Др Зоран Каделбург

ДИОФАНТОВЕ АПРОКСИМАЦИЈЕ[1]

Теорија Диофантових[2] апроксимација је грана теорије бројева у којој се проучавају апроксимације реалних бројева рационалним. Наравно, као што је добро познато, сваки реалан број се може произвољно добро апроксимирати рационалним; међутим, ако се при том за бројеве којима се врши апроксимација захтевају неки додатни услови, на пример, ограничава им се на одређени начин именилац, тада се захтевана тачност не може увек постићи.

Постоји више метода којима се ови проблеми проучавају. Међу најчешћима је метод *верижних (непрекидних) разломака* о којем је већ више пута било речи у овом часопису[3]. Овде ћемо приказати неке друге методе за испитивање Диофантових апроксимација.

1. Фарејев низ

Дефиниција 1. Фарејев[4] низ F_n је (коначан) низ свих редукованих разломака a/b интервала $[0,1]$ за које је $b \leqslant n$, поређаних по величини.

Пример 1. $F_5 = \left(\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right)$. $\triangle$

Теорема 1. *Нека* $\frac{a}{b} \in F_n$. *Нека је* $y \in \mathbf{Z}$, *такав да је* $n - b < y \leqslant n$ *и* $ay \equiv -1 \pmod{b}$ *и нека је* $x = \frac{ay+1}{b}$. *Тада је* $\frac{x}{y}$ *разломак који у* F_n *следи непосредно иза* $\frac{a}{b}$.

Приметимо да на основу познатих резултата у вези са линеарним конгруенцијама следи да су бројеви x, y који задовољавају наведене услове увек једнозначно одређени.

---

[1] Овај чланак представља део излагања у оквиру курса „Теорија бројева“ који је школске 1999/2000 године држан студентима специјалистичких студија за професоре математике на Математичком факултету у Београду.

[2] Диофант (3. век н. е.), старогрчки математичар

[3] в. нпр. Б. Малешевић: *Рационалне апроксимације реалних бројева и неке примене*, Настава математике XLIII, 3 (1998), 20–31.

[4] J. Farey (1766–1826), енглески математичар

Доказ. Из $x = \dfrac{ay+1}{b}$ следи $bx - ay = 1$ и $(x, y) = 1$. Из $y \leqslant n$ следи $\dfrac{x}{y} \in F_n$ и $\dfrac{x}{y} = \dfrac{a}{b} + \dfrac{1}{by} > \dfrac{a}{b}$. Нека је $\dfrac{c}{d}$ разломак у F_n који непосредно следи иза a/b и претпоставимо, супротно тврђењу, да је $\dfrac{a}{b} < \dfrac{c}{d} < \dfrac{x}{y}$. Тада је $xd - cy \geqslant 1$, $cb - ad \geqslant 1$ и

$$\frac{1}{by} = \frac{bx-ay}{by} = \frac{x}{y} - \frac{a}{b} = \left(\frac{x}{y} - \frac{c}{d}\right) + \left(\frac{c}{d} - \frac{a}{b}\right) = \frac{xd-cy}{dy} + \frac{cb-ad}{bd}$$
$$\geqslant \frac{1}{dy} + \frac{1}{db} = \frac{b+y}{bdy},$$

одакле $b + y \leqslant d \leqslant n$ (јер $\dfrac{c}{d} \in F_n$), па је $y \leqslant n - b$, што је контрадикција са начином избора броја y. ■

Пример 2. У F_{15} иза $\dfrac{4}{9}$ непосредно следи $\dfrac{5}{11}$, јер је $y = 11$ (једино) решење конгруенције $4y \equiv -1 \pmod 9$ у интервалу $6 < y \leqslant 15$, и $x = \dfrac{4 \cdot 11 + 1}{9} = 5$. △

Задатак 1. (Савезно такмичење 1971.) Ако су $a, b, p, q, r, s \in \mathbf{N}$, такви да је $qr - ps = 1$ и $\dfrac{p}{q} < \dfrac{a}{b} < \dfrac{r}{s}$, доказати да је $b \geqslant q + s$.

Последица 1. *Ако су* $\dfrac{a}{b} < \dfrac{c}{d}$ *суседни разломци у* F_n, *тада:* 1° $b + d > n$; 2° $bc - ad = 1$; 3° $(b, d) = 1$.

