2^t \end{pmatrix} \begin{pmatrix} a_1 & a_1 b^t \\ ba_1 & ba_1 b^t + A_1, \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 a_1 + y_2^t b a_1 & y_1 a_1 b^t + y_2^t b a_1 b^t + y_2^t A_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= a_1(y_1^2 + y_2^t b y_1 + y_1 b^t y_2 + y_2^t b b^t y_2) + y_2^t A_1 y_2 = a_1(y_1 + y_2^t b)^2 + y_2^t A_1 y_2. \end{aligned}$$

Now choose a nonzero y_2 such that $m(A_1) = y_2^t A_1 y_2$, and then y_1 such that $|y_1 + y_2^t b| \leqslant 1/2$. Then

$$a_1 \leqslant y^t B y \leqslant a_1/4 + m(A_1), \qquad a_1 \leqslant \frac{4}{3} m(A_1).$$

By induction,

$$m(A_1) \leqslant \left(\frac{4}{3}\right)^{(n-2)/2} (\det A_1)^{1/(n-1)},$$

and using $a_1 \det A_1 = \det A$, we have

$$a_1 \leqslant \left(\frac{4}{3}\right)^{n/2} \frac{(\det A)^{1/(n-1)}}{a_1^{1/(n-1)}}, \qquad a_1^{n/(n-1)} \leqslant \left(\frac{4}{3}\right)^{n/2} (\det A)^{1/(n-1)}.$$

Raising to the $(n-1)/n$th power, the proof is complete. □

Definition 3.4.4 (Minkowski reduced form)**.** We say that a matrix $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{P}_n$ is Minkowski reduced (or reduced in short), if $x^t A x \geqslant a_{k,k}$ for any vector $x = (x_1, \ldots, x_n) \in \mathbf{Z}^n$ satisfying $\gcd(x_k, \ldots, x_n) = 1$ (which automatically implies $x \neq 0$), and $a_{k,k+1} \geqslant 0$ for all $1 \leqslant k \leqslant n-1$.

Theorem 3.4.5. *In any equivalence class, there exists a matrix of Minkowski reduced form. In other words, for any $A \in \mathcal{P}_n$, there exists $\gamma \in \mathrm{GL}_n(\mathbf{Z})$ such that $A \bullet \gamma$ is Minkowski reduced.*

Proof. The proof of Theorem 3.4.3, converted into an algorithm, gives such a matrix. Set first $A_0 = A$, then take a matrix $\gamma_1 \in \mathrm{GL}_n(\mathbf{Z})$ such that the upper-left entry of $A_1 = \gamma_1^t A \gamma_1$ is minimal. Then in the kth step, we use a matrix $\gamma_k = \left(\begin{smallmatrix} \mathrm{id}_k & * \\ 0 & * \end{smallmatrix}\right)$ such that the kth diagonal entry of $A_k = \gamma_k^t A_{k-1} \gamma_k$ is minimal. Altogether this algorithm gives a matrix $A_n = B = (b_{i,j})_{1 \leqslant i,j \leqslant n}$ equivalent to A (in other words, we made an integer base change), now we prove it satisfies the first requirement of being reduced.

The operation $(\cdot) \bullet \gamma_k$ leaves the upper-left $(k-1) \times (k-1)$ minor invariant. This means that the first $k-1$ basis vectors (of the basis in which we rewrote the quadratic form represented by A) were determined by $\gamma_1, \ldots, \gamma_{k-1}$ for any $2 \leqslant k \leqslant n$.

Then for any vector $x = (x_1, \ldots, x_n) \in \mathbf{Z}^n$ and any $1 \leqslant k \leqslant n$, if $\gcd(x_k, \ldots, x_n) = 1$, then x is linearly independent of the first $k-1$ basis vectors, that is, x was taken into account when we took the minimum in the kth step. This means $x^t B x \geqslant b_{k,k}$.

As for the second requirement, i.e. the close-to-diagonal entries are nonnegative, we record that $(\cdot) \bullet E_k$ (where E_k is a diagonal matrix with -1 in position k and 1's otherwise) multiplies both the kth row and the kth column by -1 (in particular, it does not alter the diagonal entry). This operation does not affect the first requirement. This means that the above B can further be transformed to a Minkowski reduced matrix. □

Proposition 3.4.6. *If $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{P}_n$ is a Minkowski reduced matrix, then*

(a) $0 < a_{1,1} \leqslant \ldots \leqslant a_{n,n}$;

(b) $2|a_{k,l}| \leqslant \min(a_{k,k}, a_{l,l})$ *for any* $1 \leqslant k < l \leqslant n$.

Proof. Let $e_k = (0, \dots, 0, 1, 0, \dots, 0)^t$ be the unit vector with the 1 at position k.

(a) We know that $a_{k,k} \leqslant e_{k+1}^t A e_{k+1} = a_{k+1,k+1}$ for any $1 \leqslant k \leqslant n-1$. Also, $0 < e_1^t A e_1 = a_{1,1}$.

(b) For any $1 \leqslant k < l \leqslant n$, we have $a_{l,l} \leqslant (e_k \pm e_l)^t A (e_k \pm e_l) = a_{k,k} \pm 2a_{k,l} + a_{l,l}$. □

Definition 3.4.7 (discriminant of a binary quadratic form)**.** Given a quadratic form represented by a matrix A, its discriminant is $-4 \det A$.

Recalling Proposition 3.4.2, we see that the discriminant of a quadratic form does not depend on the representing matrix, only on its equivalence class.

We conclude this section by an application of Minkowski's reduction theory, proving that for any given discriminant, there are only finitely many equivalence classes of positive definite, integer, binary quadratic forms.

Proposition 3.4.8 (finiteness of the class number)**.** *Let $D < 0$ be fixed. There exists a finite collection of matrices $\gamma_1, \dots, \gamma_k \in \mathcal{P}_2 \cap \mathrm{Mat}^{2\times 2}(\mathbf{Z})$ of discriminant D such that any $\gamma \in \mathcal{P}_2 \cap \mathrm{Mat}^{2\times 2}(\mathbf{Z})$ of discriminant D is equivalent to some γ_j with $1 \leqslant j \leqslant k$.*

Proof. Let $R(D)$ be the set of integer matrices of discriminant D in $\mathcal{P}_2$ which are Minkowski reduced. By Theorem 3.4.5, it suffices to show that $R(D)$ is finite (since in each equivalence class, there is a Minkowski reduced matrix).

Consider the matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \in R(D).$$

Then $a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = -D/4 > 0$, and since $0 \leqslant a_{1,2} = a_{2,1} \leqslant \min(a_{1,1}, a_{2,2})/2$, $0 < a_{1,1}a_{2,2} \leqslant -D/3$. Obviously, there are finitely many such choices for the diagonal entries $a_{1,1}, a_{2,2}$. Then by $0 \leqslant a_{1,2} = a_{2,1} \leqslant a_{1,1}/2$, there are finitely many choices for the nondiagonal entries. □

3.5 Sum of three squares

Earlier in this chapter, we described the positive integers that can be written as the sum of two and four squares. Now we work out the the problem of three squares.

