

Basic Number Theory

Instructor: Laszlo Babai
Notes by Vincent Lucarelli and the instructor

Last revision: June 11, 2001

Notation: Unless otherwise stated, all variables in this note are *integers*. For $n \geq 0$, $[n] = \{1, 2, \dots, n\}$. The formula $d|n$ denotes the relation “ d divides n ,” i. e., $(\exists k)(n = dk)$. We also say “ d is a divisor of n ” or “ n is a multiple of d .” Note that $(\forall a)(a|a)$, including $0|0$ (even though we do not allow division by zero!). In fact $0|n \iff n = 0$. Note also that $(\forall n)((\forall k)(n|k) \iff k = \pm 1)$. We write $a \equiv b \pmod{m}$ if $m|a - b$ (“ a is congruent to b modulo m ”).

1 Gcd, congruences

Exercise 1.1 Prove that the product of n consecutive integers is always divisible by $n!$.
Hint. One-line proof.

Exercise 1.2 (The Divisor Game) Select an integer $n \geq 2$. Two players alternate naming positive divisors of n subject to the following rule: no divisor of any previously named integer can be named. The first player forced to name “ n ” loses. Example: if $n = 30$ then the following is a possible sequence of moves: 10, 3, 6, 15, at which point it is the first player’s move; he is forced to say “30” and loses.

1. Find a winning strategy for the first player when n is a prime power or the product of two prime powers or when n is square-free (n is not divisible by the square of any prime).
2. Prove: $\forall n \geq 2$, the first player has a winning strategy. (*Hint:* prove, in two or three lines, the *existence* of a winning strategy.)

Let $\text{Div}(n)$ denote the set of positive divisors of n .

Exercise 1.3 Prove: $(\forall a, b)(\exists d)(\text{Div}(a) \cap \text{Div}(b) = \text{Div}(d))$. A nonnegative d satisfying this statement is called the g.c.d. of a and b . Note that $\text{g.c.d.}(a, b) = 0 \iff a = b = 0$. Define l.c.m. analogously. When is $\text{l.c.m.}(a, b) = 0$?

Exercise 1.4 Prove: $\text{g.c.d.}(a^k - 1, a^\ell - 1) = a^d - 1$, where $d = \text{g.c.d.}(k, \ell)$.

Definition 1.5 The Fibonacci numbers are defined by the recurrence $F_n = F_{n-1} + F_{n-2}$, $F_0 = 0$, $F_1 = 1$.

Exercise 1.6 Prove: $\text{g.c.d.}(F_k, F_\ell) = F_d$, where $d = \text{g.c.d.}(k, \ell)$.

Exercise 1.7 Prove: if $a \equiv b \pmod{m}$ then $\text{g.c.d.}(a, m) = \text{g.c.d.}(b, m)$.

Exercise 1.8 Prove: if $a, b \geq 0$ then $\text{g.c.d.}(a, b) \cdot \text{l.c.m.}(a, b) = ab$.

Exercise 1.9 Prove: congruence modulo m is an equivalence relation on \mathbb{Z} . The equivalence classes are called the *residue classes* mod m . There are m residue classes modulo m . Under the natural operations they form the ring $\mathbb{Z}/m\mathbb{Z}$. The additive group of this ring is cyclic.

Exercise 1.10 Prove that the sequence of Fibonacci numbers mod m is periodic. The length of the period is $\leq m^2 - 1$.

Exercise 1.11 An *integer-preserving polynomial* is a polynomial $f(x)$ such that $(\forall a \in \mathbb{Z})(f(a) \in \mathbb{Z})$. Prove that $f(x)$ is integer-preserving if and only if it can be written as

$$f(x) = \sum_{i=0}^n a_i \binom{x}{i} \quad (1)$$

with suitable integer coefficients a_i . Here

$$\binom{x}{i} = \frac{x(x-1)\dots(x-i+1)}{i!}; \quad \binom{x}{0} = 1.$$

Exercise 1.12 A *congruence-preserving polynomial* is an integer-preserving polynomial such that $(\forall a, b, m \in \mathbb{Z})(a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m})$. Prove that $f(x)$ is congruence-preserving if and only if $(\forall i)(e_i | a_i)$ in the expression (1), where $e_i = \text{l.c.m.}(1, 2, \dots, i)$.