Доказ. Сва три тврђења лако следе из $n - b < d \leqslant n$, $ad \equiv -1 \pmod b$ и $c = \dfrac{ad+1}{b}$. ■

Последица 2. *Ако су* $\dfrac{a}{b} < \dfrac{x}{y} < \dfrac{c}{d}$ *узастопни чланови у* F_n, *тада је* $\dfrac{x}{y} = \dfrac{a+c}{b+d}$ *(медијанта бројева* $\dfrac{a}{b}$ *и* $\dfrac{c}{d}$*).*

Доказ. Из претходног следи да је $bx - ay = 1$, $cy - dx = 1$, одакле је $x = \dfrac{a+c}{bc-ad}$, $y = \dfrac{b+d}{bc-ad}$ и $\dfrac{x}{y} = \dfrac{a+c}{b+d}$. ■

Последица 3. *Сваки разломак из* F_{n+1} *са имениоцем* $n+1$ *лежи између два суседна разломка из* F_n *и њихова је медијанта.*

Дакле, да бисмо, знајући F_n, формирали F_{n+1}, довољно је наћи оне суседне разломке у F_n чији је збир именилаца $n + 1$.

Пример 3. $F_6 = \left(\dfrac{0}{1}, \dfrac{1}{6}, \dfrac{1}{5}, \dfrac{1}{4}, \dfrac{1}{3}, \dfrac{2}{5}, \dfrac{1}{2}, \dfrac{3}{5}, \dfrac{2}{3}, \dfrac{3}{4}, \dfrac{4}{5}, \dfrac{5}{6}, \dfrac{1}{1}\right)$. △

2. Најбоља апроксимација

Дефиниција 2. Рационалан број a/b је *најбоља апроксимација* броја $\alpha \in \mathbf{R}$ ако не постоји рационалан број $\dfrac{x}{y}$ за који је $y \leqslant b$ и $\left|\alpha - \dfrac{x}{y}\right| < \left|\alpha - \dfrac{a}{b}\right|$.

Другим речима, a/b је најбоља апроксимација броја α ако сви рационални бројеви интервала $(\alpha - a/b, \alpha + a/b)$ имају именилац већи од b.

Пример 4. $\dfrac{3}{2}$ је најбоља апроксимација броја $\sqrt{2}$, а $\dfrac{143}{100}$ то није (мада је његово растојање од $\sqrt{2}$ мање него растојање броја $\dfrac{3}{2}$), јер је $\dfrac{142}{100} = \dfrac{71}{50}$ ближи броју $\sqrt{2}$ него што је то $\dfrac{143}{100}$. $\triangle$

Теорема 2. *Ако $\alpha \in \mathbf{R} \cap (0,1)$ лежи између два суседна броја из F_n, тада је бар један од њих најбоља апроксимација за α.*

Приметимо да није искључено да и други од поменутих бројева буде најбоља апроксимација (макар му растојање од α било и веће).

Доказ. Нека су $\dfrac{a}{b}$ и $\dfrac{c}{d}$ узастопни чланови у F_n и $\dfrac{a}{b} < \alpha < \dfrac{c}{d}$; нека је при том растојање броја $\dfrac{a}{b}$ од α мање или једнако него растојање броја $\dfrac{c}{d}$. Тада је $\dfrac{a}{b}$ најбоља апроксимација броја α. Заиста, ако би $\dfrac{x}{y}$ био ближи α него што је то $\dfrac{a}{b}$, тада би $\dfrac{x}{y}$ припадао интервалу $\left(\dfrac{a}{b}, \dfrac{c}{d}\right)$. Пошто су $\dfrac{a}{b}$ и $\dfrac{c}{d}$ узастопни чланови у F_n, разломак $\dfrac{x}{y}$ не би припадао F_n, па би важило $y > n \geqslant b$. ■

Теорема 3. *Нека су $\dfrac{a}{b}$, $\dfrac{c}{d}$ узастопни чланови у F_n и $\dfrac{a}{b} < \alpha < \dfrac{c}{d}$. Тада међу редукованим разломцима са имениоцем $n+1$ најбоља апроксимација за α може бити једино $\dfrac{a+c}{b+d}$. Он то јесте ако и само ако је $b+d = n+1$ и његово растојање од α није веће него растојања $\dfrac{a}{b}$ и $\dfrac{c}{d}$ од α.*

