Chapter 11

Rational approximations to real numbers

11.1. The pigeonhole principle

Exercise 11.1.1. Prove that for any irrational real number α there are arbitrarily small real numbers of the form $a + b\alpha$ with $a, b \in \mathbb{Z}$.

Exercise 11.1.2 (Simultaneous approximation)**.** Suppose that $\alpha_1, \dots, \alpha_k$ are given real numbers. Prove that for any positive integer N there exists a positive integer $n \le N^k$ such that, for each j in the range $1 \le j \le k$, there exists an integer m_j for which

$$|n\alpha_j - m_j| \;<\; \frac{1}{N}.$$

Deduce that given $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ there exist integers q, $1 \le q \le Q$, and $p_1, \dots, p_k$ such that

$$\left|\alpha_1 - \frac{p_1}{q}\right| \le \frac{1}{q^{1+1/k}}, \quad \left|\alpha_2 - \frac{p_2}{q}\right| \le \frac{1}{q^{1+1/k}}\ , \dots, \ \left|\alpha_k - \frac{p_k}{q}\right| \le \frac{1}{q^{1+1/k}}.$$

Exercise 11.1.3. Suppose that $\alpha_1, \dots, \alpha_k$ are given real numbers. Prove that for any positive integer N there exist integers $n_1, n_2, \dots, n_k$, not all zero, with each $|n_j| \le N$, and an integer m for which

$$|n_1\alpha_1 + n_2\alpha_2 + \cdots + n_k\alpha_k - m| \;<\; \frac{1}{N^k}.$$

11.2. Pell's equation

Exercise 11.2.1. Show that $y \ne 0$ using the fact that $(m, n) = 1$ for each such pair m, n.

Exercise 11.2.2. Prove that if $a + \sqrt{d}b = x + \sqrt{d}y$ where a, b, x, y, d are integers and d is not a square, then $a = x$ and $b = y$.

Exercise 11.2.3. Prove, by induction, that $x_{n+2} = 2x_1x_{n+1} - x_n$ and $y_{n+2} = 2x_1y_{n+1} - y_n$ for all $n \ge 0$.

Exercise 11.2.4. Show that all solutions to Pell's equation (not just the positive integer solutions) are given by the values $\pm(x_1 + \sqrt{d}y_1)^n$ (not just "+"), with $n \in \mathbb{Z}$ (not just $n \in \mathbb{N}$).

Exercise 11.2.5. The smallest solution to $x^2 - 2y^2 = 1$ is given by $(x, y) = (3, 2)$, which implies that 2^3 and 3^2 are consecutive *powerful numbers* (integer n is powerful if p^2 divides n whenever a prime p divides n). Use the theory of the solutions to $x^2 - 2y^2 = 1$ to prove that there are infinitely many pairs of consecutive powerful numbers.

11.3. *Descent on solutions of* $x^2 - dy^2 = n,\ d > 0$

Exercise 11.3.1. Find all integer solutions x, y to (a) $x^2 - 5y^2 = -4$; (b) $x^2 - 5y^2 = 4$; (c) $x^2 - 5y^2 = -1$; (d) $x^2 - 5y^2 = 1$; (e) $x^2 - 5y^2 = -20$; (f) $x^2 - 5y^2 = -11$.

Exercise 11.3.2. Prove that for any non-square positive integer d and integer n there is either no solution or infinitely many solutions to $x^2 - dy^2 = n$.

11.4. Transcendental numbers

Exercise 11.4.1. Prove that if $\alpha \in \mathbb{C}\setminus\mathbb{R}$, then there exists a constant $\beta_\alpha > 0$ such that $|\alpha - p/q| \geq \beta_\alpha$ for all rational approximations p/q.

Exercise 11.4.2. Prove that if $f(t) = a_d \prod_{i=1}^{d}(t - \alpha_i)$, then $f'(\alpha_i) = a_d \prod_{j=1,\ j\neq i}^{d}(\alpha_i - \alpha_j)$.