Exercise 1.13 A *multiplicative inverse* of a modulo m is an integer x such that $ax \equiv 1 \pmod{m}$; notation: $x = a^{-1} \pmod{m}$. Prove: $\exists a^{-1} \pmod{m} \iff \text{g.c.d.}(a, m) = 1$.

Exercise 1.14 (Wilson's theorem) Prove: $(p-1)! \equiv -1 \pmod{p}$. *Hint:* match each number with its multiplicative inverse in the product $(p-1)!$

Exercise 1.15 Prove: if $\text{g.c.d.}(a, p) = 1$ then $\prod_{j=1}^{p-1} j \equiv \prod_{i=1}^{p-1} (ai) \pmod{p}$. *Hint.* Match terms on the right hand side with terms on the left hand side so that corresponding terms satisfy $j \equiv ai \pmod{p}$.

Exercise 1.16 Infer **Fermat's little Theorem** from the preceding exercise: if $\text{g.c.d.}(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$.

Exercise 1.17 Use the same idea to prove the **Euler–Fermat theorem**: if $\text{g.c.d.}(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$. (φ is Euler’s φ function, see below).

Exercise 1.18 Prove: if p is a prime and f is a polynomial with integer coefficients then $f(x)^p \equiv f(x^p) \pmod{p}$. Here the congruence of two polynomials means coefficientwise congruence.

The multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ consists of the mod m residue classes relatively prime to m . Its order is $\varphi(m)$.

Exercise⁺ 1.19 Prove: if p is a prime then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. A generator of this group is called a *primitive root mod p* .

Exercise⁺ 1.20 Prove: if p is an odd prime then $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic.

Exercise⁺ 1.21 If $k \geq 2$ then the group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is not cyclic but the direct sum of a cyclic group of order 2 and a cyclic group of order 2^{k-2} .

2 Arithmetic Functions

Definition 2.1 (Euler’s Phi Function)

$$\begin{aligned} \varphi(n) &= \left| \{k \in [n] : \text{g.c.d.}(k, n) = 1\} \right| \\ &= \text{number of positive integers not greater than } n \text{ which are relatively prime to } n \end{aligned}$$

Exercise 2.2 Show that the number of complex primitive n -th roots of unity is $\varphi(n)$. Show that if $d|n$ then the number of elements of order d in a cyclic group of order n is $\varphi(d)$.

Exercise 2.3 Show

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

Exercise⁺ 2.4 Let $D_n = (d_{ij})$ denote the $n \times n$ matrix with $d_{ij} = \text{g.c.d.}(i, j)$. Prove:

$$\det D_n = \varphi(1)\varphi(2) \cdots \varphi(n).$$

(*Hint.* Let $Z = (z_{ij})$ be the matrix with $z_{ij} = 1$ if $i|j$ and $z_{ij} = 0$ otherwise. Consider the matrix $Z^T F Z$ where F is the diagonal matrix with entries $\varphi(1), \dots, \varphi(n)$ and Z^T is “ Z -transpose” (reflection in the main diagonal).)

Definition 2.5 (Number of [positive] divisors)

$$d(n) = \left| \{d \in \mathbb{N} : d|n\} \right|$$

Exercise 2.6 Prove: $d(n) < 2\sqrt{n}$.

Exercise⁺ 2.7 Prove: $(\forall \epsilon > 0)(\exists n_0)(\forall n > n_0)(d(n) < n^\epsilon)$. (*Hint.* Use a consequence of the Prime Number Theorem (see the next section).) Prove that $d(n) < n^{c/\ln \ln n}$ for some constant c . The best asymptotic constant is $c = \ln 2 + o(1)$.

Exercise⁺ 2.8 Prove that for infinitely many values of n the reverse inequality $d(n) > n^{c/\ln \ln n}$ holds (with another constant $c > 0$). (Again, use the PNT.)

Exercise⁺ 2.9 Let $D(n) = (1/n) \sum_{i=1}^n d(i)$ (the average number of divisors). Prove: $D(n) \sim \ln(n)$. (*Comment.* If we pick an integer t at random between 1 and n then $D(n)$ will be the *expected number* of divisors of t . – Make your proof very simple (3 lines). Do not use the PNT.)

Exercise⁺ 2.10 Prove: $(1/n) \sum_{i=1}^n d(i)^2 = \Theta((\ln n)^3)$.