Доказ. На основу последице 3, у скупу $F_n \cap \left(\dfrac{a}{b}, \dfrac{c}{d}\right)$ може се налазити само један елемент из F_{n+1} — то је медијанта $\dfrac{a+c}{b+d}$, и то само у случају да је $b+d = n+1$. Ако је тај услов испуњен и $\dfrac{a+c}{b+d}$ је заиста ближи α него што су то и $\dfrac{a}{b}$ и $\dfrac{c}{d}$, тада је он ближи броју α него сви остали чланови F_{n+1}. Обратно је очигледно. ■

Пример 5. Најбоље апроксимације броја $\ln 2 = 0{,}69314718\ldots$ са имениоцима мањим од 50 су: 1, $\dfrac{1}{2}$, $\dfrac{2}{3}$, $\dfrac{5}{7}$, $\dfrac{7}{10}$, $\dfrac{9}{13}$ и $\dfrac{34}{49}$. $\triangle$

Важан резултат теорије Диофантових апроксимација је следећа *Дирихлеова*[5] *теорема.*

Теорема 4. *Нека је α произвољан реалан број и $t \in \mathbf{N}$. Тада постоји рационалан број p/q, такав да важи*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qt} \quad \text{и} \quad q \leqslant t.$$

[5] P. G. L. Dirichlet (1805–1859), немачки математичар

Први доказ. Није ограничење општости ако се претпостави да је $0 \leqslant \alpha < 1$. Нека су $\frac{a}{b}$, $\frac{c}{d}$ суседни бројеви у F_t и $\frac{a}{b} \leqslant \alpha \leqslant \frac{c}{d}$. Нека је, на пример, $\frac{a}{b} \leqslant \alpha \leqslant \frac{a+c}{b+d}$. Тада је

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} < \frac{1}{bt},$$

јер је $bc - ad = 1$ и $b + d > t$ и при томе је $b \leqslant t$.

Други доказ. Посматрајмо $t+1$ бројева $\alpha x - [\alpha x]$ за $x = 0,\ 1,\ \ldots,\ t$. Сви они припадају интервалу $[0, 1)$. Поделимо тај интервал на t интервала

$$\left[0, \frac{1}{t}\right), \quad \left[\frac{1}{t}, \frac{2}{t}\right), \quad \ldots \quad , \quad \left[\frac{t-1}{t}, 1\right).$$

На основу Дирихлеовог принципа, бар један од тих интервала садржи два од датих бројева; нека су то бројеви $\alpha x_1 - [\alpha x_1]$ и $\alpha x_2 - [\alpha x_2]$ и нека је, на пример, $x_2 > x_1$. Тада је

$$\frac{1}{t} > \left|(\alpha x_2 - [\alpha x_2]) - (\alpha x_1 - [\alpha x_1])\right| = \left|\alpha(x_2 - x_1) - ([\alpha x_2] - [\alpha x_1])\right|.$$

Означимо $q = x_2 - x_1$, $[\alpha x_2] - [\alpha x_1] = p$ и важиће $0 < q \leqslant t$ и

$$|\alpha q - p| < \frac{1}{t}, \quad \text{тј.} \quad \left|\alpha - \frac{p}{q}\right| < \frac{1}{tq}. \quad \blacksquare$$

Поменимо да је претпоставка да је t природан број небитна; уз малу измену доказује се да теорема важи за сваки реалан број $t \geqslant 1$.

Претпоставимо сада да је, специјално, α ирационалан број. Докажимо да у том случају имениоци q разломака који апроксимирају број α у Дирихлеовој теореми могу бити произвољно велики, ако дозволимо да број t расте. Заиста, претпоставимо супротно, да су ти имениоци ограничени одозго неким бројем q_0 за све $t \in \mathbf{N}$. Означимо

$$\beta_q = \min_p \left|\alpha - \frac{p}{q}\right| \quad \text{за} \quad q \in \{1, 2, \ldots, q_0\}$$

и

$$\beta = \min_{1 \leqslant q \leqslant q_0} \beta_q.$$

Тада је $\beta > 0$ због ирационалности броја α и за свако $p \in \mathbf{Z}$ и $q \in \mathbf{N}$ важи неједнакост

$$\left|\alpha - \frac{p}{q}\right| \geqslant \beta.$$

Но, ова неједнакост за довољно велико t противречи неједнакости Дирихлеове теореме.