Proposition 3.5.1. *If a positive integer is of the form $n = 4^m(8k+7)$ for some nonnegative integers m, k, then it cannot be represented as the sum of three squares.*

Proof. We prove by induction on m. For $m = 0$, $n = 8k + 7$. The squares modulo 8 have residue $0, 1, 4$. One can easily check that three of these do not sum up to 7 modulo 8.

Now let $m \geqslant 1$, and assume the statement holds for any $m' \leqslant m - 1$. By contradiction, assume

$$n = 4^m(8k+7) = x^2 + y^2 + z^2$$

for some integers $x, y, z \in \mathbf{Z}$. Considering this modulo 4, we see that none of x, y, z can be odd (since squares modulo 4 have residue $0, 1$). Then

$$n/4 = 4^{m-1}(8k+7) = (x/2)^2 + (y/2)^2 + (z/2)^2.$$

But this is a contradiction by the induction hypothesis. □

The main goal is to prove the converse.

Proposition 3.5.2. *Assume that for some $n \in \mathbf{N}$, the symmetric integer matrix*

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{2,1} & a_{2,2} & 0 \\ 1 & 0 & n \end{pmatrix}$$

satisifies

$$d_1 = a_{1,1} > 0, \qquad d_2 = a_{1,1}a_{2,2} - a_{1,2}a_{2,1} > 0, \qquad d_3 = d_2 n - a_{2,2} = 1. \tag{3.5.1}$$

Then A is equivalent to the identity matrix (in the sense of Section 3.4).

Proof. We know from linear algebra that A is positive definite (since all the upper-left minors have positive determinant). Let

$$\begin{pmatrix} r_{1,1} & r_{1,2} & r_{1,3} \\ r_{2,1} & r_{2,2} & r_{2,3} \\ r_{3,1} & r_{3,2} & r_{3,3} \end{pmatrix}$$

be the Minkowski reduced matrix constructed in the proof of Theorem 3.4.5. From the algorithm given there, it follows that

$$r_{1,1} = m(A) \leqslant \frac{4}{3},$$

by the notation and the statement of Theorem 3.4.3. Since $m(A)$ is an integer, $r_{1,1} = m(A) = 1$. Then by Proposition 3.4.6, $r_{1,2} = r_{2,1} = r_{1,3} = r_{3,1} = 0$. By the same argument applied to the bottom-right 2×2 block, we obtain $r_{2,2} = 1$, $r_{2,3} = r_{3,2} = 0$. Then since $d_3 = 1$, $r_{3,3} = 1$. □

Proposition 3.5.3. *Assume $n \equiv 2, 6 \bmod 8$. Then there exist integers $a_{1,1}, a_{1,2} = a_{2,1}, a_{2,2}$ satisfying (3.5.1).*

Proof. By Dirichlet's theorem (Theorem 2.1.3), there exist an integer $m > 0$ such that $4nm + (n-1) = p$ is a prime (using that $4n$ and $n-1$ are coprime). Set then $d_2 = 4m + 1$ and $d_2 = \prod_{j=1}^{r} q_j^{\alpha_j}$ for its canonical form (1.2.1) (note that each q_j is odd). Then we have, from Theorem 1.7.6,

$$\left(\frac{-d_2}{p}\right) = \left(\frac{d_2}{p}\right) = \prod_{j=1}^{r} \left(\frac{q_j}{p}\right)^{\alpha_j} = \prod_{j=1}^{r} \left(\frac{p}{q_j}\right)^{\alpha_j} = \prod_{j=1}^{r} \left(\frac{d_2 n - 1}{q_j}\right)^{\alpha_j} = \prod_{j=1}^{r} \left(\frac{-1}{q_j}\right)^{\alpha_j} = 1,$$

where we used also Corollary 1.7.3; that -1 is a quadratic resiude modulo primes congruent to 1 modulo 4 (which follows simply from Proposition 1.6.10) and is a quadratic non-residue modulo primes congruent to -1 modulo 4 (which we have already seen in the proof of Proposition 3.1.8); and that d_2 has even many prime divisors congruent to -1 modulo 4 (when counted with multiplicity).

Now let $a_{2,2} = d_2 n - 1 = p$, and choose $a_{1,2} = a_{2,1}$ such that $a_{1,2}^2 \equiv -d_2 \bmod p$. Finally, let $a_{1,1} = (d_2 + a_{1,2}^2)/a_{2,2}$, which is clearly an integer. Then all the requirement imposed in (3.5.1) are fulfilled. □

Proposition 3.5.4. *Assume $n \equiv 1, 3, 5 \bmod 8$. Then there exist integers $a_{1,1}, a_{1,2} = a_{2,1}, a_{2,2}$ satisfying (3.5.1).*

Proof. Choose $c \in \{1, 3\}$ as follows: if $n \equiv 1, 5 \bmod 8$, then let $c = 3$, if $n \equiv 3 \bmod 8$, then let $c = 1$. Apply again Dirichlet's theorem (Theorem 2.1.3) (using that $4n$ and $(cn-1)/2$ are coprime) to get an integer $m > 0$ such that $4nm + (cn-1)/2 = p$ is a prime. Let now $d_2 = 8m + c$.

Then we have $2p = 8mn + cn - 1 = (8m + c)n - 1 = d_2 n - 1$. Similar calculations to the above one (using also Corollary 1.7.5 and Corollary 1.7.8) lead in each case to that $-d_2$ is a quadratic residue modulo p.

First, when $n \equiv 1 \bmod 8$, then $d_2 \equiv c = 3 \bmod 8$ (this gives $\left(\frac{-2}{d_2}\right) = 1$), and $p \equiv (3n-1)/2 \equiv 1 \bmod 4$. Then

$$\left(\frac{-d_2}{p}\right) = \left(\frac{d_2}{p}\right)\left(\frac{-2}{d_2}\right) = \left(\frac{p}{d_2}\right)\left(\frac{-2}{d_2}\right) = \left(\frac{-2p}{d_2}\right) = \left(\frac{1 - d_2 n}{d_2}\right) = 1.$$

Second, when $n \equiv 3 \bmod 8$, then $d_2 \equiv c = 1 \bmod 8$ (this gives $\left(\frac{-2}{d_2}\right) = 1$), and $p \equiv (n-1)/2 \equiv 1 \bmod 4$. Then

$$\left(\frac{-d_2}{p}\right) = \left(\frac{d_2}{p}\right)\left(\frac{-2}{d_2}\right) = \left(\frac{p}{d_2}\right)\left(\frac{-2}{d_2}\right) = \left(\frac{-2p}{d_2}\right) = \left(\frac{1 - d_2 n}{d_2}\right) = 1.$$

Third, when $n \equiv 5 \bmod 8$, then $d_2 \equiv c = 3 \bmod 8$ (this gives $\left(\frac{-2}{d_2}\right) = 1$), and $p \equiv (3n-1)/2 \equiv -1 \bmod 4$. Then

$$\left(\frac{-d_2}{p}\right) = -\left(\frac{d_2}{p}\right)\left(\frac{-2}{d_2}\right) = \left(\frac{p}{d_2}\right)\left(\frac{-2}{d_2}\right) = \left(\frac{-2p}{d_2}\right) = \left(\frac{1 - d_2 n}{d_2}\right) = 1.$$

Also, $-d_2$ is odd, therefore it is a square not only modulo p, but modulo $2p$ as well (assume $x^2 \equiv (p-x)^2 \equiv -d_2 \bmod p$, then choose out of x and $p - x$ the odd one: its square is odd and congruent to $-d_2$ modulo p, so it is $-d_2$ modulo $2p$).