Definition 2.11 (Sum of [positive] divisors)

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

Definition 2.12 Let $n = p_1^{k_1} \cdots p_r^{k_r}$ where the p_i are distinct primes and $k_i > 0$. Set $\nu(n) = r$ (number of distinct prime divisors; so $\nu(1) = 0$). Set $\nu^*(n) = k_1 + \cdots + k_r$ (total number of prime divisors; so $\nu^*(1) = 0$).

Exercise⁺ 2.13 Prove that the expected number of distinct prime divisors of a random integer $i \in [n]$ is asymptotically $\ln \ln n$:

$$\frac{1}{n} \sum_{i=1}^n \nu(i) \sim \ln \ln n.$$

How much larger is ν^* ? On average, not much. Prove that the average value of ν^* is also asymptotic to $\ln \ln n$.

Terminology. n is **square-free** if $(\forall p \text{ prime})(p^2 \nmid n)$.

Definition 2.14 (Möbius Function)

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k \text{ where the } p_i \text{ are distinct (} n \text{ is square-free)} \\ 0 & \text{if } (\exists p)(p^2 | n) \end{cases}$$

Exercise 2.15 Let $\delta(n) = \sum_{d|n} \mu(d)$. Evaluate $\delta(n)$.

Definition 2.16 For $s > 1$ define the zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Exercise 2.17 Prove Euler's identity:

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}.$$

Exercise 2.18 Prove:

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Exercise 2.19 Prove:

$$(\zeta(s))^2 = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}.$$

Exercise 2.20 Prove:

$$\zeta(s)(\zeta(s) - 1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}.$$

Exercise* 2.21 Prove: $\zeta(2) = \pi^2/6$.

Exercise 2.22 Give a natural definition which will make following statement sensible and true: “the probability that a random positive integer n satisfies $n \equiv 3 \pmod{7}$ is $1/7$.” Our choice of a “random positive integer” should be “uniform” (obviously impossible). (*Hint.* Consider the integers up to x ; then take the limit as $x \rightarrow \infty$.)

Exercise 2.23 Make sense out of the question “What is the probability that two random positive integers are relatively prime?” Prove that the answer is $6/\pi^2$. *Hint.* To prove that the required limit exists may be somewhat tedious. If you want to see the fun part, assume the existence of the limit, and prove in just two lines that the limit must be $1/\zeta(2)$.

Definition 2.24 Let F be a field. $f: \mathbb{N} \rightarrow F$ is called **multiplicative** if

$$(\forall a, b)(\text{g.c.d.}(a, b) = 1 \Rightarrow f(ab) = f(a)f(b)).$$

f is called **completely multiplicative** if

$$(\forall a, b)(f(ab) = f(a)f(b)).$$

f is called **additive** if

$$(\forall a, b)(\text{g.c.d.}(a, b) = 1 \Rightarrow f(ab) = f(a) + f(b)).$$

Exercise 2.25 Show that

1. φ, σ, d , and μ are multiplicative but not completely multiplicative

2. ν is additive and ν^* is completely additive.

Exercise 2.26 Show

1. $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$
2. $d(p^k) = k+1$
3. $\sigma(p^k) = \frac{p^{k+1} - 1}{p-1}$

Exercise 2.27 Show

1. $\varphi\left(\prod_{i=1}^r p_i^{k_i}\right) = \prod_{i=1}^r (p_i - 1)p_i^{k_i-1}$
2. $d\left(\prod_{i=1}^r p_i^{k_i}\right) = \prod_{i=1}^r (k_i + 1)$
3. $\sigma\left(\prod_{i=1}^r p_i^{k_i}\right) = \prod_{i=1}^r \frac{p_i^{k_i+1} - 1}{p_i - 1}$

Exercise 2.28 Show

$$\varphi(n) = n \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

Let F be a field and $f: \mathbb{N} \rightarrow F$. Define

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

Exercise 2.29 (Möbius Inversion Formula) Show

$$f(n) = \sum_{d|N} g(d) \mu\left(\frac{n}{d}\right).$$

Exercise 2.30 Use the Möbius Inversion Formula together with Exercise 2.3 for a second proof of Exercise 2.28.

Exercise 2.31 Prove that the sum of the complex primitive n -th roots of unity is $\mu(n)$.

Definition 2.32 The n -th cyclotomic polynomial $\Phi_n(x)$ is defined as $\Phi_n(x) = \prod_{\omega} (x - \omega)$ where the product ranges over all complex primitive n -th roots of unity. Note that the degree of $\Phi_n(x)$ is $\varphi(n)$. Also note that $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$.