Приметимо даље да из неједнакости теореме следи да је, због $0 < q \leqslant t$,

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

Из претходно доказаног следи да последња неједнакост за ирационалне α има решења са имениоцима већим од произвољног унапред задатог броја. На тај начин, важи:

Последица 4. *За сваки ирационалан број α неједначина $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ има бесконачно много решења по $p \in \mathbf{Z}$, $q \in \mathbf{N}$.*

С друге стране, лако се доказује да важи

Теорема 5. *Ако је $\alpha \in \mathbf{Q}$, онда постоји реалан број $c > 0$, такав да је за сваки рационалан број $\frac{p}{q} \neq \alpha$ испуњена неједнакост:*

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{c}{q}.$$

Доказ. Нека је $\alpha = a/b$, $b \geqslant 1$. Ако је p/q произвољан рационалан број, $\frac{p}{q} \neq \frac{a}{b}$, онда је $aq - bp \neq 0$, па за цео број $|aq - bp|$ важи $|aq - bp| \geqslant 1$. Због тога је

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geqslant \frac{1}{bq} = \frac{1/b}{q}.$$

Дакле, за c се може узети $1/b$. ■

Задатак 2. Користећи претходну теорему доказати да је број

$$\alpha = 1 - \frac{1}{2^1} + \frac{1}{2^4} - \frac{1}{2^9} + \cdots + \frac{(-1)^n}{2^{n^2}} + \cdots$$

ирационалан.

Ако упоредимо резултате последице 4 и теореме 5, закључујемо да се ирационални бројеви могу „боље“ апроксимирати рационалним бројевима него сами рационални бројеви. Прецизније, уводи се:

Дефиниција 3. 1° Број $\alpha \in \mathbf{R}$ *допушта апроксимацију рационалним бројевима поретка* $\nu \in \mathbf{N}$ ако постоји константа $c = c_1(\alpha) > 0$ таква да неједначина

$$(*) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^\nu}$$

има бесконачно много решења по $\frac{p}{q} \in \mathbf{Q}$, $\frac{p}{q} \neq \alpha$.

2° $\nu = \nu(\alpha)$ је *најбољи поредак апроксимације* броја α рационалним бројевима, ако α допушта тај поредак и постоји константа $c = c_2(\alpha) > 0$ таква да неједначина $(*)$ нема решења.

Дакле:

1° за рационалне бројеве α је $\nu(\alpha) = 1$; неједнакост $\nu(\alpha) \leqslant 1$ следи из теореме 5, а $\nu(\alpha) \geqslant 1$ важи јер једначине $pb - aq = \pm 1$ за $(a, b) = 1$ увек имају бесконачно много решења;

2° за ирационалне бројеве α је $\nu(\alpha) \geqslant 2$, на основу последице 4. При том се може доказати да постоје бројеви α за које је баш $\nu(\alpha) = 2$; такав је, на пример, број $\alpha = \dfrac{1+\sqrt{5}}{2}$ (видети [1]).

Поставља се питање да ли се у овом смислу може извршити прецизнија класификација реалних бројева и, специјално, да ли постоје реални бројеви који допуштају произвољно велики поредак апроксимације. Да бисмо дали одговор, уведимо појмове алгебарских и трансцендентних бројева.

3. Алгебарски и трансцендентни бројеви

Дефиниција 4. Комплексан (специјално, реалан) број α је *алгебарски* ако је он корен неког полинома с целим коефицијентима који нису сви једнаки нули. Ако такав полином за број α не постоји, α је *трансценденатан*[6] број.

Јасно је да смо уместо захтева да полином о коме је реч има целе коефицијенте могли захтевати да су његови коефицијенти рационални бројеви (не сви једнаки нули). Посматраћемо овде углавном само реалне алгебарске бројеве.

Како из $f(\alpha) = 0$ следи $f(\alpha)g(\alpha) = 0$ за произвољан полином $g(x)$ са целим коефицијентима, јасно је да за сваки алгебарски број α постоји бесконачно много полинома с целим (рационалним) коефицијентима чији је он корен. Од свих таквих полинома обично се посматра онај најмањег степена.