We complete the proof as above: choose $a_{2,2} = 2p$, then $a_{1,2} = a_{2,1}$ such that $d_2 + a_{1,2}^2$ is divisible by $a_{2,2}$, then $a_{1,1} = (d_2 + a_{1,2}^2)/a_{2,2}$. □

That is, for a given $n \equiv 1, 2, 3, 5, 6 \bmod 8$, by Proposition 3.5.3 and Proposition 3.5.4, there exists a symmetric, positive definite matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{2,1} & a_{2,2} & 0 \\ 1 & 0 & n \end{pmatrix}$$

satisfying (3.5.1). It is easy to see that

$$\begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{2,1} & a_{2,2} & 0 \\ 1 & 0 & n \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = n.$$

Also, by Proposition 3.5.2, there is a matrix $\gamma \in \mathrm{GL}_3(\mathbf{Z})$ such that $\gamma^t A \gamma$ is the identity. Then setting $\gamma^{-1} \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}^t = \begin{pmatrix} x & y & z \end{pmatrix}^t$, we obtain

$$n = \left(\begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \gamma^{-t} \right) (\gamma^t A \gamma) \left(\gamma^{-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} x & y & z \end{pmatrix} \mathrm{id}_3 \begin{pmatrix} x \\ y \\ z \end{pmatrix} = x^2 + y^2 + z^2,$$

showing that any number congruent to $1, 2, 3, 5, 6$ modulo 8 is representable as the sum of three squares.

Now if n is of the form $4^m(8k + a)$ for some $a \in \{1, 2, 3, 5, 6\}$, represent $8k + a$ as $x^2 + y^2 + z^2$, then

$$n = (2^m x)^2 + (2^m y)^2 + (2^m z)^2.$$

Altogether, we arrive at the main result of this section.

Theorem 3.5.5. *A positive integer is representable as the sum of three squares if and only if it is not of the form $4^m(8k + 7)$ $(m, k \in \mathbf{Z})$.* □

Chapter 4
The proof of Dirichlet's theorem

In this chapter, we give a complex-analytic proof of Dirichlet's theorem (Theorem 2.1.3) claiming that for any $a, q \in \mathbf{N}$ satisfying $\gcd(a, q) = 1$, there are infinitely many primes $p \equiv a \bmod q$.

4.1 Facts from complex analysis

This section is a collection of complex-analytic facts usually covered in a first-semester course on complex analysis.

Definition 4.1.1 (complex derivation)**.** Assume $D \subseteq \mathbf{C}$ is an open, connected domain of the complex plane. We say that a function $f : D \to \mathbf{C}$ is differentiable at a point $z_0 \in D$ and its derivative is $f'(z_0) \in \mathbf{C}$, if

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

We say that f is holomorphic on the domain D, if it is differentiable at each point of D.

In what follows, D will always stand for an open, connected subset of $\mathbf{C}$.

Fact 4.1.2 (differentiable functions are analytic)**.** *Assume $f : D \to \mathbf{C}$ is differentiable. Then for any $z_0 \in D$, f can be expanded into Taylor series around z_0:*

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n.$$

This expansion is valid on any disc B centered at z_0 which is contained in D.

Moreover, on B, we can compute the derivatives as the formal derivatives of the power series, i.e. f is differentiable infinitely many times, and

$$f^{(k)}(z) = \sum_{n=k}^{\infty} n \cdot \ldots \cdot (n - k + 1) a_n (z - z_0)^{n-k}.$$

for any $k \in \mathbf{N} \cup \{0\}$. The coefficients in the Taylor expansion are connected with the derivatives of f at z_0:

$$f^{(k)}(z_0) = k! a_k.$$

Definition 4.1.3. Given a sequence of functions $f_n : D \to \mathbf{C}$ and one more function $f : D \to \mathbf{C}$. We say that f_n converges to f locally uniformly, if the following holds. For any compact $C \subset D$, and any $\varepsilon > 0$, there exists $n_0 = n_0(C, \varepsilon)$ such that

$$|f_n(z) - f(z)| < \varepsilon, \text{ if } z \in C \text{ and } n > n_0.$$

Fact 4.1.4. *Assume the sequence (f_n) of holomorphic functions $f_n : D \to \mathbf{C}$ converges locally uniformly to a function f. Then f is holomorphic, and for any $z \in D$, $k \in \mathbf{N} \cup \{0\}$,*

$$f^{(k)}(z) = \lim_{n \to \infty} f_n^{(k)}(z).$$

Definition 4.1.5 (poles)**.** Assume $z_0 \in D$ and $f : D \setminus \{z_0\} \to \mathbf{C}$ is holomorphic. If there is a disc B centered at z_0 and contained in D such that for $z \in B \setminus \{z_0\}$,

$$f(z) = \sum_{n=-m}^{\infty} a_n (z - z_0)^n = \frac{a_m}{(z - z_0)^m} + \ldots + \frac{a_{-1}}{z - z_0} + \text{holomorphic}$$

with some positive integer m and complex numbers a_n for $n \geqslant -m$ (where m is chosen to be minimal with this property, i.e. $a_{-m} \neq 0$), then we say that f has a pole at z_0 of order m.

Example 4.1.6. The reciprocal function $z \mapsto z^{-1}$ has a pole of order 1 at 0, since

$$z^{-1} = \frac{1}{z} + 0 = \frac{1}{z} + \text{holomorphic}.$$

Definition 4.1.7 (meromorphic functions)**.** Assume D is an open, connected domain as above, and E is a discrete subset of D. Then a function $f : D \setminus E \to \mathbf{C}$ is said to be meromorphic on D, if it is holomorphic on $D \setminus E$, and at each point of E, it has a pole.

At the exceptional points (where we have a pole), we can think of the functions as taking the value infinity, so in fact, meromorphic functions are understood as functions from D to $\overline{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$.

Fact 4.1.8. *Given a domain D, its meromorphic functions form a field with respect to pointwise addition and multiplication.*

Remark 4.1.9. This fact includes the notion of (analytic) continuation, by which we mean the following. Assume f is holomorphic in a neighborhood of z_0 and it is bounded there. Then $\lim_{z \to z_0} f(z)$ exists, and we can define $f(z_0)$ to be $\lim_{z \to z_0} f(z)$, the resulting (analytically continued) f is holomorphic in a neighborhood of z_0.

