Lecture 1. Theorems of Dirichlet and Hurwitz

M. Klazar

Oct 4, 2024

We use $\equiv$ as the defining equality sign; $x \equiv y$ defines the new symbol x by the already known expression y. Sometimes x and y may exchange their roles. $\mathbb{N} = \{1, 2, \dots\}$, $\mathbb{N}_0 = \{0, 1, \dots\}$, $\mathbb{Z}$ are the integers, $\mathbb{Q}$ are the fractions and $\mathbb{R}$ are the real numbers. For $n \in \mathbb{N}$ we set $[n] \equiv \{1, 2, \dots, n\}$. For $m, n \in \mathbb{Z}$ we write $(m, n) = 1$ to express that m and n are coprime, their largest common divisor is 1. Every number $\alpha \in \mathbb{R}$ decomposes uniquely as the sum

$$\alpha = \lfloor \alpha \rfloor + \{\alpha\}$$

of the *(lower) integer part* $\lfloor \alpha \rfloor \in \mathbb{Z}$ and the *fractional part* $\{\alpha\} \in [0, 1)$. By $\lceil \alpha \rceil$ we denote the *upper integer part*, the smallest integer $\geq \alpha$. Let $\|\alpha\| \equiv \min(\{\{\alpha\}, \lceil \alpha \rceil - \alpha\})$ $(\in [0, \frac{1}{2}])$ be the distance of α from the nearest integer.

The next theorem and corollary are due to Dirichlet in [2].

Theorem 1 (P. Dirichlet, 1842) *For every $\alpha \in \mathbb{R}$ and every $Q \in \mathbb{N}$ with $Q \geq 2$ there exist $p, q \in \mathbb{Z}$ such that $1 \leq q < Q$ and*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq}\ .$$

Proof. We consider Q numbers $\{n\alpha\}$ $(\in [0, 1))$ for $n = 0, 1, \dots, Q - 1$. We can think of them as points lying on a circle with circumference 1. Two of them have arc distance $\leq \frac{1}{Q}$. It means that for some $m, n, r, s \in \mathbb{Z}$ with $0 \leq n < m < Q$,

$$|m\alpha - r - (n\alpha - s)| \leq \frac{1}{Q}\ .$$

We set $p \equiv r - s$, $q \equiv m - n$, divide the inequality by q and get that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq} \ \text{ with } \ 1 \leq q < Q\ .$$

□

Corollary 2 *For every $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ there exist infinitely many distinct fractions $\frac{p}{q}$ such that*

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

Proof. We construct infinitely many fractions $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$, ... such that for each the displayed inequality holds and $|\alpha - \frac{p_1}{q_1}| > |\alpha - \frac{p_2}{q_2}| > \cdots > 0$. We begin with $p_1 \equiv \lfloor \alpha \rfloor$ and $q_1 \equiv 1$. If $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ are already constructed, we take any $Q \in \mathbb{N}$ such that $|\alpha - \frac{p_n}{q_n}| > \frac{1}{Q}$ (this is possible, α is irrational) and use Dirichlet's theorem. We get a fraction $\frac{p}{q}$ such that $1 \le q < Q$ and $|\alpha - \frac{p}{q}| \le \frac{1}{Qq} < \frac{1}{q^2}$. Also, $|\alpha - \frac{p}{q}| \le \frac{1}{Q} < |\alpha - \frac{p_n}{q_n}|$. Thus we can set $p_{n+1} \equiv p$ and $q_{n+1} \equiv q$. □

In the proof of Theorem 1 we used the obvious (?) fact that among any n points on the *circle C with unit circumference* always some two have arc distance at most $\frac{1}{n}$. We mention an interesting, fifty six years old (still younger than me), related problem which is still unsolved. It is called the *Lonely Runner Conjecture*, see the interesting survey article [6].