11.5. *The* abc*-conjecture*

Exercise 11.5.1. Let α be an algebraic number which is a root of $f(t) \in \mathbb{Z}[t]$, a polynomial of degree d. Let $F(x, y) = y^d f(x/y)$, and suppose that there exists a constant $\kappa > 0$ such that $|F(m, n)| \geq \kappa |n|^{d-2-\epsilon}$ for all integers m, n. Deduce that there exists a constant $c > 0$ such that $|\alpha - m/n| > c/n^{2+\epsilon}$ for all integers $m, n \neq 0$. (Thus Corollary 11.5.1 is "equivalent" to Roth's Theorem.)

Additional exercises

Exercise 11.6.1. Suppose $(p, q) = 1$ and $q \geq 1$. Determine *all* rationals m/n for which $\left|\frac{p}{q} - \frac{m}{n}\right| = \frac{1}{qn}$.

Exercise 11.6.2. Reprove exercise 7.10.21(a) using (11.0.1).

Exercise 11.6.3.[†] Prove that there are infinitely many solutions to the Pell equation $u^2 - dv^2 = 1$ with $u \equiv 1 \pmod d$.

Exercise 11.6.4. Prove that if α is transcendental, then so is α^k for every non-zero integer k.

Exercise 11.6.5 (The "three gaps" theorem).[‡] Given $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, we put the fractional parts $\{\alpha\}, \{2\alpha\}, \ldots, \{N\alpha\} \in [0, 1)$ in ascending order as $0 < \{a_1\alpha\} < \{a_2\alpha\} < \cdots < \{a_N\alpha\} < 1$ (so that $\{a_1, \ldots, a_N\}$ is a reordering of $\{1, \ldots, N\}$). We will prove that there are at most three distinct values in the set of consecutive differences, $D(A) := \{\{a_{j+1}\alpha\} - \{a_j\alpha\} : j = 1, \ldots, N-1\}$.

(a) Show that if $\{(a_{j+1} - 1)\alpha\} - \{(a_j - 1)\alpha\} \notin D(A)$, then either $a_j = 1$ or $a_{j+1} = 1$, or there exists k such that $\{(a_j - 1)\alpha\} < \{a_k\alpha\} < \{(a_{j+1} - 1)\alpha\}$.

(b) Show that if $\{(a_j - 1)\alpha\} < \{a_k\alpha\} < \{(a_{j+1} - 1)\alpha\}$, then $a_k = N$.

(c) Deduce from (a) and (b) that every element of $D(A)$ equals one of $\{a_1\alpha\}$, $1 - \{a_N\alpha\}$, or $\{a_1\alpha\} + 1 - \{a_N\alpha\}$.

Exercise 11.6.6. Suppose that a and b are given integers, with $3 \nmid a$.

(a) Show that we can select a congruence class $r \pmod 3$ such that if integer $m \equiv r \pmod 3$, then $x + y\sqrt{3} = (2 + \sqrt{3})^m(a + b\sqrt{3})$, then 3 divides y.

(b) Deduce that if integer N can be written in the form $a^2 - 3b^2$ where $3 \nmid N$, then there are infinitely many pairs of powerful numbers that differ by exactly N.

Exercise 11.6.7. Find an explicit value that can be used for c_α in Liouville's Theorem when $\alpha = \sqrt{D}$ where $D > 1$ is a squarefree positive integer.

Exercise 11.6.8. Fix $\epsilon > 0$, and integers $a_0, \dots, a_d$. Deduce from Roth's Theorem that there are only finitely many pairs of coprime integers m, n for which $|a_0 n^d + a_1 n^{d-1} m + \cdots + a_d m^d| \leq \max\{|m|, |n|\}^{d-2-\epsilon}$.

Exercise 11.6.9. Assume the *abc*-conjecture to show that there are only finitely many sets of integers $x, y > 0$ and $p, q > 1$ for which $x^p - y^q = 1$.

Exercise 11.6.10. Suppose that $x^p + y^q = z^r$ with x, y, z pairwise coprime and $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.

