Lecture 1

M. Klazar

September 30, 2025

Chapter 1. Diophantine approximations

Dirichlet's theorem

Recall that fractions $\frac{p}{q}$ are pairs of integers p, q $(\in \mathbb{Z})$ with $q \neq 0$, that the set of fractions is denoted by $\mathbb{Q}$, and that we have $\frac{p}{q} = \frac{r}{s}$ iff $ps = qr$. We say that a fraction $\frac{p}{q}$ is in *lowest terms* if $q > 0$ and $(p, q) = 1$ (the greatest common divisor of p and q is 1). We may and will assume that the denominator $q > 0$.

Proposition 1. *If $\frac{p}{q} \neq \frac{r}{s}$ are fractions, then their distance*

$$\left|\frac{r}{s} - \frac{p}{q}\right| \geq \frac{1}{sq}\,.$$

Proof. Indeed, $\frac{r}{s} - \frac{p}{q} = \frac{rq-sp}{sq}$ and the numerator is a nonzero integer. $\square$

In other words, if $\alpha \in \mathbb{Q}$ then for every fraction $\frac{p}{q} \neq \alpha$ we have

$$\left|\alpha - \frac{p}{q}\right| \gg \frac{1}{q}$$

— no fraction α can be well approximated by other fractions. We will show that every irrational real number has infinitely many good approximations by fractions.

We denote the set of real numbers by $\mathbb{R}$, and the set of natural numbers $\{1, 2, \dots\}$ by $\mathbb{N}$. We denote nonnegative integers $\{0, 1, \dots\}$ by $\mathbb{N}_0$. For $\alpha \in \mathbb{R}$, *the integer part* of α is denoted by $\lfloor \alpha \rfloor$. It is the maximum $m \in \mathbb{Z}$ such that $m \leq \alpha$. *The fractional part* of α is $\{\alpha\} := \alpha - \lfloor \alpha \rfloor$ $(\in [0, 1))$. The following theorem and corollary are due to the German mathematician Peter L. Dirichlet (1805–1859)

Theorem 2 (P. L. Dirichlet, 1842). *Let $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$ with $Q \geq 2$. Then there exist integers p and q such that*

$$1 \leq q < Q \ \text{ and } \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}\,.$$

Proof. Let α and Q be as stated. Among the $Q+1$ numbers

$$0,\, \{\alpha\},\, \{2\alpha\},\, \dots,\, \{(Q-1)\alpha\},\, 1$$

in the interval $[0,1]$ some two, but not 0 and 1, have distance $\le \frac{1}{Q}$. Thus there exist integers a, b, c and d such that $0 \le a < b < Q$ and

$$|(b\alpha - c) - (a\alpha - d)| \le Q^{-1}\,.$$

Setting $q := b - a$ and $p := c - d$, and dividing the inequality by q, we get $1 \le q < Q$ and

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

$\square$

Corollary 3 (P. Dirichlet, 1842). *For every number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ there exist infinitely many distinct fractions $\frac{p}{q} \in \mathbb{Q}$ such that*

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

Proof. Let α be an irrational real number. We define an infinite sequence of distinct fractions $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots$ such that for every n,

$$\left|\alpha - p_n/q_n\right| < q_n^{-2}\,.$$

We begin with $q_1 := 1$ and $p_1 := \lfloor \alpha \rfloor$. Suppose that $\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}$ are already defined. We take $Q \in \mathbb{N}$ such that $Q^{-1} < |\alpha - p_i/q_i|$ for every $i = 1, 2, \dots, n$ (this is possible due to irrationality of α) and use Theorem 2:

$$\left|\alpha - p/q\right| < 1/qQ$$

for some integers p, q with $1 \le q < Q$. We may set $\frac{p_{n+1}}{q_{n+1}} := \frac{p}{q}$ because $\frac{1}{qQ} < \frac{1}{q^2}$ and $\frac{1}{qQ} \le \frac{1}{Q}$, so that $\frac{p}{q} \ne \frac{p_i}{q_i}$ for every $i = 1, 2, \dots, n$. $\square$

We use Theorem 2 to prove the old result of Leonhard Euler (1707–1783) that every prime number $p = 4n + 1$ is a sum of two squares. Thus $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$ and so on. Also, $2 = 1^2 + 1^2$. On the other hand, it is easy to see by reduction modulo 4 that no prime number $p = 4n + 3$ is a sum of two squares. For the proof we need a lemma.