Example 4.1.10. Let $D = \mathbf{C}$. If $f(z) = z^{-1}$, $g(z) = z$, then $(fg)(z) = 1$, first only for $z \neq 0$, but then also for $z = 0$ by continuation.

Example 4.1.11. Let $D = \mathbf{C}$. If $f(z) = z^{-1}$, $g(z) = -z^{-1}$, then $(f + g)(z) = 0$, first only for $z \neq 0$, but then also for $z = 0$ by continuation.

Remark 4.1.12. Analytic continuation can be understood in a broader sense, we usually mean by that the replacing of a function by another one, which makes sense on a larger domain. Consider for example $f(z) = 1 + z + z^2 + \ldots$, a holomorphic function on the domain $\{z : |z| < 1\}$. We know very well that for $|z| < 1$, $f(z) = 1/(1 - z)$. That is, we can continue analytically f to the domain $\mathbf{C} \setminus \{1\}$ by setting f to be $1/(1 - z)$: it keeps the original value where there was an original value at all, and it is holomorphic everywhere (where it is defined).

Definition 4.1.13. For $z \in \mathbf{C}$, we define

$$\exp(z) = e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}, \qquad \cos z = \sum_{n=0}^{\infty} (-1)^n \frac{z^n}{(2n)!}, \qquad \sin z = \sum_{n=0}^{\infty} (-1)^n \frac{z^n}{(2n+1)!}.$$

Fact 4.1.14. *The functions $e^z, \cos z, \sin z$ are holomorphic on $\mathbf{C}$, and they are connected by the formula*

$$e^{iz} = \cos z + i \sin z.$$

Restricting to the real line, they coincide with the real exponential, cosine and sine functions, respectively.

As a consequence, $|e^z| = e^{\Re z}$, since the imaginary part of z only rotates around the origin by the angle $\Im z$.

For the purpose of Dirichlet's theorem, we do not need to understand the logarithm function (the inverse of exponental) completely (which would be a subtle thing in general), but we have to define it for positive real numbers. This is easy to do: for $z \in \mathbf{R}^+$, let $\log z$ be the real logarithm of z.

4.2 Dirichlet series

Definition 4.2.1 (complex powers of positive real numbers)**.** For $x > 0$ and $s \in \mathbf{C}$, let

$$x^s = e^{s \log x}.$$

Definition 4.2.2 (Dirichlet series)**.** Let (a_n) be a sequence of complex numbers (as n runs through $\mathbf{N}$). Then the attached Dirichlet series $D_{(a_n)}$ is defined as

$$D_{(a_n)}(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

A priori this is only a formal definition, but if the given series is convergent for some $s \in \mathbf{C}$, then $D_{(a_n)}$ is considered as a complex function mapping s to $D_{(a_n)}(s)$. Now we turn to the issue of the convergence domain.

Proposition 4.2.3. *Assume $D_{(a_n)}$ is convergent for some $s_0 \in \mathbf{C}$. Then for any s satisfying $\Re s > \Re s_0$, $D_{(a_n)}(s)$ is convergent. Moreover, the sequence of partial sums*

$$\sum_{n=1}^{N} a_n n^{-s}$$

converges locally uniformly on $\{s : \Re s > \Re s_0\}$ to $D_{(a_n)}(s)$ as $N \to \infty$.

Proof. Let C be any compact subset of the half-plane $\{s : \Re s > \Re s_0\}$. First take an angular sector starting from s_0 that contains C, i.e. take some $H \in \mathbf{N}$ such that for any $s \in C$,

$$\left| \frac{\Im s - \Im s_0}{\Re s - \Re s_0} \right| < H.$$

Let further $\varepsilon > 0$ be given, we have to check the uniform convergence for the input C, ε.

Take any $s \in C$, we would like to use Cauchy's convergence criterion. For any natural numbers $M < N$,

$$\sum_{n=1}^{N} a_n n^{-s} - \sum_{n=1}^{M} a_n n^{-s} = \sum_{n=M+1}^{N} a_n n^{-s}.$$

Set, for any $u \in \mathbf{N}$,

$$R(u) = \sum_{n=u+1}^{\infty} n^{-s_0},$$

this tends to zero, as u tends to infinity, since $D_{(a_n)}$ is convergent at s_0. Using this notation, we have $a_n n^{-s} = (R(n-1) - R(n)) n^{s_0 - s}$. Then

$$\begin{aligned} \sum_{n=M+1}^{N} a_n n^{-s} &= \sum_{n=M+1}^{N} (R(n-1) - R(n)) n^{s_0 - s} \\ &= \sum_{n=M+1}^{N} R(n-1)(n^{s_0-s} - (n-1)^{s_0-s}) + R(M) M^{s_0-s} - R(N) N^{s_0-s}. \end{aligned}$$

Now if M, N are large enough, then $R(u) < \varepsilon$ for $u \geqslant M$, so

$$\left| \sum_{n=M+1}^{N} a_n n^{-s} \right| \leqslant \varepsilon \sum_{n=M+1}^{N} \left| n^{s_0-s} - (n-1)^{s_0-s} \right| + 2\varepsilon.$$

Now observe that

$$n^{s_0-s} - (n-1)^{s_0-s} = (s_0 - s) \int_{n-1}^{n} z^{s_0-s-1} dz$$

by Newton-Leibniz formula, and taking absolute values,

$$\left|n^{s_0-s}-(n-1)^{s_0-s}\right| \leqslant |s_0-s| \int_{n-1}^{n} z^{\Re s_0-\Re s-1}dz,$$

therefore

$$\begin{aligned}\sum_{n=M+1}^{N} \left|n^{s_0-s}-(n-1)^{s_0-s}\right| &\leqslant |s_0-s| \int_{M}^{N} z^{\Re s_0-\Re s-1}dz \\ &\leqslant \frac{|s_0-s|}{|\Re s_0-\Re s|} \leqslant \frac{|\Re s_0-\Re s|+|\Im s_0-\Im s|}{|\Re s_0-\Re s|} < H+1.\end{aligned}$$

Altogether,

$$\left|\sum_{n=M+1}^{N} a_n n^{-s}\right| < (H+3)\varepsilon,$$

and the proof is complete. □

Therefore, given a Dirichlet series $D_{(a_n)}$, its convergence domain is a half-plane $\{s : \Re s > \sigma_0\}$, where

$$\sigma_0 = \inf\{\Re s : D_{(a_n)} \text{ is convergent at } s.\}$$

On the open half-plane, the derivatives of $D_{(a_n)}$ can be computed formally as

$$D^{(k)}_{(a_n)}(s) = \sum_{n=1}^{\infty} a_n (n^{-s})^{(k)} = \sum_{n=1}^{\infty} a_n (-\log n)^k n^{-s}. \tag{4.2.1}$$

Theorem 4.2.4 (Landau)**.** *Assume the coefficient sequence (a_n) consists of nonnegative real numbers. If the real boundary point of the convergence domain is σ_0, then $D_{(a_n)}$ cannot be continued holomorphically to any neighborhood of σ_0.*

Proof. First of all, we rescale the coefficients as follows:

$$\sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} a_n n^{-\sigma_0} n^{-(s-\sigma_0)} = \sum_{n=1}^{\infty} b_n n^{-(s-\sigma_0)},$$

where $b_n = a_n n^{-\sigma_0} \geqslant 0$. From this, we see that $D_{(a_n)}$ is convergent at s if and only if $D_{(b_n)}$ is convergent at $s-\sigma_0$. By this observation, we may assume that $\sigma_0 = 0$, and our aim is to prove that $D_{(a_n)}(s)$, as a complex function on $\{s : \Re s > 0\}$, cannot be continued to any neighborhood of 0.