Exercise 2.33 Prove that $\Phi_n(x)$ has integer coefficients. What is the coefficient of $x^{\varphi(n)-1}$?

Exercise 2.34 Prove: if p is a prime then $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Exercise 2.35 Prove:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Exercise⁺ 2.36 (Bateman) Let A_n denote the sum of the absolute values of the coefficients of $\Phi_n(x)$. Prove that $A_n < n^{d(n)/2}$. Infer from this that $A_n < \exp(n^{c/\ln \ln n})$ for some constant c . *Hint:* We say that the power series $\sum_{n=0}^{\infty} a_n x^n$ dominates the power series $\sum_{n=0}^{\infty} b_n x^n$ if $(\forall n)(|b_n| \leq a_n)$. Prove that the power series

$$\prod_{d|n} \frac{1}{1 - x^d}$$

dominates $\Phi_n(x)$.

Note: Erdős proved that this bound is tight, apart from the value of the constant: for infinitely many values of n , $A_n > \exp(n^{c/\ln \ln n})$ for another constant $c > 0$.

Exercise⁺ 2.37 (Hermite) Let $f(x) = \sum_{i=0}^n a_i x^i$ be a monic polynomial of degree n (i. e., $a_n = 1$) with integer coefficients. Suppose all roots of f have unit absolute value. Prove that all roots of f are roots of unity. (In other words, if all algebraic conjugates of a complex algebraic number z have unit absolute value then z is a root of unity.)

3 Prime Numbers

Exercise 3.1 Prove:

$$\sum_{i=1}^n \frac{1}{i} = \ln n + O(1).$$

Exercise 3.2 Prove:

$$\prod_{p \leq x} \frac{1}{1 - 1/p} = \sum' \frac{1}{i},$$

where the product is over all primes $\leq x$ and the summation extends over all positive integers i with no prime divisors greater than x . In particular, the sum on the right-hand side converges. It also follows that the left-hand side is greater than $\ln x$.

Exercise 3.3 Prove: $\sum 1/p = \infty$. (*Hint.* Use the preceding exercise. Take natural logarithms; use the power series expansion of $\ln(1 - z)$. Conclude that $\sum_{p \leq x} 1/p > \ln \ln x + O(1)$. (In other words, $\sum_{p \leq x} 1/p - \ln \ln x$ is bounded from below.)

Exercise⁺ 3.4 Prove: $\sum_{p \leq x} 1/p = \ln \ln x + O(1)$. (In other words, $|\sum_{p \leq x} 1/p - \ln \ln x|$ is bounded.)

Exercise⁺ 3.5 Prove $\varphi(n) = \Omega\left(\frac{n}{\ln \ln n}\right)$ and find the largest implicit asymptotic constant.

Let $\pi(x)$ the number of primes less than or equal to x .

Theorem 3.6 (Prime Number Theorem, Hadamard and de la Vallée Poussin, 1896)

$$\pi(x) \sim \frac{x}{\ln x}$$

Exercise 3.7 Use the PNT to show that $\lim_{n \rightarrow \infty} \frac{p_{n+1}}{p_n} = 1$, where p_n is the n -th prime.

Exercise 3.8 Use the PNT to prove $p_n \sim n \cdot \ln n$.

Exercise 3.9 Prove $\prod_{\substack{p \leq x \\ p \text{ prime}}} p = \exp(x(1 + o(1)))$. Prove that this result is in fact equivalent to the PNT.

Exercise 3.10 Let $e_n = \text{l.c.m.}(1, 2, \dots, n)$. Prove: $e_n = \exp(n(1 + o(1)))$. Prove that this result is in fact equivalent to the PNT.

Exercise 3.11 Prove: $\sum_{p \leq x} p \sim x^2/(2 \ln x)$. (Use the PNT.)

Definition 3.12 A *permutation* is a bijection of a set to itself. The permutations of a set form a group under composition. The *symmetric group of degree n* is the group of all permutations of a set of n elements; it has order $n!$. The *exponent* of a group is the l.c.m. of the orders of all elements of the group.

Exercise 3.13 Prove: the exponent of S_n is e_n .

Exercise⁺ 3.14 Let $m(n)$ denote the maximum of the orders of the elements in S_n . Prove: $m(n) = \exp(\sqrt{n \ln n}(1 + o(1)))$.