Lemma 4. *For every prime number $p = 4n + 1$ there is a number $m \in \mathbb{N}$ such that p divides $m^2 + 1$.*

Proof. We use the algebraic result that the set $\mathbb{Z}_p$ of p residues modulo p forms a field with respect to addition and multiplication modulo p. Let $M := \mathbb{Z}_p \setminus \{0 \bmod p\}$. We consider the partition of the set M in blocks

$$\{a,\, -a,\, a^{-1},\, -a^{-1}\} \;\; (a \in M)\,.$$

Each has 4 or 2 distinct elements. The latter case occurs iff $a = \pm a^{-1}$, that is, iff $a^2 = \pm 1$. Hence we have one or two two-element blocks:

$$\{1 \bmod p,\, -1 \bmod p\} \text{ and, possibly, } \{m \bmod p,\, -m \bmod p\}$$

if m^2 is -1 modulo p for some $m \in \mathbb{N}$. Since M has $p - 1 = 4n$ elements, there are two two-element blocks and the numbers m exist. □

Theorem 4 (L. Euler, 1747). *For every prime number $p = 4n+1$ there exist numbers $a, b \in \mathbb{N}$ such that*

$$p = a^2 + b^2\,.$$

Proof. Let p be a prime number that is 1 modulo 4. Using the previous lemma we set

$$\alpha := \frac{m}{p} \text{ and } Q := \lfloor\sqrt{p}\rfloor + 1$$

where $m \in \mathbb{N}$ is such that m^2 is -1 modulo p. By Theorem 2 there exist integers a and b such that $1 \le b < Q$ and $\big|m/p - a/b\big| \le 1/bQ$. It follows that

$$0 \le \left|\frac{m}{p} - \frac{a}{b}\right| < \frac{1}{b\sqrt{p}} \text{ and } 1 \le b < \sqrt{p}\,.$$

Multiplying the first bound by pb, squaring the result and adding to it the squared second bound $1 \le b^2 < p$ we get

$$1 \le (mb - pa)^2 + b^2 < p + p = 2p\,.$$

Since

$$(mb - pa)^2 + b^2 = (m^2+1)b^2 - 2mbpa + (pa)^2$$

is zero modulo p, we see that $(mb - pa)^2 + b^2 = p$. □

In 1985 the Dutch mathematician René Schoof (1955) found in [4] a deterministic algorithm that finds in time polynomial in $\log p$ for each input prime $p = 4n+1$ the decomposition $p = a^2 + b^2$. See [5] for more information.

Farey fractions

Let $n \in \mathbb{N}$. We consider the finite ordered list

$$F_n := \left(0 = \frac{p_0}{q_0} < \frac{p_1}{q_1} < \cdots < \frac{p_{m_n}}{q_{m_n}} = 1\right)$$

consisting of the fractions in $[0,1]$ such that every $\frac{p_i}{q_i}$ is in lowest terms and $q_i \le n$. The entries in F_n are so-called *Farey fractions* of order n. They were introduced by the geologist John Farey (1766–1826) in 1816. For example,

$$F_5 = \left(\tfrac{0}{1} < \tfrac{1}{5} < \tfrac{1}{4} < \tfrac{1}{3} < \tfrac{2}{5} < \tfrac{1}{2} < \tfrac{3}{5} < \tfrac{2}{3} < \tfrac{3}{4} < \tfrac{4}{5} < \tfrac{1}{1}\right).$$

Note that every two consecutive entries have minimum possible distance, the reciprocal of the product of denominators (cf. Proposition 1). For example, $\frac{1}{3} - \frac{1}{4} = \frac{1}{12}$ or $\frac{3}{5} - \frac{1}{2} = \frac{1}{10}$. This general property of Farey fractions was proven by Augustin-Louis Cauchy (1789–1857).

Theorem 5 (A.-L. Cauchy, 1816). *Every two consecutive fractions in F_n have minimum possible distance, for every $i \in \mathbb{N}_0$ with $i < m_n$ we have*

$$\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{1}{q_{i+1}q_i}\,.$$

Equivalently, $q_i p_{i+1} - p_i q_{i+1} = 1$.

Proof. We set $\frac{a}{b} := \frac{p_i}{q_i}$, $\frac{c}{d} := \frac{p_{i+1}}{q_{i+1}}$ and consider the equation

$$bx - ay = 1\,.$$

Since $(b, a) = 1$, it has some solution $x, y \in \mathbb{Z}$. (We consider the ideal $I = \{\alpha a + \beta b\colon\ \alpha, \beta \in \mathbb{Z}\}$ in the ring $\mathbb{Z}$. Division with remainder shows that the minimum positive element $e \in I$ divides every element of I, in particular a and b. Thus $e = 1$.) We show that c, d is a solution.