We prove by contradiction: assume there exists a neighborhood of 0, where $D_{(a_n)}$ can be continued to. Draw then an open disc centered at 1 of radius bigger than 1 on which the continuation $\widetilde{D}$ is holomorphic, and let $-\delta < 0$ be a real point of this disc.

From Taylor expansion, we have

$$\widetilde{D}(-\delta) = \sum_{k=0}^{\infty} c_k (-\delta-1)^k,$$

where

$$c_k = \frac{\widetilde{D}^k(1)}{k!} = \frac{D^k_{(a_n)}(1)}{k!} = \sum_{n=1}^{\infty} \frac{a_n(-\log n)^k}{nk!}.$$

Then

$$\widetilde{D}(-\delta) = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n((\log n)(1+\delta))^k}{nk!}.$$

Here the numbers in the double summation are nonnegative reals, so we may change the order of summation:

$$\widetilde{D}(-\delta) = \sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{k=0}^{\infty} \frac{((\log n)(1+\delta))^k}{k!} = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{(\log n)(1+\delta)} = \sum_{n=1}^{\infty} \frac{a_n}{n} n^{1+\delta} = \sum_{n=1}^{\infty} a_n n^{\delta}.$$

Here, the left-hand side is a finite number, so is the right-hand side. This means that the Dirichlet series $D_{(a_n)}$ itself is convergent at $-\delta$, which contradicts the assumption that 0 is a boundary point of the convergence half-plane. □

Problem 4.2.1. Let f, g be number-theoretic functions. To them, we may attach Dirichlet series $D_f(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$, $D_g(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$. Assume the Dirichlet series defining D_f, D_g are absolutely convergent for some $s \in \mathbf{C}$. Prove then that $D_f(s)D_g(s) = D_{f*g}(s)$, where D_{f*g} is the Dirichlet series attached to the convolution $f * g$, and it is absolutely convergent at the same $s \in \mathbf{C}$ as before. (*Hint:* write down $D_f(s), D_g(s)$ explicitly, take their product and in

$$\sum_{m=1} f(m)m^{-s} \sum_{n=1} g(n)n^{-s} = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} f(m)g(n)(mn)^{-s},$$

group the terms according to the value of mn.)

4.3 Dirichlet characters

Definition 4.3.1 (Dirichlet character)**.** Given a modulus $q \in \mathbf{N}$, we say a function $\chi : \mathbf{Z} \to \mathbf{C}$ is a Dirichlet character, if

(a) for any $n \in \mathbf{Z}$, $\chi(n+q) = \chi(n)$;

(b) for any $n \in \mathbf{Z}$, $\chi(n) \neq 0$ if and only if $\gcd(n, q) = 1$;

(c) for any $m, n \in \mathbf{Z}$, $\chi(mn) = \chi(m)\chi(n)$.

Proposition 4.3.2 (properties of Dirichlet character)**.** *Dirichlet characters of modulo q have the following properties.*

(a) The function χ can be considered as a function $\mathbf{Z}_q \to \mathbf{C}$.

(b) The function χ is a group homomorphism from $\mathbf{Z}_q^\times$ to the multiplicative group of $\varphi(q)$th roots of unity.

Proof. (a) This is obvious from the fact that χ has period q.

(b) By multiplicativity $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$, which implies $\chi(1) = 1$, since $\chi(1) = 0$ is excluded by $\gcd(1, q) = 1$. The fact that χ is a group homomorphism is a simple consequence of multiplicativity. Assume $a \in \mathbf{Z}_q^\times$. Then by Euler-Fermat (Corollary 1.6.8), and by iterating the multiplicaticity of χ,

$$(\chi(a))^{\varphi(q)} = \chi(a^{\varphi(q)}) = \chi(1) = 1,$$

which means that $\chi(a)$ is indeed a $\varphi(q)$th root of unity. □

Proposition 4.3.3 (the group of Dirichlet characters)**.** *The Dirichlet characters of modulo q form a group under pointwise multiplication. The unit element is the principal character*

$$\chi_0(a) = \begin{cases} 1 & \text{if } \gcd(a, q) = 1, \\ 0 & \text{if } \gcd(a, q) = 0; \end{cases}$$

and the inverse χ^{-1} of χ is the complex conjugate character

$$\chi^{-1}(a) = \overline{\chi(a)}.$$

The group Ξ of characters has $\varphi(q)$ elements, and it is isomorphic to the group $\mathbf{Z}_q^\times$.

Proof. The group properties (multiplication, unit element, inverse) follow easily. As for the structure of Ξ, recall that

$$\mathbf{Z}_q^\times = C_{q_1} \times \ldots \times C_{q_r}$$

for some cyclic groups $C_{q_1}, \ldots, C_{q_r}$ of order $q_1, \ldots, q_r$, respectively, satisfying $q_1 \cdot \ldots \cdot q_r = \varphi(q)$ (recall Section 1.6). Take some generators $c_1, \ldots, c_r$ of $C_{q_1}, \ldots, C_{q_r}$. Then a $\chi \in \Xi$ is determined by its values on $c_1, \ldots, c_r$, which must be q_1th, …, q_rth roots of unity, respectively. From this, both the order and the structure of Ξ are clear. □

Remark 4.3.4. More generally, for any finite abelian group G, its dual group $\widehat{G}$ is isomorphic to G. Note on the other hand that this isomorphism is not canonical (in the sense of universal algebra), since it depends on the generators of the cyclic parts. The proof of the general statement is the same, starting out from the fundamental theorem of finite abelian groups.