Дефиниција 5. Број n је *степен* алгебарског броја α ако је α корен полинома степена n с целим (рационалним) коефицијентима и не постоји полином степена нижег од n с целим (рационалним) коефицијентима чији је α корен.

Очигледно је да су сви рационални бројеви алгебарски, и то степена 1. Но, постоји много алгебарских бројева који су ирационални — такви су нпр. сви бројеви облика $\sqrt[n]{a}$, $a \in \mathbf{N}$ који нису цели. Све квадратне ирационалности су алгебарски бројеви степена 2, а нпр. $\sqrt[3]{2}$ је алгебарски број степена 3 (доказати!).

Задатак 3. Доказати да је $\sin 10^\circ$ алгебарски број степена 3, а $\sqrt{2}+\sqrt{3}$ алгебарски број степена 4.

Основни резултат у вези са Диофантовим апроксимацијама алгебарских бројева је следећа *Лиувилова*[7] *теорема* (из 1844. године). Из ње ћемо, између осталог, моћи и да изведемо доказ о постојању трансцендентних бројева (што не следи из досадашњих разматрања).

Теорема 6. *За сваки реалан алгебарски број α степена $n \geqslant 2$ постоји таква позитивна константа c да је за сваки рационалан број p/q:*

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

[6] transcendo (лат.) – превазилазити; дакле, трансцендентан је број који „превазилази“ могућности алгебре

[7] J. Liouville (1809–1882), француски математичар.

Дакле, алгебарски ирационални бројеви не могу се „јако добро“ апроксимирати рационалним бројевима. Прецизније,

Последица 5. Најбољи поредак апроксимације алгебарског броја степена n није већи од n.

Доказ теореме 6. Нека је α корен полинома

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

с целим коефицијентима ($a_n \neq 0$, $n \geqslant 2$). Тада је $f(x) = (x-\alpha)g(x)$, где је $g(x)$ полином $(n-1)$-ог степена с реалним коефицијентима. Нека је p/q произвољан рационалан број. Он не може бити корен полинома $f(x)$, јер бисмо иначе једначину $f(x) = 0$ могли да скратимо са $x - p/q$ и α би био корен полинома са рационалним коефицијентима степена нижег од n. Зато је

$$\left| f\left(\frac{p}{q}\right)\right| = \frac{|a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n|}{q^n} \neq 0.$$

Но, тада је бројилац последњег разломка цео број, већи од нуле, па је већи или једнак 1. Зато:

$$\left| f\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{q^n}, \quad \text{тј.} \quad \left|\alpha - \frac{p}{q}\right| \cdot \left| g\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{q^n}.$$

Размотримо следећа два случаја:

1° $\dfrac{p}{q} \in [\alpha - 1, \alpha + 1] = I$. Функција $|g(x)|$ је непрекидна на затвореном интервалу I, па је ограничена:

$$\max_{x \in I} |g(x)| = K < +\infty.$$

Зато је

$$\frac{1}{q^n} \leqslant \left| f\left(\frac{p}{q}\right)\right| \leqslant K \left|\alpha - \frac{p}{q}\right|, \quad \text{односно} \quad \left|\alpha - \frac{p}{q}\right| \geqslant \frac{1/K}{q^n}.$$

2° $\dfrac{p}{q} \notin I$. Онда је $\left|\alpha - \dfrac{p}{q}\right| > 1$, па пошто је q цео број, свакако и

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^n}.$$

Сада је очигледно да $c = \min\{1, 1/K\}$ задовољава све услове теореме. ■

Последица 6. *Ако за свако $c > 0$ и свако $n \in \mathbf{N}$ постоји рационалан број $\dfrac{p}{q} \neq \alpha$, такав да је*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^n},$$

онда је α трансцендентан број. ■

Ево сада и најављеног примера који доказује постојање трансцендентних бројева.

Пример 6. Лиувилов број

$$L = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots = 0,11000100\ldots010\ldots$$

је трансцендентан.

