What is Diophantine analysis? (Lecture No. 1 21.07.2024).

1.Two Dirichlet theorems.
a. **Theorem 1.** *For any $\alpha \in \mathbb{R}$ and for any $Q \in \mathbb{Z}_+$ there exists $q \in \mathbb{Z}_+$ satisfying*

$$1 \leqslant q \leqslant Q, \quad ||q\alpha|| \leqslant \frac{1}{Q}, \quad ||x|| = \min_{a \in \mathbb{Z}} |x - a| \; - \; \textit{distance to the nearest integer}$$

b. **Theorem 2.** *For any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ there exist infinitely many rational fractions $\frac{p}{q}$ such that*

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

2. Optimality. For any fraction $\frac{p}{q}$ one has

$$\left| \sqrt{2} - \frac{p}{q} \right| \geqslant \frac{c}{q^2}$$

with some positive constant c.

3. Algebraic numbers. A number $\alpha \in \mathbb{C}$ is called algebraic if there exists a non-zero polynomial $P(x) \in \mathbb{Q}[x]$ such that $P(\alpha) = 0$.
a. Do there exist (real) numbers which are not algebraic?
b. **Theorem.** *For any algebraic number α there exists the unique* **minimal polynomial** $P_\alpha(x)$ *satisfying*
1) $P_\alpha(x) \in \mathbb{Q}[x]$;
2) $P_\alpha(\alpha) = 0$;
3) the leading coefficient of $P_\alpha(x)$ is equal to 1.
4) $P_\alpha(x)$ has minimal degree among all the polynomials satisfying 1), 2), 3).

The degree $\deg \alpha$ of an algebraic number α is defined as the degree of the polynomial $P_\alpha(x)$.

4. a. **Liouville theorem.** *Let α be an algebraic number of degree $n = \deg \alpha \geqslant 2$. Then there exists positive c_α such that*

$$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{c_\alpha}{q^n} \quad \forall \frac{p}{q}.$$

5. Some history: Thue-Siegel-Roth theorem. (We will not prove it.)*Let α be an algebraic number of degree $n = \deg \alpha \geqslant 2$. Then for any $\varepsilon > 0$ there exists positive $c_{\alpha,\varepsilon}$ such that*

$$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{c_{\alpha,\varepsilon}}{q^\gamma} \quad \forall \frac{p}{q} \in \mathbb{Q},$$

where A. Thue: $\gamma = \frac{n}{2} + 1 + \varepsilon$; C. Roth: $\gamma = 2 + \varepsilon$.

S. Lang's conjecture: for algebraic α the following statement holds: $\exists c, \beta$ such that

$$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{c}{q^2 (\log q)^\beta} \quad \forall \frac{p}{q}.$$

Exercises.

0. Prove $||x+y|| \leqslant ||x|| + ||y||$.
1. "Very precise" Dirichlet theorem.
a. For any $Q \in \mathbb{Z}_+$ there exists $q \in \mathbb{Z}_+$ such that $||q\alpha|| \leqslant \frac{1}{Q+1}$, $q \leqslant Q$;
b. for any $\tau \geqslant 1$ there exists q such that $||q\alpha|| < \frac{1}{\tau}$, $q \leqslant \tau$;
c. for any $\tau \geqslant 1$ there exists an irreducible fraction $\frac{p}{q}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\tau q}, \quad 1 \leqslant q \leqslant \tau.$$

2. Golden section. Prove that for any $\varepsilon > 0$ the inequality

$$\left|\frac{\sqrt{5}+1}{2} - \frac{p}{q}\right| \leqslant \frac{1-\varepsilon}{\sqrt{5}\, q^2}.$$

has only finite number of solutions in fractions $\frac{p}{q} \in \mathbb{Q}$. (Suggestion: $q^2 \left|\frac{\sqrt{5}+1}{2} - \frac{p}{q}\right| \cdot \left|\frac{\sqrt{5}+1}{2} - \frac{p}{q} - \sqrt{5}\right| \in \mathbb{Z}_+$.)

3. Prove theorem about minimal polynomial.

4. Minimal polynomial. What are the degrees and the minimal polynomials for
 a) $\sqrt[3]{2}$?
 b) $\sqrt{2} + \sqrt{3}$?
(Suggestion for a.: $x^3 - 2$ has no rational roots.)

4. Is Liouville's theorem valid for complex algebraic nubers?

6. Transcendental numbers. Prove that the numbers are not algebraic:

$$a.\ \sum_{n=0}^{\infty} \frac{1}{2^{n!}};\ b.\ \sum_{n=0}^{\infty} \frac{1}{2^{2^{n^2}}};\quad c.\ \sum_{n=0}^{\infty} \frac{1}{3^{n!}}.$$

Introduction to Continued Fractions (Lecture No. 2, 22.07.2024).