Proposition 4.3.5. *For any $n \in \mathbf{Z}$,*

$$\frac{1}{\varphi(q)} \sum_{\chi \in \Xi} \chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod q; \\ 0 & \text{if } n \not\equiv 1 \bmod q. \end{cases}$$

Proof. If $n \equiv 1 \bmod q$ or if $\gcd(n, q) \neq 1$, then the statement trivially holds. Assume that $\gcd(n, q) = 1$ and $n \not\equiv 1 \bmod q$. When writing

$$\mathbf{Z}_q^\times = C_{q_1} \times \ldots \times C_{q_r},$$

and taking the generators $c_1, \ldots, c_r$, we have $n \equiv c_1^{n_1} \cdot \ldots \cdot c_r^{n_r} \bmod q$, where for each $1 \leqslant j \leqslant r$, $0 \leqslant n_j \leqslant q_j$, and for some $1 \leqslant i \leqslant r$ strictly $0 \leqslant n_i < q_i$. Then in that particular factor i, map c_i to a primitive q_ith root of unity, while at other factors $j \neq i$, map c_j's to 1. Obviously the resulting χ' satisfies $\chi'(n) \neq 1$. Then

$$\sum_{\chi \in \Xi} \chi(n) = \sum_{\chi \in \Xi} (\chi' \chi)(n) = \chi'(n) \sum_{\chi \in \Xi} \chi(n).$$

Here, since $\chi'(n) \neq 1$, $\sum_{\chi \in \Xi} \chi(n) = 0$, and the proof is complete. □

Corollary 4.3.6. *If $\gcd(a, q) = 1$, then for any $n \in \mathbf{Z}$,*

$$\frac{1}{\varphi(q)} \sum_{\chi \in \Xi} \overline{\chi(a)} \chi(n) = \begin{cases} 1 & \text{if } n \equiv a \bmod q; \\ 0 & \text{if } n \not\equiv a \bmod q. \end{cases}$$

Proof. Apply Proposition 4.3.5 to the residue class $a^{-1}n$. □

Proposition 4.3.7. *We have*

$$\sum_{n \bmod q} \chi(n) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

Proof. If $\chi = \chi_0$, the statement is obvious. If $\chi \neq \chi_0$, then take $a \in \mathbf{Z}_q^\times$ such that $\chi(a) \neq 1$. When n runs through the residue classes modulo q, so does an, which implies

$$\sum_{n \bmod q} \chi(n) = \sum_{n \bmod q} \chi(an) = \chi(a) \sum_{n \bmod q} \chi(n).$$

Here, since $\chi(a) \neq 1$, $\sum_{n \bmod q} \chi(n) = 0$, and the proof is complete. □

Problem 4.3.1. For any function $f : \mathbf{Z}_q^\times \to \mathbf{C}$, we define its discrete multiplicative Fourier transform $\widehat{f} : \Xi \to \mathbf{C}$ as

$$\widehat{f}(\chi) = \sum_{\substack{a \bmod q \\ \gcd(a,q)=1}} f(a) \overline{\chi(a)}.$$

Prove the inversion formula, that is, for any $x \in \mathbf{Z}_q^\times$,

$$f(x) = \frac{1}{\varphi(q)} \sum_{\chi \in \Xi} \widehat{f}(\chi) \chi(x).$$

(*Hint:* use the definition of $\widehat{f}$, change the order of summation, and use Corollary 4.3.6.)

4.4 L-functions

Definition 4.4.1 (Riemann zeta function)**.** Consider the Dirichlet series corresponding to the constant sequence $a_n = 1$ for all $n \in \mathbf{N}$, i.e.

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

Proposition 4.4.2. *The convergence domain of the Dirichlet series defining ζ is the domain $\{s : \Re s > 1\}$.*

Proof. We know from Section 4.2 that the convergence domain is a half-plane. For $s = 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

When $s > 1$ is real, then replace each term n by the preceding power of 2, this increases the sum as

$$\sum_{n=1}^{\infty} n^{-s} \leqslant \sum_{k=0}^{\infty} 2^k \cdot 2^{-ks} = \sum_{k=0}^{\infty} (2^{1-s})^k = \frac{1}{1-2^{1-s}} < \infty.$$

This completes the proof. □

For the proof of Dirichlet's theorem, it is essential to extend ζ to the domain $\{s : \Re s > 0\}$. This cannot be done holomorphically, as it follows from Theorem 4.2.4, but can be done meromorphically with a single pole of order 1 at the point $s = 1$.

Proposition 4.4.3. *The function $\zeta(s) - 1/(s-1)$ continues holomorphically to $\{s : \Re s > 0\}$.*

Proof. First, for $\Re s > 1$, we write

$$\frac{1}{s-1} = \int_1^{\infty} x^{-s} dx = \sum_{n=1}^{\infty} \int_n^{n+1} x^{-s} dx.$$

Then

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \left(n^{-s} - \int_n^{n+1} x^{-s} dx \right) = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - x^{-s}) dx$$

holds by absolute convergence when $\Re s > 1$. Moreover, we claim that the sum on the right-hand side is absolutely convergent even for $\Re s > 0$. Here,

$$\left| n^{-s} - x^{-s} \right| = \left| s \int_n^x y^{-1-s} dy \right| \leqslant |s| n^{-1-\Re s}.$$

Then

$$\sum_{n=1}^{\infty} n^{-1-\Re s}$$

is convergent for $\Re s > 0$, recall the proof of Proposition 4.4.2. Hence the sequence

$$\sum_{n=1}^{N} \left(n^{-s} - \int_n^{n+1} x^{-s} dx \right)$$

converges locally uniformly on $\{s : \Re s > 0\}$ as $N \to \infty$. Its limit

$$\sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - x^{-s}) dx$$

is holomorphic then for $\Re s > 0$. □

Remark 4.4.4. The function ζ extends to the whole complex plance $\mathbf{C}$ meromorphically, with the only pole of order 1 at $s = 1$.

Definition 4.4.5 (Dirichlet L-functions)**.** For a fixed number $q \in \mathbf{N}$ and a Dirichlet character χ modulo q, take the Dirichlet series corresponding to the sequence $a_n = \chi(n)$, i.e.

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}.$$

One can see that this simplifies to ζ for $q = 1$. Also, it is easy to see that for $\Re s > 1$, $L(s,\chi)$ is absolutely convergent, recall Proposition 4.4.2.

Proposition 4.4.6 (Euler product)**.** *For $\Re s > 1$, we have*

$$L(s,\chi) = \prod_{p \text{ prime}} (1 - \chi(p)p^{-s})^{-1}.$$

Proof. For each prime p, write

$$(1 - \chi(p)p^{-s})^{-1} = \sum_{k=0}^{\infty} (\chi(p)p^{-s})^k = \sum_{k=0}^{\infty} \chi(p^k)(p^k)^{-s}.$$

Then the claim follows from the fundamental theorem of arithmetic (Theorem 1.2.9):

$$\chi(n)n^{-s} = \prod_{j=1}^{r} \chi\left(p_j^{\alpha_j}\right)\left(p_j^{\alpha_j}\right)^{-s},$$

if the canonical form (1.2.1) of n is $\prod_{j=1}^{r} p_j^{\alpha_j}$. Manipulations concerning the order of summation are verified by absolute convergence. □

When specifying to ζ, we obtain

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$$

for $\Re s > 1$.