If $x, y \in \mathbb{Z}$ is a solution, then so is $x - ra, y - rb$ for any integer r. Thus for every interval $J \subset \mathbb{Z}$ of length b there exist a solution $x, y \in \mathbb{Z}$ of the equation with $y \in J$. Hence we take a solution $x_1, y_1 \in \mathbb{Z}$ such that

$$n - b < y_1 \le n\,.$$

From $bx_1 - ay_1 = 1$ we get the expression

$$\frac{x_1}{y_1} = \frac{1}{by_1} + \frac{a}{b}\,.$$

We claim that $x_1/y_1 \in F_n$. Indeed, $bx_1 - ay_1 = 1$ shows that $(x_1, y_1) = 1$, $0 \le n - b < y_1 \le n$ and $0 \le x_1 = \frac{1}{b} + \frac{a}{b}y_1 \le y_1$ because $\frac{a}{b} < 1$, hence $\frac{a}{b} \le 1 - \frac{1}{b}$. It follows that $x_1/y_1 \ge c/d$. We show that strict inequality here leads to a contradiction.

So let us assume that $x_1/y_1 > c/d$. We add the bounds

$$\frac{x_1}{y_1} - \frac{c}{d} \ge \frac{1}{dy_1} \quad \text{and} \quad \frac{c}{d} - \frac{a}{b} \ge \frac{1}{bd}$$

of Proposition 1 and get, using the above expression, that

$$\frac{1}{by_1} = \frac{x_1}{y_1} - \frac{a}{b} \ge \frac{b + y_1}{bdy_1}\,.$$

Thus $d \ge b + y_1 > n$, which is a contradiction because $\frac{c}{d} \in F_n$.

Therefore $x_1/y_1 = c/d$. Since these are fractions in lowest terms, we see that $x_1 = c$ and $y_1 = d$. Thus c, d is a solution of the equation and

$$bc - ad = q_i p_{i+1} - p_i q_{i+1} = 1\,.$$

$\square$

The theorem of Hurwitz

How much can one strengthen Corollary 3? Is there a constant $c > 1$ such that for every $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ the inequality

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

has infinitely many rational solutions $\frac{p}{q}$? You can obtain such strengthening with $c = 2$ as an exercise, starting with the assumption that $\frac{a}{b} < \alpha < \frac{c}{d}$ for two consecutive Farey fractions of some order. The best possible strengthening with $c = \sqrt{5}$ was obtained by the German mathematician Adolf Hurwitz (1859–1919).

Theorem (A. Hurwitz, 1891). *The following is true.*

1. *For every $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$$

has infinitely many rational solutions $\frac{p}{q}$.

2. *Let $\beta := (\sqrt{5} - 1)/2$ and $c > \sqrt{5}$. Then the inequality*

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{cq^2}$$

has only finitely many rational solutions $\frac{p}{q}$.

Proof. 1. For details see [1]. I only say that now one employs three fractions, two consecutive Farey fractions $\frac{a}{b} < \frac{c}{d}$ (of some order) and their median $\frac{a+c}{b+d}$.

2. We assume for the contrary that $c > \sqrt{5}$ and that (p_n/q_n) is a sequence of distinct fractions such that $q_n \to +\infty$ as $n \to \infty$ and that for every n,

$$\beta = \frac{p_n}{q_n} + \frac{\delta_n}{q_n^2} \text{ with } \delta_n \in \mathbb{R} \text{ such that } |\delta_n| < 1/c\,.$$

Hence for every n,

$$\frac{\delta_n}{q_n} - \frac{q_n\sqrt{5}}{2} = q_n\beta - p_n - \frac{q_n\sqrt{5}}{2} = -\frac{q_n}{2} - p_n\,.$$

By squaring and subtracting $5q_n^2/4$ we get that for every n,

$$\frac{\delta_n^2}{q_n^2} - \delta_n\sqrt{5} = p_n^2 + p_nq_n - q_n^2\,.$$

For every $n \geq n_0$ the left-hand side is in absolute value < 1. For every n the right-hand side is an integer. Thus

$$p_n^2 + p_n q_n - q_n^2 = 0$$

for every $n \geq n_0$. But this is equivalent with $(2p_n + q_n)^2 - 5q_n^2 = 0$ and we get $\sqrt{5} \in \mathbb{Q}$, which is a contradiction. $\Box$

The lonely runner conjecture

An interesting and still unresolved conjecture in Diophantine approximations is the lonely runner conjecture.

> If $n \in \mathbb{N}$ runners on a circular track with unit length run with mutually distinct speeds, then each will be at some moment lonely, at least $1/n$ apart from other runners.

See [2] for more information and [3] for recent progress.

References

[1] M. Klazar, *Introduction to Number Theory*, 2006, `https://kam.mff.cuni.cz/~klazar/ln_utc.pdf`

[2] Lonely runner conjecture, Wikipedia article, `https://en.wikipedia.org/wiki/Lonely_runner_conjecture#For_specific_n`

[3] M. Rosenfeld, The lonely runner conjecture holds for eight runners, arXiv:2509.14111v1 [math.CO], 2025, 10 pp.

[4] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483–494

[5] Schoof's algorithm, Wikipedia article, `https://en.wikipedia.org/wiki/Schoof%27s_algorithm`