1. What is Euclidean algorithm and how it is related to continued fractions of rational numbers?

2. Formal infinite continued fraction.

$$[a_0; a_1, a_2, ..., a_\nu, ...], \quad a_0 \in \mathbb{Z}, \quad a_j \in \mathbb{Z}_+, j = 1, 2, 3, ... \tag{1}$$

a_j - partial quotients,

$$\frac{p_\nu}{q_\nu} = [a_0; a_1, a_2, ..., a_\nu] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_\nu}}}, \quad (p_\nu, q_\nu) = 1 - \text{ convergents.}$$

3. Recursive formulas for the convergents' numerators and denominators.

$$p_{\nu+1} = a_{\nu+1} p_\nu + p_{\nu-1}, \quad q_{\nu+1} = a_{\nu+1} q_\nu + q_{\nu-1}, \quad p_\nu q_{\nu-1} - q_\nu p_{\nu-1} = (-1)^{\nu-1}.$$

4. The value of continued fraction (1). Prove that
a. $\frac{p_{2\nu}}{q_{2\nu}}$ is an increasing sequence;
b. $\frac{p_{2\mu+1}}{q_{2\mu+1}}$ is a decreasing sequence;
c. $\frac{p_{2\nu}}{q_{2\nu}} < \frac{p_{2\mu+1}}{q_{2\mu+1}}$ for all μ, ν;
d. $\left|\frac{p_\nu}{q_\nu} - \frac{p_{\nu+1}}{q_{\nu+1}}\right| = \frac{1}{q_\nu q_{\nu+1}}$;
e. there exists $\lim_{\nu\to\infty} \frac{p_\nu}{q_\nu}$ which is called the value of continued fraction (1).

5. For every real number α there exists a continued fraction of the form (1) which value is α.

6. Problem of uniqueness. Prove that every irrational number has the unique representation as a value of a continued fraction of the form (1). What happens with rational numbers, and what is the correct statement about uniqueness for rationals?

7. Prove that

$$||q_\nu \alpha|| = \frac{1}{q_\nu(\alpha_{\nu+1} + \alpha_\nu^*)},$$

where

$$\alpha_{\nu+1} = [a_{\nu+1}; a_{\nu+2}, a_{\nu+3}, ...], \quad \alpha_\nu^* = [0; a_\nu, a_{\nu-1}, ..., a_1].$$

8. **Lagrange Theorem.** *α is a quadratic irrationality if and only if its continued fraction is eventually periodic.*

9. **Zaremba's Conjecture.**

$$\forall\, q \in \mathbb{Z}_+ \quad \exists\, a : \quad (a, q) = 1 \text{ such that in c.f. expansion } \frac{a}{q} = [0; a_1, ..., a_t] \text{ one has } \quad a_j \leqslant 5, \ \forall j.$$

(We will not prove it.)

Exercises.

1. Prove that for any α and for any ν one has $q_\nu \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{\nu-1}$.

2. **Valen's Theorem.** *For any ν either*

$$q_\nu ||q_\nu \alpha|| < 1/2,$$

or

$$q_{\nu+1}||q_{\nu+1}\alpha|| < 1/2$$

holds.

3. Suppose that in (1) $a_0 \geqslant 1$. Prove that $\frac{p_n}{p_{n-1}} = [a_n; a_{n-1}, ..., a_0]$.

4. Prove that
a. $\sqrt{d^2+1} = [d; \overline{2d}]$;
b. $\sqrt{d^2+2} = [d; \overline{d, 2d}]$;
c. $[\underbrace{2; 2, ..., 2}_{n}] = \frac{(1+\sqrt{2})^{n+1}-(1-\sqrt{2})^{n+1}}{(1+\sqrt{2})^{n}-(1-\sqrt{2})^{n}}$.

5. Prove that each rational number $\frac{a}{b}$ can be represented in a form

$$b_0 - \cfrac{1}{b_1 - \cfrac{1}{b_2 - \cdots - \cfrac{1}{b_\nu}}} \tag{2}$$

with $b_j \geqslant 2, j = 1, 2, ..., \nu$.

6. Prove Zaremba's Conjecture for
a. $q = F_n$ - Fibonacci numbers;
b. $q = 2^n$;
c. for all the numbers of the form $q = 2^n 3^m$;
d. for representation of rationals as continues fractions (2), that is, you should prove that for any $q \in \mathbb{Z}_+$ there exists $a \in \mathbb{Z}$ such that $(a, q) = 1$ and in the decomposition

$$b_0 - \cfrac{1}{b_1 - \cfrac{1}{b_2 - \cdots - \cfrac{1}{b_\nu}}}$$

we have $b_j \leqslant 5\, \forall j$.