For the principal character χ_0, $L(s,\chi_0)$ is simply a multiple of ζ, namely

$$L(s,\chi_0) = \zeta(s) \prod_{\substack{p \text{ prime} \\ p|q}} (1 - p^{-s}) \tag{4.4.1}$$

by Proposition 4.4.6, first only for $\Re s > 1$, then for $\Re s > 0$ by analytic continuation, since the quotient is just a finite product over primes dividing q. This implies, in particular, that $L(s,\chi_0)$ has a pole at $s = 1$, that is,

$$L(s,\chi_0) = \frac{r_q}{s-1} + \text{holomorphic}$$

on the domain $\{s : \Re s > 0\}$, where

$$r_q = \prod_{\substack{p \text{ prime} \\ p|q}} (1 - p^{-1}) = \frac{\varphi(q)}{q},$$

its exact value is however not that important, we will use only that it is nonzero (so $L(s,\chi_0)$ has a pole of order 1 at $s = 1$).

Characters different from the principal character lead to a larger convergence domain.

Proposition 4.4.7. *If $\chi \neq \chi_0$, then the convergence domain of the Dirichlet series defining $L(s,\chi)$ is the domain $\{s : \Re s > 0\}$.*

Proof. We know from Section 4.2 that the convergence domain is a half-plane. Obviously

$$\sum_{n=1}^{\infty} \chi(n)n^{-0} = \sum_{n=1}^{\infty} \chi(n)$$

is not convergent, since the absolute value of the summand is 1 infinitely many times.

If $s > 0$ is real, then set $X(n) = \sum_{j=1}^{n} \chi(j)$. With this notation, for any positive integers $M < N$,

$$\begin{aligned}\sum_{n=M+1}^{N} \chi(n)n^{-s} &= \sum_{n=M+1}^{N} (X(n) - X(n-1))n^{-s} \\ &= \sum_{n=M+1}^{N} X(n)(n^{-s} - (n+1)^{-s}) - X(M)(M+1)^{-s} + X(N)(N+1)^{-s}.\end{aligned}$$

By Proposition 4.3.7, $|X(n)| \leqslant q$, since $\chi \neq \chi_0$. Using this,

$$\sum_{n=M+1}^{N} \chi(n)n^{-s} \ll_q M^{-s} + N^{-s} + \sum_{n=M+1}^{N} (n^{-s} - (n+1)^{-s}).$$

The last sum is a telescopic sum, dominated by its first term. Therefore,

$$\sum_{n=M+1}^{N} \chi(n)n^{-s} \ll_q M^{-s}.$$

Then we are done by Cauchy's convergence criterion (using that $s > 0$). □

Theorem 4.4.8 (nonvanishing of L-functions at 1)**.** *If $\chi \neq \chi_0$, then $L(1, \chi) \neq 0$.*

Proof. Assume by contradiction that for some character $\widetilde{\chi} \neq \chi_0$ modulo q, $L(1, \widetilde{\chi}) = 0$. Consider then the function

$$F(s) = \prod_{\chi \in \Xi} L(s, \chi).$$

First we claim that $F(s)$ is holomorphic on $\{s : \Re s > 0\}$. Indeed, take the Taylor expansion of the vanishing L-function at $s = 1$:

$$L(s, \widetilde{\chi}) = a_0(s-1) + a_1(s-1)^2 + \dots,$$

then

$$L(s, \widetilde{\chi})L(s, \chi_0) = (s-1) \cdot \text{holomorphic} \cdot \frac{1}{s-1} \cdot \text{holomorphic} = \text{holomorphic},$$

that is, the pole of $L(s, \chi_0)$ is killed by the zero of $L(s, \widetilde{\chi})$. Therefore $L(s, \widetilde{\chi})L(s, \chi_0)$ is holomorphic on $\{s : \Re s > 0\}$. The remaining L-factors do not cause any problem, since they are all holomorphic on the indicated domain.

Second, we investigate the Dirichlet series expansion for $\Re s > 1$. From Proposition 4.4.6, we have

$$F(s) = \prod_{p \nmid q} \prod_{\chi \in \Xi} (1 - \chi(p)p^{-s})^{-1}.$$

Fix a prime $p \nmid q$. Take a character χ' such that the order $\mathbf{o}(p) = \mathbf{o}(\chi'(p))$ of $\chi'(p)$ modulo q is maximal, then other $\mathbf{o}(\chi(p))$'s are divisors of $\mathbf{o}(p)$. Using

$$1 - x^{\mathbf{o}(p)} = \prod_{j=1}^{\mathbf{o}(p)} (1 - (\chi'(p))^j x),$$

we obtain, for any $\chi \in \Xi$,

$$\prod_{j=1}^{\mathbf{o}(p)} (1 - (\chi'(p))^j \chi(p)p^{-s}) = 1 - (\chi(p))^{\mathbf{o}(p)} p^{-s\mathbf{o}(p)} = 1 - p^{-s\mathbf{o}(p)}.$$

The whole Ξ can be written as the disjoint union of $\varphi(q)/\mathbf{o}(p)$ sets of the form

$$\{\chi\chi', \chi\chi'^2, \dots, \chi\chi'^{\mathbf{o}(p)} = \chi\},$$

recall the proof of Theorem 1.6.4. Then altogether the Euler factor at the prime p is

$$\left(1 - p^{-s\mathbf{o}(p)}\right)^{-\varphi(q)/\mathbf{o}(p)} = \left(1 + p^{-\mathbf{o}(p)s} + p^{-2\mathbf{o}(p)s} + \dots\right)^{\varphi(q)/\mathbf{o}(p)}.$$

This means that when we take the product over the primes p not dividing q, we obtain a Dirichlet series of nonnegative coefficients. Applying Theorem 4.2.4, we obtain that the Dirichlet series of F is convergent for $\Re s > 0$.

Considering again the Euler factors just computed, we also see that for any prime $p \nmid q$, the coefficient corresponding to $p^{-\varphi(q)}$ is positive:

$$\left(1 + p^{-\mathbf{o}(p)s} + p^{-2\mathbf{o}(p)s} + \dots\right)^{\varphi(q)/\mathbf{o}(p)} = 1 + p^{-\varphi(q)s} + \text{other terms}.$$

Then

$$F\left(\frac{1}{\varphi(q)}\right) \geqslant \sum_{p \nmid q} \frac{1}{p} = \infty$$

by Theorem 2.1.2, a contradiction. □

Problem 4.4.1. Prove that if $s_1 > s_0 > 1$ are real numbers, then $\zeta(s_1) < \zeta(s_0)$. (*Hint:* use that for any $n \geqslant 2$, $n^{-s_0} > n^{-s_1}$ and the finiteness of $\zeta(s_0), \zeta(s_1)$.)