Exercise* 3.15 Let $a(n)$ denote the “typical” order of elements in S_n . Prove that $\ln a(n) = O((\ln n)^2)$. (“Typical” order means that 99% of the elements has order falling in the stated range. Here “99” is arbitrarily close to 100.) *Hint.* Prove that a typical permutation has $O(\ln n)$ cycles.

Erdős and Turán proved in 1965 that in fact $\ln a(n) \sim (\ln n)^2/2$.

Exercise 3.16 Prove from first principles: $\prod_{\substack{p < x \\ p \text{ prime}}} p < 4^x$. (*Hint:* if $n < p \leq 2n$ then $p \mid \binom{2n}{n}$.)

Exercise 3.17 Prove: if $p > \sqrt{2n}$ then $p^2 \nmid \binom{2n}{n}$.

Exercise 3.18 Prove: if q is a prime power dividing $\binom{2n}{n}$ then $q \leq n$. (*Hint.* Give a formula for the highest exponent of a prime p which divides $\binom{2n}{n}$. First, find a formula for the exponent of p in $n!$.)

Exercise 3.19 Prove from first principles: $\prod_{\substack{p < x \\ p \text{ prime}}} p > (2 + o(1))^x$. (*Hint.* Consider the prime-power decomposition of $\binom{x}{x/2}$. Show that the contribution of the powers of primes $\leq \sqrt{x}$ is negligible.)

Exercise 3.20 Paul Erdős was an undergraduate when he found a simple proof of Chebyshev's theorem based on the prime factors of $\binom{2n}{n}$. Chebyshev's theorem is a precursor of the PNT; it says that

$$\pi(x) = \Theta\left(\frac{x}{\ln x}\right).$$

Following Erdős, prove Chebyshev's Theorem from first principles. The proof should be only a few lines, based Exercises 3.16 and 3.19.

4 Quadratic Residues

Definition 4.1 a is a **quadratic residue mod p** if $(p \nmid a)$ and $(\exists b)(a \equiv b^2 \pmod{p})$.

Exercise 4.2 Prove: a is a quadratic residue mod $p \iff a^{(p-1)/2} \equiv 1 \pmod{p}$.

Definition 4.3 a is a **quadratic non-residue mod p** if $(\forall b)(a \not\equiv b^2 \pmod{p})$.

Exercise 4.4 Prove: a is a quadratic non-residue mod $p \iff a^{(p-1)/2} \equiv -1 \pmod{p}$.

Definition 4.5 (Legendre Symbol)

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \\ 0 & \text{if } p \mid a \end{cases}$$

Let \mathbb{F}_q be a finite field of odd prime power order q .

Definition 4.6 $a \in \mathbb{F}_q$ is a **quadratic residue** if $a \neq 0$ and $(\exists b)(a = b^2)$.

Exercise 4.7 Prove: a is a quadratic residue in $\mathbb{F}_q \iff a^{(q-1)/2} = 1$.

Definition 4.8 $a \in \mathbb{F}_q$ is a **quadratic non-residue** if $(\forall b)(a \neq b^2)$.

Exercise 4.9 Prove: a is a quadratic non-residue in $\mathbb{F}_q \iff a^{(q-1)/2} = -1$.

Exercise 4.10 Prove: in \mathbb{F}_q , the number of quadratic residues equals the number of quadratic non-residues; so there are $(q-1)/2$ of each. (As before, q is an odd prime power.)

Definition 4.11 Let q be an odd prime power. We define the **quadratic character** $\chi: \mathbb{F}_q \rightarrow \{0, 1, -1\} \subset \mathbb{C}$ by

$$\chi(a) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \\ -1 & \text{if } a \text{ is a non-residue} \\ 0 & \text{if } a = 0 \end{cases}$$

Note that if $q = p$ (i.e. prime and not prime power) then $\chi(a) = \left(\frac{a}{p}\right)$.

Exercise 4.12 Prove χ is multiplicative.

Exercise 4.13 The Legendre Symbol is completely multiplicative in the numerator.

Exercise 4.14 Prove that -1 is a quadratic residue in \mathbb{F}_q if and only if $q \equiv 1 \pmod{4}$.

Exercise 4.15 Prove that $\sum_{a \in \mathbb{F}_q} \chi(a(a-1)) = -1$. *Hint.* Divide by a^2 .