Conjecture 3 (LRC) *If n runners start in the origin and run on C with distinct speeds then for each of them there is a moment when the $n-1$ arc distances to other runners are all at least $\frac{1}{n}$. Formally, for every n distinct real numbers $v_1, v_2, \ldots, v_n$ for every $i \in [n]$ there is a real number $t_i \ge 0$ such that for every $j \in [n] \setminus \{i\}$ we have that $\|v_i t_i - v_j t_i\| \ge \frac{1}{n}$.*

In [6] we read that the LRC is proven for every $n \le 7$ and that it is due to Wills [9] and Cusick [1]. You can prove as an exercise that the next simpler formulation is equivalent to the previous one.

Conjecture 4 (LRC) *For every n nonzero real numbers $v_1, v_2, \ldots, v_n$ there exists a real number t such that for every $i \in [n]$ we have that $\|v_i t\| \ge \frac{1}{n+1}$.*

To obtain an optimum strengthening of Corollary 2, which is Theorem 6 below, we need *Farey fractions*. For every $n \in \mathbb{N}$ we consider the ordered list

$$F_n \equiv \left(\tfrac{0}{1} = \tfrac{p_1}{q_1} < \tfrac{p_2}{q_2} < \cdots < \tfrac{p_m}{q_m} = \tfrac{1}{1}\right)$$

of all $m = m(n)$ fractions $\frac{p}{q} \in [0,1]$ such that $0 < q \le n$ and $(p,q) = 1$. These are the *Farey fractions (of order n)*. For example,

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

We read in the interesting and thorough survey [5] that the correct attribution of the next theorem is to Haros in [3].

Theorem 5 (Ch. Haros, 1802) *If $\frac{a}{b} < \frac{c}{d}$ are two consecutive fractions in the list F_n then*

$$\frac{c}{d} - \frac{a}{b} = \frac{1}{bd}$$

— in other words, $bc - ad = 1$.

Proof. Let $\frac{a}{b}$, $\frac{c}{d}$ and n be as stated. We need to show that the Diophantine equation

$$bx - ay = 1$$

has solution $x = c$ and $y = d$. Since $(a,b) = 1$, there is at least one solution $x_0, y_0 \in \mathbb{Z}$. Indeed, the set $I \equiv \{bx + ay : x, y \in \mathbb{Z}\}$ is an ideal in the ring $\mathbb{Z}$, both $a, b \in I$ and division with remainder shows that $c \equiv \min(\{x \in I : \ x > 0\})$ divides every element of I, thus $c = 1$ and $1 \in I$.

So $bx_0 - ay_0 = 1$ and we see that for any $r \in \mathbb{Z}$ the pair $x = x_0 - ra$ and $y = y_0 - rb$ is also a solution. It follows that there is a solution $x_1, y_1 \in \mathbb{Z}$ such that

$$n - b < y_1 \leq n \ .$$

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

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

We claim that $\frac{x_1}{y_1} \in F_n$. Indeed, from the above we see that $1 \leq y_1 \leq n$ and that $(x_1, y_1) = 1$. From $bx_1 - ay_1 = 1$ and $0 < a < b$ it follows that $0 < x_1 \leq y_1$.

Since $\frac{x_1}{y_1} \in F_n$ and $\frac{x_1}{y_1} > \frac{a}{b}$, it follows that $\frac{x_1}{y_1} \geq \frac{c}{d}$. We assume that $\frac{x_1}{y_1} > \frac{c}{d}$ and obtain a contradiction. By adding the trivial inequalities

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

we get that

$$\frac{1}{by_1} = \frac{x_1}{y_1} - \frac{a}{b} \geq \frac{1}{dy_1} + \frac{1}{bd} = \frac{b + y_1}{bdy_1} \ \text{ and hence } \ d \geq b + y_1 \ .$$

But we know that $b + y_1 > n$, and get the contradiction that $d > n$ (recall that $\frac{c}{d} \in F_n$).