Problem 4.4.2. Give an elementary proof to the fact that if χ is a Dirichlet character modulo 8, then $L(1, \chi) \neq 0$. (*Hint:* we may freely assume χ is nonprincipal. Then the possibilities for χ are the following:

$$\begin{array}{llll} \chi_1(1) = 1, & \chi_1(3) = 1, & \chi_1(5) = -1, & \chi_1(7) = -1; \\ \chi_2(1) = 1, & \chi_2(3) = -1, & \chi_2(5) = 1, & \chi_2(7) = -1; \\ \chi_3(1) = 1, & \chi_3(3) = -1, & \chi_3(5) = -1, & \chi_3(7) = 1. \end{array}$$

Prove that for each $1 \leqslant j \leqslant 3$, and any $n \in \mathbf{N} \cup \{0\}$,

$$\frac{\chi_j(8n+1)}{8n+1} + \frac{\chi_j(8n+3)}{8n+3} + \frac{\chi_j(8n+5)}{8n+5} + \frac{\chi_j(8n+7)}{8n+7} > 0,$$

using the convexity of $x \mapsto 1/x$ on $\{x : x > 0\}$.)

4.5 Completion of the proof

Definition 4.5.1 (von Mangoldt function)**.** Define

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \in \mathbf{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 4.5.2. *For any $\chi \in \Xi$, on the domain $\{s : \Re s > 1\}$,*

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n=1}^{\infty} \Lambda(n)\chi(n)n^{-s}.$$

Proof. By multiplying, we have to prove

$$L'(s,\chi) = -\sum_{n=1}^{\infty} \Lambda(n)\chi(n)n^{-s} \cdot L(s,\chi).$$

On the left-hand side, the coefficient corresponding to n^{-s} is $-\chi(n)\log n$ by (4.2.1). On the right-hand side, it is $-\sum_{d|n}\chi(d)\Lambda(d)\chi(n/d)$, so it suffices to show

$$\log n = \sum_{d|n}\Lambda(d).$$

If the canonical form (1.2.1) of n is $n = \prod_{j=1}^{r} p_j^{\alpha_j}$, then both sides are clearly $\sum_{j=1}^{r}\alpha_j \log p_j$. □

Proposition 4.5.3. *For any* $\gcd(a,q)=1$, *we have*

$$\sum_{n\equiv a \bmod q}\Lambda(n)n^{-1} = \lim_{s\to 1+}\sum_{n\equiv a \bmod q}\Lambda(n)n^{-s} = \infty.$$

Proof. As the first equality is obvious from the second one, it suffices to prove the latter. First we apply Corollary 4.3.6 to see that for $\Re s > 1$,

$$\sum_{n\equiv a \bmod q}\Lambda(n)n^{-s} = \frac{1}{\varphi(q)}\sum_{n=1}^{\infty}\sum_{\chi\in\Xi}\overline{\chi(a)}\chi(n)\Lambda(n)n^{-s}.$$

Changing the order of summation, then applying Proposition 4.5.2, we obtain

$$\sum_{n\equiv a \bmod q}\Lambda(n)n^{-s} = -\frac{1}{\varphi(q)}\sum_{\chi\in\Xi}\overline{\chi(a)}\frac{L'(s,\chi)}{L(s,\chi)}.$$

Now let s tend to 1 from above. For each $\chi\in\Xi$ different from the principal character χ_0, $L'(s,\chi)/L(s,\chi)$ is a finite number, since $L(s,\chi)$ is differentiable on $\{s : \Re s > 0\}$ and $L(1,\chi)\neq 0$ (therefore $L(s,\chi)\neq 0$ in a sufficiently small neighborhood of 1). Altogether,

$$\lim_{s\to 1+}\sum_{n\equiv a \bmod q}\Lambda(n)n^{-s} = -\frac{1}{\varphi(q)}\lim_{s\to 1+}\frac{L'(s,\chi_0)}{L(s,\chi_0)} + \text{finite}.$$

Here, using (4.4.1) and Proposition 4.5.2,

$$-\lim_{s\to 1+}\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \text{constant}\cdot\lim_{s\to 1+}\sum_{n=1}^{\infty}\Lambda(n)n^{-s},$$

where the constant is nonzero. Now we are going to prove

$$\lim_{s\to 1+}\sum_{n=1}^{\infty}\Lambda(n)n^{-s} = \infty,$$

using

$$\sum_{p \text{ prime}}\frac{\log p}{p} = \infty$$

(which follows trivially from Theorem 2.1.2). Indeed,

$$\sum_{n=1}^{\infty}\Lambda(n)n^{-s}$$

increases when s decreases to 1. Assume there is a bound

$$\sum_{n=1}^{\infty}\Lambda(n)n^{-s} \leqslant A$$

holding for any $s > 1$. If X is large enough,

$$\sum_{\substack{p\leqslant X\\ p \text{ prime}}}\frac{\log p}{p} \geqslant A+1.$$

Now

$$A \geqslant \lim_{s\to 1+} \sum_{n=1}^{\infty} \Lambda(n)n^{-s} \geqslant \lim_{s\to 1+} \sum_{n\leqslant X} \Lambda(n)n^{-s} \geqslant \lim_{s\to 1+} \sum_{\substack{p\leqslant X \\ p \text{ prime}}} \frac{\log p}{p^s} = \sum_{\substack{p\leqslant X \\ p \text{ prime}}} \frac{\log p}{p} \geqslant A+1,$$

a contradiction. □

We are now very close to our goal, the only problem is that Λ is positive not only for primes, but also for prime powers.

Proposition 4.5.4. *We have*

$$\sum_{p \text{ prime}} \sum_{k=2}^{\infty} \Lambda(p^k)p^{-k} < \infty.$$

Proof. For any prime p,

$$\sum_{k=2}^{\infty} p^{-k} = p^{-2} \sum_{k=0}^{\infty} \frac{1}{1-\frac{1}{p}} \leqslant 2p^{-2}.$$

Therefore,

$$\sum_{p \text{ prime}} \sum_{k=2}^{\infty} \Lambda(p^k)p^{-k} \leqslant 2 \sum_{p \text{ prime}} \frac{\log p}{p^2} \ll \sum_{n=1}^{\infty} n^{-3/2} = \zeta(3/2) < \infty,$$

and the proof is complete. □

Combining Proposition 4.5.3 and Proposition 4.5.4, we obtain

$$\sum_{\substack{p\equiv a \bmod q \\ p \text{ prime}}} \frac{\log p}{p} = \infty,$$

and the proof of Theorem 2.1.3 is complete.

Remark 4.5.5. There are many proofs for Dirichlet's theorem. In most of them, as here, the crucial point is to show $L(1,\chi) \neq 0$.

Remark 4.5.6. The investigation of L-functions and the function ζ itself is of extreme importance in number theory. As we saw, the fact that the L-functions do not vanish at 1 led to the infinitude of prime numbers in arithmetic progressions. The prime number theorem (Theorem 2.1.6) follows from the even deeper fact that ζ does not vanish on the line $\{s : \Re s = 1\}$. One of the most important problems in mathematics (a Millennium Prize Problem) is the Riemann Hypothesis: all zeros of ζ lying in the half-plane $\{s : \Re s > 0\}$ actually lie on the line $\{s : \Re s = 1/2\}$.