Analytic and Combinatorial Number Theory 2025: two theorems of Roth, the PNT and Dirichlet's theorem on primes in AP

Martin Klazar

March 6, 2025

(lecture notes for the course taught in summer term 2025)

Contents

Introduction

These lecture notes

Notation.

Chapter 1

Roth's theorem on Diophantine approximation

In the first chapter ...

1.1 Liouville's inequality and Thue equations

Recall that $\alpha \in \mathbb{C}$ is *algebraic* if $\sum_{j=0}^{n} c_j \alpha^j = 0$, $n \in \mathbb{N}$, for some $n+1$ fractions $c_j \in \mathbb{Q}$ where $c_n \neq 0$. The least such n is called the *degree* of α. Non-algebraic numbers are also called *transcendental*. In 1844 the French mathematician *Joseph Liouville (1809–1882)* found the first examples of transcendental numbers. His method of obtaining them is based on the following lower bound on approximability of irrational algebraic numbers by fractions.

Theorem 1.1 (Liouville, 1844) *If $\alpha \in \mathbb{R}$ is an algebraic (irrational) number with degree $n \geq 2$, then there is a constant $c = c(\alpha) > 0$ such that*

$$\left|\alpha - \tfrac{p}{q}\right| > cq^{-n}$$

for every fraction $\frac{p}{q} \in \mathbb{Q}$.

Proof.

□

Corollary 1.2 *For every $k \in \mathbb{N}$, $k \geq 2$, the real number $\lambda_k = \sum_{j=1}^{\infty} k^{-j!}$ is transcendental.*

Proof. The fractions $\frac{p_m}{q_m} = \sum_{j=1}^{m} k^{-j!}$, $m = 1, 2, \ldots$, violate Liouville's inequality for λ_k for every $c > 0$ and every $n \in \mathbb{N}$. Thus λ_k is transcendental. Fill in details as an exercise. □

A *Thue equation* is a Diophantine equation with two unknowns x and y and the form

$$F(x,\, y) = \textstyle\sum_{j=0}^{n} c_j x^j y^{n-j} = m\,,$$

where $n \in \mathbb{N}$, $n \geq 3$, $c_j, m \in \mathbb{Z}$ and $c_n \neq 0$, and where $F(x, y) \in \mathbb{Z}[x, y]$ is such that the univariate polynomial $F(x, 1) \in \mathbb{Z}[x]$ with degree n is irreducible over $\mathbb{Q}[x]$. For example, the simplest Thue equations are

$$x^3 - 2y^3 = m \;\; (\in \mathbb{Z})\,.$$

In fact, every Thue equation has only finitely many solutions $x, y \in \mathbb{Z}$, but it is very hard to prove it.

This contrasts with the fact, well known to those who attended my course *Introduction to Number Theory*, that for every $d \in \mathbb{N}$ that is not a square and every $m \in \mathbb{Z}$, $m \neq 0$, the *generalized Pell equation*

$$x^2 - dy^2 = m$$

has infinitely many (integral) solutions if it has at least one solution $x, y \in \mathbb{Z}$. (It is easy to see that $x^2 - dy^2 = 0$ has only the trivial solution $x = y = 0$.) Thus, for example, each of the equations

$$x^2 - 2y^2 = 1,\; -1,\; 2,\; -2,\; 4,\; -4,\; 7,\; -7,\; \ldots$$

has infinitely many (integral) solutions.

The finiteness of solution sets of Thue equations would easily follow from any non-trivial strengthening of Liouville's inequality in Theorem 1.1 for degrees $n \geq 3$. Those who attended my course *Introduction to Number Theory* know very well that for the degree $n = 2$ it cannot be non-trivially strengthened (only by some constant factors) because the following theorem, due to the German mathematician *Peter L. Dirichlet (1805–1859)*, holds.

Theorem 1.3 (Dirichlet, 1842) *For every irrational number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ there exist infinitely many fractions $\frac{p}{q} \in \mathbb{Q}$ such that*

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

But for degrees $n \geq 3$ we have the following reduction.

Proposition 1.4 (a reduction) *If it is true that for every algebraic number $\alpha \in \mathbb{R}$ with degree $n \geq 3$ there is a function $\omega(q) = \omega(q, \alpha)\colon \mathbb{N} \to (0, +\infty)$ such that $\omega(q) \to +\infty$ as $q \to \infty$ and for every fraction $\frac{p}{q} \in \mathbb{Q}$, $q > 0$, it holds that*

$$\left|\alpha - \tfrac{p}{q}\right| > \omega(q) q^{-n}\,,$$

then every Thue equation $F(x, y) = m$ has only finitely many solutions $x, y \in \mathbb{Z}$.

Proof.