(a) Prove that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{42}$.

(b) Assume the *abc*-conjecture. Prove that there exists a constant B for which $|x^p|, |y^q|, |z^r| < B$.

Exercise 11.6.11. The *abc*-conjecture is "best possible" in that one cannot take $\epsilon = 0$. To establish this, we need to find examples of solutions to $a + b = c$ in which $(1/c)\prod_{p|abc} p$ gets arbitrarily small.

(a) Prove that if $m^2 | b$, then $\prod_{p|b} p \leq b/m$.

(b) Prove that for any odd integer m there exists an integer n for which $2^n \equiv 1 \pmod{m^2}$.

(c)† Combine these two observations to show that for any $\epsilon > 0$ there exist coprime integers $a + b = c$ for which $\prod_{p|abc} p < \epsilon c$.

Appendix 11A. Uniform distribution

11.7. $n\alpha$ mod 1

Exercise 11.7.1. Show that the conclusion of the theorem is not true if α is rational.

Exercise 11.7.2. Prove Kronecker's Theorem when $n\alpha \pmod 1 \in (1 - \epsilon, 1)$.

Exercise 11.7.3. (a) Show that $\sum_{n=1}^N e(\{n\alpha\}) = \frac{e(N\alpha)-1}{1-e(-\alpha)}$ if $\alpha \notin \mathbb{Z}$, and then deduce that $|\sum_{n=1}^N e(\{n\alpha\})| \leq \frac{1}{|\sin \pi\alpha|}$.

(b) Use Weyl's uniform distribution theorem to deduce that if α is a real, irrational number, then $\{n\alpha\}_{n\geq 1}$ is uniformly distributed mod 1.

Exercise 11.7.4. Let $x_1, x_2, \ldots \in [0, 1)$ be a sequence of numbers. Suppose that there are arbitrarily large integers M for which

$$\lim_{N\to\infty} \frac{1}{N} \# \left\{ n \leq N : \frac{m}{M} \leq x_n \leq \frac{m+1}{M} \right\} \text{ exists and equals } \frac{1}{M},$$

for $0 \leq m \leq M - 1$. Deduce that $\{x_n\}_{n\geq 1}$ is uniformly distributed mod 1.

Exercise 11.7.5.‡ Let α be a real, irrational number. In this exercise we sketch a proof that $\{n\alpha\}_{n\geq 1}$ is uniformly distributed mod 1. Fix $\epsilon > 0$ arbitrarily small.

(a) Use Kronecker's Theorem to show that there exists an integer $N \geq 1$ such that $\{N\alpha\} = \delta \in (0, \epsilon)$.

(b) Prove that if $\{n\alpha\} < 1 - \delta$, then $\{(n + N)\alpha\} = \{n\alpha\} + \delta$. What if $\{n\alpha\} \geq 1 - \delta$?

(c) Suppose that $0 < t < 1 - 2\delta$. Show that $\{n\alpha\} \in [t, t + \delta]$ if and only if $\{(n + N)\alpha\} \in [t + \delta, t + 2\delta]$, and so deduce that

$$|\#\{1 \leq n \leq x : t \leq \{n\alpha\} < t + \delta\} - \#\{1 \leq n \leq x : t + \delta \leq \{n\alpha\} < t + 2\delta\}| \leq N.$$

Now let $\delta = 1/M$ for some large integer M.

(d)† Use (c) to show that if $0 \leq m \leq M - 1$, then

$$\left| \# \left\{ 1 \leq n \leq x : \frac{m}{M} \leq \{n\alpha\} < \frac{m+1}{M} \right\} - \frac{x}{M} \right| \leq MN.$$

(e) Deduce that $\{n\alpha\}_{n\geq 1}$ is uniformly distributed mod 1 using exercise 11.7.4.

Kronecker's Theorem in n dimensions.