Thus $\frac{x_1}{y_1} = \frac{c}{d}$. Since these are fractions in lowest terms, $x_1 = c$ and $y_1 = d$. Hence $x = c$ and $y = d$ is a solution of $bx - ay = 1$. □

The distance between two consecutive fractions $\frac{a}{b} < \frac{c}{d}$ in F_n is therefore minimum possible for two distinct fractions. Clearly, $0 < \frac{c}{d} - \frac{a}{b} \leq \frac{1}{n}$. It is interesting that their *mediant* $\frac{a+c}{b+d}$ of $\frac{a}{b}$ and $\frac{c}{d}$, which need not be in F_n, lies in the minimum distance to each fraction:

$$(a + c)b - (b + d)a = cb - da = 1 \ \text{ and } \ (b + d)c - (a + c)d = bc - ad = 1 \ .$$

If $\frac{a}{b} < \frac{c}{d} < \frac{e}{f}$ are three consecutive fractions in F_n then

$$\frac{a + e}{b + f} = \frac{c}{d}$$

— the middle fraction is the mediant of the outer two — prove it as an exercise.

The next optimum strengthening of Corollary 2 is due to Hurwitz in [4]. I learned the proof long time ago in [8] (the English original is [7]).

Theorem 6 (A. Hurwitz, 1891) 1. *For every $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ there exist infinitely many distinct fractions $\frac{p}{q}$ such that*

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

2. *On the other hand, for every real* $c > \sqrt{5}$*, the inequality*

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

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

Proof. 1. We make use of Farey fractions. We may assume, by replacing α with $\{\alpha\}$, that $0 < \alpha < 1$. As in the proof of Corollary 2 we construct a sequence of fractions $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ in $[0,1]$ such that for each the inequality in 1 holds and $|\alpha - \frac{p_1}{q_1}| > |\alpha - \frac{p_2}{q_2}| > \cdots > 0$.

We claim that $\frac{p_1}{q_1}$ may be one of the three fractions $\frac{0}{1}$, $\frac{1}{2}$ and $\frac{1}{1}$. This follows from the fact that the sum of the lengths of the intervals $[0, \frac{1}{\sqrt{5}}]$ and $[\frac{1}{2} - \frac{1}{4\sqrt{5}}, \frac{1}{2}]$ is larger than the length of $[0, \frac{1}{2}]$: $\frac{1}{\sqrt{5}} + \frac{1}{4\sqrt{5}} > \frac{1}{2}$ as $\frac{5}{16} > \frac{1}{4}$.

If $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ are defined, we take an $m \in \mathbb{N}$ such that $|\alpha - \frac{p_n}{q_n}| > \frac{1}{m} > 0$ (recall that α is irrational), take two consecutive fractions $\frac{a}{b} < \frac{c}{d}$ in the list F_m such that $\frac{a}{b} < \alpha < \frac{c}{d}$ and show that for a fraction

$$\frac{p}{q} \in \left\{\frac{a}{b}, \frac{e}{f} \equiv \frac{a+c}{b+d}, \frac{c}{d}\right\}$$

the inequality in 1 holds. Since $|\alpha - \frac{p}{q}| \le \frac{1}{m}$, it also holds that $|\alpha - \frac{p}{q}| < |\alpha - \frac{p_n}{q_n}|$, and we may set $p_{n+1} \equiv p$ and $q_{n+1} \equiv q$.

Suppose for the contrary that none of the three fractions satisfies the inequality in 1,

$$\alpha - \frac{a}{b} \ge \frac{1}{b^2\sqrt{5}} \wedge \pm\left(\alpha - \frac{e}{f}\right) \ge \frac{1}{f^2\sqrt{5}} \wedge \frac{c}{d} - \alpha \ge \frac{1}{d^2\sqrt{5}}\,.$$

If the sign is $+$ we add the first and third, and the second and third, inequality and get that $(+)$: $\frac{1}{bd} = \frac{c}{d} - \frac{a}{b} \ge \frac{1}{\sqrt{5}}(\frac{1}{b^2} + \frac{1}{d^2})$ and $\frac{1}{df} = \frac{c}{d} - \frac{e}{f} \ge \frac{1}{\sqrt{5}}(\frac{1}{f^2} + \frac{1}{d^2})$. If the sign is $-$ we add the first and second, and the first and third, inequality and get that $(-)$: $\frac{1}{bf} = \frac{e}{f} - \frac{a}{b} \ge \frac{1}{\sqrt{5}}(\frac{1}{b^2} + \frac{1}{f^2})$ and $\frac{1}{bd} = \frac{c}{d} - \frac{a}{b} \ge \frac{1}{\sqrt{5}}(\frac{1}{b^2} + \frac{1}{d^2})$. In $(+)$ and $(-)$ the equalities follow from Theorem 5 and the definition of $\frac{e}{f}$.