Exercise 4.16 Prove that each of the four pairs $(\pm 1, \pm 1)$ occur a roughly equal number of times ($\approx q/4$) as $(\chi(a), \chi(a-1))$ ($a \in \mathbb{F}_q$). “Roughly equal” means the difference is bounded by a small constant. Moral: for a random element $a \in \mathbb{F}_q$, the values of $\chi(a)$ and $\chi(a-1)$ are nearly independent.

Exercise 4.17 Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial over \mathbb{F}_q ($a, b, c \in \mathbb{F}_q$, $a \neq 0$). Prove: if $b^2 - 4ac \neq 0$ then $|\sum_{a \in \mathbb{F}_q} \chi(f(a))| \leq 2$. What happens if $b^2 - 4ac = 0$?

Exercise 4.18 $a^2 + b^2 \not\equiv -1 \pmod{4}$.

Exercise* 4.19 (Gauss) Prove: a prime p can be written as the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Hint. The necessity is clear from the preceding exercise. For sufficiency, assume $p \equiv 1 \pmod{4}$. Then $\left(\frac{-1}{p}\right) = 1$ and therefore $(\exists a)(p | a^2 + 1)$. Consider the lattice (plane grid) $L \subset \mathbb{Z}^2$ consisting of all integral linear combinations of the vectors $(a, 1)$ and $(p, 0)$. Observe that if $(x, y) \in L$ then $p | x^2 + y^2$. Moreover, the area of the fundamental parallelogram of the lattice is p . Apply Minkowski’s Theorem (below) to this lattice to obtain a nonzero lattice point (x, y) satisfying $x^2 + y^2 < 2p$. (This proof is due to P. Turán.)

5 Lattices and diophantine approximation

Definition 5.1 An n -dimensional *lattice* (grid) is the set L of all integral linear combinations $\sum_{i=1}^n a_i \mathbf{b}_i$ of a basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of \mathbb{R}^n ($a_i \in \mathbb{Z}$). The set of those linear combinations with $0 \leq a_i \leq 1$ ($a_i \in \mathbb{R}$) form a *fundamental parallelepiped*.

Exercise 5.2 The volume of the fundamental parallelepiped of the lattice L is $\det(L) := |\det(\mathbf{b}_1, \dots, \mathbf{b}_n)|$.

Exercise* 5.3 (Minkowski's Theorem) Let L be an n -dimensional lattice and let V be the volume of its fundamental parallelepiped. Let $A \subset \mathbb{R}^n$ be an n -dimensional convex set, symmetrical about the origin (i. e., $-A = A$), with volume greater than $2^n V$. Then $A \cap L \neq \{0\}$, i. e., A contains a lattice point other than the origin.

Hint. Linear transformations don't change the proportion of volumes, and preserve convexity and central symmetry. So WLOG $L = \mathbb{Z}^n$ with $\{\mathbf{b}_i\}$ the standard basis. The fundamental parallelepiped is now the unit cube C . Consider the lattice $2L = (2\mathbb{Z})^n$. Then the quotient space $\mathbb{R}^n / (2\mathbb{Z})^n$ can be identified with the cube $2C$ which has volume 2^n . Since A has volume $> 2^n$, there exist two points $u, v \in A$ which are mapped to the same point in $2C$, i. e., all coordinates of $u - v$ are even integers. Show that $(u - v)/2 \in A \cap L$.

Exercise 5.4 Finding "short" vectors in a lattice is of particular importance. Prove the following corollary to Minkowski's Theorem:

$$(\exists v \in L)(0 < \|v\|_\infty \leq (\det L)^{1/n}.$$

Definition 5.5 Let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$. A simultaneous ϵ -approximation of the α_i is a sequence of fractions p_i/q with a common denominator $q > 0$ such that $(\forall i)(|q\alpha_i - p_i| \leq \epsilon)$.

Exercise+ 5.6 (Dirichlet) $(\forall \alpha_1, \dots, \alpha_n \in \mathbb{R})(\forall \epsilon > 0)(\exists$ an ϵ -approximation with the denominator satisfying $0 < q \leq \epsilon^{-n}$).

Hint. Apply the preceding exercise to the $(n+1)$ -dimensional lattice L with basis $\mathbf{e}_1, \dots, \mathbf{e}_n, \mathbf{f}$ where $\mathbf{f} = \sum_{i=1}^n \alpha_i \mathbf{e}_i + \epsilon^{n+1} \mathbf{e}_{n+1}$ and $\{\mathbf{e}_1, \dots, \mathbf{e}_{n+1}\}$ is the standard basis.