Exercise 11.7.6. Let $\alpha_1, \ldots, \alpha_k, \theta_1, \ldots, \theta_k \in \mathbb{R}$ be given, and assume that there are integers $c_0, \ldots, c_k$ for which $c_0 + c_1\alpha_1 + \cdots + c_k\alpha_k = 0$. Suppose that for all $\epsilon > 0$ there are infinitely many n for which $\|n\alpha_j - \theta_j\| < \epsilon$ for $j = 1, 2, \ldots, k$. Prove that $c_1\theta_1 + \cdots + c_k\theta_k \in \mathbb{Z}$.

11.8. Bouncing billiard balls

Exercise 11.8.1. Show that by rescaling with the map $x \to x/\ell$, $y \to y/w$ we can assume, without any loss of generality, that the billiards table is the unit square.

Exercise 11.8.2. Show that the billiard ball is at (x, y) after time t, where x and y are given as follows:
Let $m = [u + t]$. If m is even, let $x = \{u + t\}$; if m is odd, let $x = 1 - \{u + t\}$.
Let $n = [v + \alpha t]$. If n is even, let $y = \{v + \alpha t\}$; if n is odd, let $y = 1 - \{v + \alpha t\}$.

Exercise 11.8.3. Show that if α is rational, then the ball eventually ends up exactly where it started from, and so it does not get arbitrarily close to every point on the table.

So how close does the trajectory get to the point (r, s), where $r, s \in [0, 1)$? Let us consider all of those values of t for which $x = r$, with m and n even to simplify matters (with m and n as in exercise 11.8.2), and see if we can determine whether y is ever close to s.

Exercise 11.8.4. Show that $[z]$ is even if and only if $\{z/2\} \in [0, 1/2)$. Deduce that $[z]$ is even and $\{z\} = r$ if and only if $\{z/2\} = r/2$.

Exercise 11.8.5. Imagine a trajectory inside the unit circle. A ball is hit and continues indefinitely. When it hits a side at angle θ (compared to the normal line at that point), it bounces off at angle $-\theta$.

(a) Suppose that the first two points at which the ball hits the edge are at $e(\beta)$ and then at $e(\beta + \alpha)$. Show that the ball hits the edge at $e(\beta + n\alpha)$ for $n = 0, 1, 2, \ldots$.
(b) Prove that the ball falls into a repeated trajectory if and only if α is rational.
(c) Show that if α is irrational, then the points at which the ball hits the circle edge are dense (i.e., eventually the ball comes arbitrarily close to any point on the edge) but that it never hits the same edge point twice.
(d) Prove that the ball's trajectory never comes inside the circle of radius $|\cos(\alpha/2)|$. Deduce that the trajectory of the ball is *never* dense inside the unit circle.
(e) Prove that if α is irrational, then the trajectory of the ball is dense inside the ring between the circle of radius $|\cos(\alpha/2)|$ and the circle of radius 1. (The technical word for a ring is an *annulus*.)

Appendix 11B. Continued fractions

11.9. Continued fractions for real numbers

Exercise 11.9.1. Explain why if α has a finite length continued fraction, then the last term is an integer ≥ 2.

Exercise 11.9.2. Show that if a, b, A, B, u, v are positive reals, then $\frac{au+Av}{bu+Bv}$ lies between $\frac{a}{b}$ and $\frac{A}{B}$.

Exercise 11.9.3. Deduce that
$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_{2j}}{q_{2j}} < \cdots < \frac{p_{2j+1}}{q_{2j+1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$
and that p_n/q_n tends to a limit as $n \to \infty$.

Exercise 11.9.4. Show how to use the continued fraction to determine, for any irrational real number α, arbitrarily small real numbers of the form $a + b\alpha$ with $a, b \in \mathbb{Z}$.

11.10. How good are these approximations?

Exercise 11.10.1. Deduce that if $1 \leq q < q_n$, then $\left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p}{q}\right|$.

Exercise 11.10.2. Show that if $-\sqrt{d}+\frac{1}{2} < p^2 - dq^2 \leq \sqrt{d}$ with $p, q \geq 1$, then p/q is a convergent in the continued fraction for $\sqrt{d}$.