□

In view of the simplicity of the proof of Theorem 1.1, one might think that it might not be too difficult to improve upon the argument and obtain the function $\omega(q)$. The truth is that it can be done and the required $\omega(q)$ can be obtained, but it is quite hard. The first who succeeded in a breakthrough result was the Norwegian mathematician *Axel Thue (1863–1922)*. Thue equations were named after him to honor this achievement.

Theorem 1.5 (Thue, 1909) *Suppose that $\alpha \in \mathbb{R}$ is an algebraic number with degree $n \geq 3$ and that $\varepsilon > 0$. Then the inequality*

$$\left|\alpha - \tfrac{p}{q}\right| < q^{-n/2-1-\varepsilon} = q^{-n} \cdot q^{n/2-1-\varepsilon}$$

has only finitely many rational solutions $\frac{p}{q} \in \mathbb{Q}$, $q > 0$.

It is easy to see that this gives the reduction in Proposition 1.4 with the function $\omega(q) = c(\alpha, \varepsilon) \cdot q^{n/2-1-\varepsilon}$, for every $\varepsilon > 0$ and some constants $c(\alpha, \varepsilon) > 0$ depending only on α and ε.

1.2 Roth's first theorem: auxiliary results

Theorem 1.6 (Roth, 1955) *Let α be a real algebraic irrational number and $\varepsilon > 0$. Then the inequality*

$$\left|\alpha - \tfrac{p}{q}\right| < q^{-2-\varepsilon}$$

has only finitely many rational solutions $\frac{p}{q} \in \mathbb{Q}$, $q > 0$.

Lemma 1.7 (4A) *Let $m, r_1, \ldots, r_m \in \mathbb{N}$ and $\varepsilon \in (0, 1)$. Then*

$$\begin{aligned} &\left|\left\{(i_1, \ldots, i_m) \in \textstyle\prod_{h=1}^m [r_h]_0 \colon \left|\sum_{h=1}^m \frac{i_h}{r_h} - \frac{m}{2}\right| \geq \varepsilon m\right\}\right| \\ &\leq 2(r_1 + 1) \ldots (r_m + 1) \cdot \mathrm{e}^{-\varepsilon^2 m/4}. \end{aligned}$$

Proof.

□

Lemma 1.8 (4B) *Let $n \in \mathbb{N}$ and $r \in \mathbb{N}_0$. Then*

$$|\{(i_1, \ldots, i_n) \in \mathbb{N}_0^n \colon r_1 + \cdots + r_n = r\}| = \tbinom{r+n-1}{r}.$$

Proof. The LHS is the coefficient of x^r in expanded $(1 + x + x^2 + \ldots)^n$, which is $(1 - x)^{-n} = \sum_{r \geq 0} \binom{-n}{r}(-1)^r x^r$. Thus the LHS is $\binom{-n}{r}(-1)^r = \binom{n+r-1}{r}$. □

Lemma 1.9 (4C) *Let* $n, m, r_1, \dots, r_m \in \mathbb{N}$, $n \geq 2$ *and* $\varepsilon \in (0,1)$. *Then*

$$\Big|\Big\{\big(i_{h,\,k}\big)_{h,\,k=1}^{m,\,n} \in \mathbb{N}_0^{m\times n}:\ \sum_{k=1}^{n} i_{h,\,k} = r_h \ \text{ for } h \in [m] \text{ and } \Big|\sum_{h=1}^{m} \frac{i_{h,\,1}}{r_h} - \frac{m}{n}\Big| \geq \varepsilon m\Big\}\Big| \leq 2\binom{r_1+n-1}{r_1}\dots\binom{r_m+n-1}{r_m}\cdot \mathrm{e}^{-\varepsilon^2 m/4}\,.$$

Proof.

□

Lemma 1.10 (5B, Siegel's lemma) $M, N \in \mathbb{N}$, $N > M$, *for* $j \in [M]$ *we have* M *linear forms*

$$L_j(\overline{z}) = \sum_{k=1}^{N} a_{j,k} z_k$$

with N *variables* z_k *and coefficients* $a_{j,k} \in \mathbb{Z}$ *such that always* $|a_{j,k}| \leq A$. *Then there exists an* N*-tuple* $\overline{z} \in \mathbb{Z}^N$ *such that* $\overline{z} \neq \overline{0}$, $L_j(\overline{z}) = 0$ *for every* $j \in [M]$ *and for every* $k \in [N]$,

$$|z_k| \leq \lfloor (NA)^{M/(N-M)} \rfloor\,.$$

Proof.

□

Bibliography

[1] W. M. Schmidt, *Diophantine Approximation*, Springer-Verlag, Berlin 1980

[2] V. Šmidt, *Diofantovy približenija*, Mir, Moskva 1983 (translated from English by V. G. Čirskij, revised by A. B. Šidlovskij)