Заиста, нека су $n \in \mathbf{N}$ и $c > 0$ произвољни. Посматрајмо бројеве

$$p = 10^{k!}\left(\frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{k!}}\right), \quad q = 10^{k!}.$$

За њих важи:

$$\begin{aligned}\left|L - \frac{p}{q}\right| &= \frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \cdots \\ &< \frac{1}{10^{(k+1)!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = \frac{2}{10^{k!}} \cdot \frac{1}{10^{k!\,k}}.\end{aligned}$$

Изаберимо k тако да је $k > n$ и $\dfrac{2}{10^{k!}} < c$. Тада је

$$\left|L - \frac{p}{q}\right| < \frac{c}{(10^{k!})^k} < \frac{c}{q^n},$$

па из претходне последице следи да је L трансцендентан број. $\triangle$

О неким побољшањима Лиувилове теореме видети, на пример, [1] или [5].

Коришћењем Канторове[8] теорије кардиналних бројева лако се изводи да трансцендентних бројева има и „више“ него алгебарских (прецизније, скуп алгебарских бројева је пребројив, а скуп трансцендентних то није). Међутим, то нимало не олакшава испитивање алгебарске природе неких конкретних бројева.

Бројеви e и π не само да су ирационални, већ су и трансцендентни. За број e то је први доказао Ермит[9] 1873. године, а за π Линдеман[10] 1882. године. Наводимо Ермитов доказ трансцендентности броја e.

Теорема 7. *Број e је трансцендентан.*

Доказ. Претпоставимо, супротно тврђењу, да постоје цели бројеви a_0, a_1, $\ldots$, a_n такви да је

$$a_0 + a_1 e + \cdots + a_n e^n = 0. \tag{1}$$

Нека је $M = \max_{0 \leqslant k \leqslant n} |a_k|$. Изаберимо довољно велики прост број p (тачан смисао услова „довољно велики“ разјаснићемо касније; за сада претпоставимо само да је $p > n$ и $p > |a_0|$) и посматрајмо полином

$$f(x) = \frac{x^{p-1}}{(p-1)!}(x-1)^p(x-2)^p \cdots (x-n)^p.$$

[8] G. Cantor (1845–1918), немачки математичар

[9] Ch. Hermite (1822–1901), француски математичар

[10] K. L. F. Lindeman (1852–1939), немачки математичар

За њега помоћу парцијалне интеграције добијамо

$$\begin{aligned}\int_0^x e^{x-t}f(t)\,dt &= -f(x)+e^x f(0)+\int_0^x e^{x-t}f'(t)\,dt\\ &= -[f(x)+f'(x)]+e^x[f(0)+f'(0)]+\int_0^x e^{x-t}f''(t)\,dt\\ &= \cdots = -[f(x)+f'(x)+\cdots]+e^x[f(0)+f'(0)+\cdots]\\ &= -F(x)+e^xF(0),\end{aligned}$$

где је (коначан) збир $f(x)+f'(x)+\cdots$ означен са $F(x)$. Стављајући у добијену релацију, редом, $x=k=0,1,\ldots,n$, множењем добијених релација, редом, са a_k и сабирањем, добијамо

$$\begin{aligned}(2)\quad &\sum_{k=0}^{n} a_k\int_0^k e^{k-t}f(t)\,dt =\\ &= -[a_0F(0)+a_1F(1)+\cdots+a_nF(n)]+F(0)[a_0+a_1e+\cdots+a_ne^n]=R,\end{aligned}$$

где је, на основу (1), $R=-[a_0F(0)+a_1F(1)+\cdots+a_nF(n)]$.

Проценимо сада изразе на обе стране релације (2). Развијањем израза за $f(x)$ добија се да је

$$f(x)=\frac{1}{(p-1)!}(A_{p-1}x^{p-1}+A_px^p+\cdots),\qquad A_i\in\mathbf{Z},$$

при чему је $f(0)=f'(0)=\cdots=f^{(p-2)}(0)=0$, $f^{(p-1)}(0)=A_{p-1}=(-1)^{np}(n!)^p$ и није дељив са p (јер је p прост и већи од n), а сви даљи изводи $f^{(p)}(0)$, $f^{(p+1)}(0)$, $\ldots$ су дељиви са p (нпр. $f^{(p)}(0)=pA_p$). Због тога $F(0)$ није дељиво са p, а како је $p>|a_0|$, то ни $a_0F(0)$ није дељиво са p.