We show that the two inequalities in $(+)$ are contradictory. We multiply the first one by $b^2d^2\sqrt{5}$, the second one by $d^2f^2\sqrt{5}$, and add the results. We get that

$$d\sqrt{5}(2b+d) = d\sqrt{5}(b+f) \ge b^2 + 2d^2 + f^2 = 2b^2 + 3d^2 + 2bd\,.$$

This is equivalent with $0 \ge \frac{1}{2}((\sqrt{5}-1)d - 2b)^2$. Hence $(\sqrt{5}-1)d - 2b = 0$ and $\sqrt{5} \in \mathbb{Q}$, which is a contradiction.

We obtain the same contradiction in $(-)$. We multiply the first inequality by $b^2f^2\sqrt{5}$, the second one by $b^2d^2\sqrt{5}$, and add the results. We get that

$$b\sqrt{5}(b+2d) = b\sqrt{5}(f+d) \ge 2b^2 + f^2 + d^2 = 3b^2 + 2d^2 + 2bd\,.$$

It is the same contradiction as before, only b and d are interchanged.

2. Let $\beta \equiv \frac{\sqrt{5}-1}{2}$ and $c > \sqrt{5}$. Suppose for the contrary that there exist infinitely many (distinct) fractions $\frac{p}{q}$ such that $|\beta - \frac{p}{q}| < \frac{1}{q^2 c}$. Thus the equation

$$\beta = \frac{p}{q} + \frac{\delta}{q^2}$$

has infinitely many solutions $\frac{p}{q} \in \mathbb{Q}$ and $\delta \in (-\frac{1}{c}, \frac{1}{c})$. We rewrite it as

$$\frac{\delta}{q} - \frac{q\sqrt{5}}{2} = \left(q\beta - p - \frac{q\sqrt{5}}{2}\right) = -\frac{q}{2} - p\,.$$

We square the equation, subtract $\frac{5q^2}{4}$ and get that

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = p^2 + pq - q^2\,.$$

It follows that there is a solution $\frac{p}{q}$ and δ such that the left side is in absolute value less than 1. Then $p^2+pq-q^2 = 0$ which is equivalent with $(2p+q)^2 = 5q^2$. This is the familiar contradiction that $\sqrt{5} \in \mathbb{Q}$. □

References

[1] T. W. Cusick, View-obstruction problems, *Aequationes Math.* **9** (1973), 165–170

[2] L. P. G. Dirichlet, Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen, *S. B. Preuss. Akad. Wiss.* (1842), 93–95

[3] C. Haros, Tables pour évaluer une fraction ordinaire avec autand de decimals qu'on voudra; et pour trouver la fraction ordinaire la plus simple, et dui a approche sensiblement d'une fraction décimale, *Journal de l'École Polytechnique* **4** (1802), 364–368

[4] A. Hurwitz, Über die angenäherte Darstellung der Irrationalen durch rationale Brüche, *Math. Annalen* **39** (1891), 279–284

[5] P. Pavlíková, O Fareyových zlomcích, *Pokroky matematiky, fyziky a astronomie* **55** (2010), 97–110

[6] G. Perarnau and O. Serra, The Lonely Runner Conjecture turns 60, arXiv:2409.20160v1, 2024, 38 pp.

[7] V. M. Schmidt, *Diophantine Approximation*, Springer-Verlag, Berlin 1980

[8] V. Šmidt, *Diofantovy priblizheniya*, Mir, Moskva 1983

[9] J. M. Wills, Zur simultanen homogenen diophantische Aproximation. I, *Monats. Math.* **72** (1968), 254–263