Exercise 11.10.3. Show that if $d \equiv 1 \pmod 4$ and $\frac{-\sqrt{d}+1}{2} < p^2 - pq + (\frac{1-d}{4})q^2 \leq \frac{\sqrt{d}}{2}$ with $p, q \geq 1$, then p/q is a convergent in the continued fraction for $\frac{1+\sqrt{d}}{2}$.

Exercise 11.10.4. Show that $\frac{1+\sqrt{5}}{2} = [1, 1, 1, 1, \ldots]$ and so the convergents are F_{n+1}/F_n where F_n is the nth Fibonacci numbers. By using the general formula for Fibonacci numbers, determine how good these approximations are; i.e., prove a strong version of the formula in section 11.4:

$$\left|\frac{1+\sqrt{5}}{2} - \frac{F_{n+1}}{F_n} + \frac{(-1)^n}{\sqrt{5}F_n^2}\right| \leq \frac{1}{5F_n^4}.$$

11.11. Periodic continued fractions and Pell's equation

Exercise 11.11.1. What numbers have continued fraction $[a, b, a, b, a, \ldots]$ where a and b are integers ≥ 1? Can you use this to find solutions to a family of Pell equations?

11.12. Quadratic irrationals and periodic continued fractions

Exercise 11.12.1. Deduce that the continued fraction for α is eventually periodic.

Exercise 11.12.2. Prove that if $a = 1$, then $a_n \leq \sqrt{d} + 1$ for all $n \geq 3$ in (11.12.2).

Exercise 11.12.3. Prove that $\sqrt{d} + [\sqrt{d}]$ has a periodic continued fraction for any squarefree integer $d > 1$.

11.13. Solutions to Pell's equation from a well-selected continued fraction

Exercise 11.13.1. Prove that if $b_{n+j} = b_j$ for all $j \geq 1$, then m divides n.

11.14. Sums of two squares from continued fractions

Exercise 11.14.1. The number $\phi = \frac{1+\sqrt{5}}{2}$ satisfies the equation $\phi = 1 + 1/\phi$.

(a) Iterate this to obtain $\phi = 1 + 1/(1 + 1/\phi)$, and then reprove the first part of exercise 11.10.4.

(b) Show that if α is the positive root of $x^2 - ax - b = 0$ where a and b are positive integers, then

$$\alpha = a + \cfrac{b}{a + \cfrac{b}{a + \cfrac{b}{a + \cdots}}}.$$

Exercise 11.14.2. Let $\phi = \frac{1+\sqrt{5}}{2}$.

(a) Show that $\phi = \sqrt{1+\phi}$.

(b) Iterate this to obtain $\phi = \sqrt{1+\sqrt{1+\phi}}$, and then prove that

$$\frac{1+\sqrt{5}}{2} = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\cdots}}}}.$$

(c) Show that if α is the positive root of $x^2 - ax - b = 0$ where a and b are positive integers, then

$$\alpha = \sqrt{b + a\sqrt{b + a\sqrt{b + a\sqrt{b+\cdots}}}}.$$

Exercise 11.14.3 (Hermite, Serret 1848).‡ We give an efficient way to determine, for a given prime $p \equiv 1 \pmod 4$, integers a and b for which $p = a^2 + b^2$: Let $r^2 \equiv -1 \pmod p$ with $0 < r < p/2$, and write $p/r = [a_0, \dots, a_n]$. We will show that $n = 2m+1$ is odd and a and b can be determined from $a/c = [a_0, a_1, \dots, a_m]$ and $b/d = [a_0, a_1, \dots, a_{m-1}]$.

(a) Use that $a_n \geq 2$ to deduce that $0 < s < p/2$ where $s/\ell = [a_0, a_1, \dots, a_{n-1}]$.

(b) Prove that $s = r$ and $n = 2m+1$ for some integer m.

(c) Show that $a_j = a_{n-j}$ for $j = 0, 1, \dots, n$.