Аналогним поступком се, међутим, доказује да $p\mid F(k)$ за све $k=1,2,\ldots,n$, па $|R|=|a_0F(0)+a_1F(1)+\cdots+a_nF(n)|$ није дељиво са p. Но, како је R цео број, он није једнак нули, па је $|R|\geqslant 1$.

С друге стране, у сваком од интеграла на левој страни релације (2) променљива интеграције задовољава услов $t\in[0,n]$, па је у њима

$$|f(t)|=\frac{t^{p-1}}{(p-1)!}|(t-1)^p\cdots(t-n)^p|\leqslant\frac{n^{p-1}\cdot n^{np}}{(p-1)!}.$$

Зато је $\left|\int_0^k e^{k-t}f(t)\,dt\right|<e^n\,\dfrac{n^{(n+1)p}}{(p-1)!}$, па је

$$|R|\leqslant M(n+1)e^n\,\frac{n^{(n+1)p}}{(p-1)!}.$$

Међутим, важи $\lim\limits_{q\to\infty}M(n+1)e^n\,\dfrac{n^{(n+1)q}}{(q-1)!}=0$, па се прост број p може изабрати тако да (поред досадашњих захтева) задовољава и услов $|R|<\dfrac{1}{2}$. Но, то је контрадикција са претходном проценом. ■

Без доказа (за доказ видети нпр. [5]) наведимо и Линдеманову теорему:

Теорема 8. *Ако је* $C_1e^{\alpha_1} + C_2e^{\alpha_2} + \cdots + C_ne^{\alpha_n} = 0$, *при чему су* C_i *алгебарски бројеви, од којих је бар један различит од нуле, а* α_i *су међусобно различити бројеви, такви да су* $\alpha_2, \ldots, \alpha_n$ *алгебарски, тада је* α_1 *трансцендентан број.*

Последица 7. Број π је трансцендентан.

Доказ. Следи из Линдеманове теореме и Ојлерове[11] релације $e^{2i\pi} = 1$. ■

Доказ трансцендентности броја π имао је за последицу коначно решавање вековног проблема квадратуре круга — није могуће, служећи се лењиром и шестаром, конструисати квадрат чија је површина једнака површини датог круга.

Пример 7. Ако је α алгебарски број већи од нуле и различит од 1, тада је $\ln\alpha$ трансцендентан број. △

Задатак 4. (Савезно такмичење 1979.) Да ли постоје бројеви $a, b > 0$ такви да је: (а) $a, b \notin \mathbf{Q}$ и $a^b \in \mathbf{Q}$; (б) $a, b, a^b \notin \mathbf{Q}$; (в) $a \in \mathbf{Q}$ и $b, a^b \notin \mathbf{Q}$?

За конкретне бројеве проблем одређивања да ли су они алгебарски или трансцендентни често је веома тежак. За многе бројеве, на пример $2^{\sqrt{2}}$, $\log_2 3$, e^π, до одговора се не може доћи на неки од досад описаних начина. Гељфонд[12] је 1934. године доказао да су сви бројеви облика α^β трансцендентни, под претпоставком да је α алгебарски број, различит од 0 и 1, а β алгебарски ирационалан. На пример, такви су сви бројеви облика $a^{\sqrt[n]{b}}$, где је a цео број, већи од 1, b цео, различит од n-тог степена целог броја; затим сви логаритми рационалних бројева са рационалним основама који нису сами рационални итд. За неке бројеве који се често срећу ни до данас се не зна да ли су алгебарски или трансцендентни. На пример, Ојлерова константа C, позната из математичке анализе, јесте број за који се чак не зна ни да ли је рационалан или ирационалан.

ЛИТЕРАТУРА

[1] А. А. Бухштаб, *Теория чисел*, «Просвещение», Москва 1966.

[2] Г. М. Фихтенгольц, *Курс дифференциального и интегрального исчисления, II*, «Наука», Москва 1969.

[3] В. Мићић, З. Каделбург, *Увод у теорију бројева*, треће издање, Друштво математичара Србије, Београд 2001.

[4] I. Niven, H. S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York 1980.

[5] А. Б. Шидловский, *Диофантовы приближения и трансцендентные числа*, Изд. Московкого университета, Москва 1982.

[11] L. Euler (1707–1783), швајцарски математичар

[12] А. О. Гельфонд (1906–1968), совјетски математичар