(d) Show that $p = a^2 + b^2$.

Appendix 11C. Two-variable quadratic equations

11.15. Integer solutions to 2-variable quadratics

Exercise 11.15.1. What happens in the exceptional cases $a = b = c = 0$ and $b^2 - 4ac = 0$?

Appendix 11D. Transcendental numbers

11.16. Diagonalization

Exercise 11.16.1. Any given algebraic number α has a minimum polynomial $\sum_{i=0}^d a_i x^i \in \mathbb{Z}[x]$ with $d \geq 1$. Assign a weight $w(\alpha) := d\sum_{i=0}^d |a_i|$.

(a) Prove that there are finitely many α of any given weight.

(b) Deduce that the algebraic numbers are countable.

Exercise 11.16.2. Reprove the last result using the bijection $\mathbb{Z}[x] \leftrightarrow \mathbb{Q}$ defined by

$$a_0 + a_1 x + \cdots + a_d x^d \leftrightarrow 2^{a_0} 3^{a_1} \cdots p_{d+1}^{a_d},$$

where $p_1 = 2 < p_2 < \cdots$ is the sequence of primes. Can you construct a bijection $\mathbb{Z}[x] \leftrightarrow \mathbb{Z}$?

11.17. The hunt for transcendental numbers

Exercise 11.17.1. Suppose that e is rational, say $e = p/q$, and let $r = q!(1 + 1/1! + \cdots + 1/q!)$.

(a) Show that r is an integer and therefore $q! \cdot \frac{p}{q} - r$ is an integer.

(b) Prove that $q!e - r \in (0, 1)$.

(c) Use these remarks to establish a contradiction.

Exercise 11.17.2. Given $f(x) \in \mathbb{C}[x]$, define $F(x) := f(x) - f^{(2)}(x) + f^{(4)}(x) - f^{(6)}(x) + \cdots$ where $f^{(k)}(x) = \frac{d^k f}{dx^k}$.

(a) Prove that $\frac{d}{dx}(F'(x)\sin x - F(x)\cos x) = f(x)\sin x$.
(b) Deduce that $\int_0^\pi f(x)\sin x \, dx = F(\pi) + F(0)$.
(c) Show that if $f(x) = f(\pi - x)$, then $F(\pi) = F(0)$.
(d) Now, suppose that π is rational, say $\pi = p/q$, and let $f(x) = x^n(p - qx)^n/n!$ for some integer $n \geq 1$. By establishing that $f^{(k)}(0)$ is an integer for all $k \geq 0$, prove that $F(0)$ and $F(\pi)$ are integers.
(e) Show that if $0 < x < \pi$, then $0 < f(x) < (\frac{\pi^2}{4}q)^n/n!$.
Assume that $n > \frac{\pi^2}{4} \cdot eq$.
(f) In exercise 4.14.2 we proved that $n! > 2n^n/e^n$. Deduce that if $0 < x < \pi$, then $0 < f(x) < \frac{1}{2}$.
(g) Prove that $\int_0^\pi |\sin x| dx = 2$, and deduce that $0 < \int_0^\pi f(x)\sin x \, dx < 1$.
(h) Combine the above to deduce that π is irrational.

Exercise 11.17.3. Let $\alpha := \sqrt{2}^{\sqrt{2}}$. We wish to show that there exist irrational numbers x, y such that x^y is rational. Use either α or $\alpha^{\sqrt{2}}$ to prove this.

Exercise 11.17.4. Prove that if β is transcendental, then $a_0 + a_1\beta + \cdots + a_n\beta^n$ is also transcendental whenever the $a_j \in \overline{\mathbb{Q}}$ (the set of algebraic numbers, which is the *algebraic closure* of $\mathbb{Q}$) with $n \geq 1$ and $a_n \neq 0$.

11.18. Normal numbers

Exercise 11.18.1. Complete the details of the proof of the equivalence of normality in base b, and the sequence $\{nb^{m-1}\}_{m\geq 1}$ being uniformly distributed mod 1.