Pokroky matematiky, fyziky a astronomie

Břetislav Novák

O sedmém Hilbertově problému

Pokroky matematiky, fyziky a astronomie, Vol. 17 (1972), No. 5, 245--256

Persistent URL: `http://dml.cz/dmlcz/138124`

O SEDMÉM HILBERTOVĚ PROBLÉMU

BŘETISLAV NOVÁK, Praha

Z celkového počtu dvaceti tří problémů, které D. Hilbert v r. 1900 formuloval, spadají sedmý až dvanáctý problém do teorie čísel. Bez nadsázky lze nyní říci, že řešení těchto problémů ovlivnilo podstatným způsobem rozvoj teorie čísel. Sám Hilbert – jak je ostatně všeobecně známo – se teorii čísel aktivně věnoval a mnohými svými pracemi položil základy některých odvětví teorie čísel a mohl tedy zasvěceně vyzdvihnout klíčové problémy.

Sedmý Hilbertův problém se týká iracionality a transcendence některých čísel. V knize [8] o něm píše zasvěceně A. O. GELFOND (1906–1968), který také tento problém v r. 1934 rozřešil. Naznačme nejprve v hrubých rysech stav celé problematiky do konce devatenáctého století.

Jak známo, nazýváme reálné číslo x racionálním, můžeme-li je vyjádřit ve tvaru $x = p/q$, kde p je celé číslo, q přirozené. Jinak řečeno: racionální čísla jsou všechna řešení rovnic $a_0x + a_1 = 0$, kde a_0, a_1 jsou celá, $a_0 \neq 0$. Ostatní reálná čísla nazveme iracionální. Přirozeným zobecněním dostaneme pojem *algebraického čísla:* jsou to všechna čísla (obecně i komplexní), která jsou kořeny nějakého polynomu

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \tag{1}$$

s celočíselnými koeficienty, stupně alespoň prvého. Je tedy každé racionální číslo číslem algebraickým; snadno ověříme, že čísla $\sqrt{2}$, i, $e^{\pi i r}$, kde r je racionální, jsou algebraická – zřejmě také všechna čísla tvaru $a + bi$, kde a a b jsou racionální, jsou také algebraická.

Každé číslo (obecně komplexní), které není algebraické, nazveme *transcendentní.* Snadno nahlédneme, že algebraická čísla tvoří spočetnou množinu (každý polynom (1) s celočíselnými $a_0, \ldots, a_n$, kde $a_0 \neq 0$, má nejvýše n kořenů a těchto polynomů je spočetně mnoho). Tvoří tedy transcendentní čísla nespočetnou množinu (CANTOR 1874). Transcendentních čísel je tedy „podstatně více" než čísel algebraických. Historicky prvé náznaky této problematiky můžeme nalézt již v r. 1748 u EULERA (v naší terminologii řečeno: Euler předpokládal, že logaritmy racionálních čísel při racionálním základu jsou buď racionální, nebo transcendentní). Základy teorie transcendentních čísel klademe však až do r. 1844, kdy LIOUVILLE poprvé dokázal existenci transcendentních čísel. Načrtněme Liouvillovu myšlenku.

Snadno lze ukázat, že ke každému iracionálnímu*) číslu α existuje nekonečně mnoho dvojic p, q celých čísel, $q > 0$, tak, že je

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

(viz [6], str. 73 – je to důsledek známé Dirichletovy věty). Na základě tohoto tvrzení můžeme každému iracionálnímu číslu α přiřadit číslo $\Theta = \Theta(\alpha)$ definované takto: Θ je supremum všech čísel $\beta > 0$, pro něž nerovnost

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\beta} \tag{3}$$

má nekonečně řešení v celých p, q, $q > 0$. Tedy pro každé iracionální α je $\Theta = \Theta(\alpha) \geqq 2$. Zásadní důležitost má

Liouvillova věta. Buď α iracionální kořen polynomu (1) stupně alespoň druhého s celočíselnými koeficienty. Potom $\Theta = \Theta(\alpha) \leqq n$.

Důkaz. Buďte p, q celá, $q > 0$. Zvolme $\varepsilon > 0$ takové, že v intervalu $(\alpha - \varepsilon, \alpha + \varepsilon)$ neleží žádný kořen polynomu (1) různý od α. Je-li $|\alpha - p/q| < \varepsilon$, je podle věty o přírůstku funkce pro vhodné $\xi \in (\alpha - \varepsilon, \alpha + \varepsilon)$

$$0 \neq P\left(\frac{p}{q}\right) = P\left(\frac{p}{q}\right) - P(\alpha) = \left(\frac{p}{q} - \alpha\right) P'(\xi)\,.$$

Levá strana je zřejmě racionální nenulové číslo, které lze napsat ve tvaru l/q^n, kde l je celé nenulové. Je-li tedy $M = \sup\limits_{x-\alpha \leqq \varepsilon} |P'(x)|$, máme

$$\frac{1}{q^n} \leqq \frac{|l|}{q^n} \leqq \left|\frac{p}{q} - \alpha\right| M\,.$$

Pro všechna celá p, q, $q > 0$ vyjde tedy

$$\left|\alpha - \frac{p}{q}\right| \geqq \frac{C}{q^n}\,,$$

kde $C = \min\,(\varepsilon, 1/M)$ je kladná konstanta, závislá jen na α a P. Odtud plyne, že $\Theta(\alpha) \leqq n$.

---

*) Kdyby bylo $\alpha = p_0/q_0$, p_0, q_0 celá, $q_0 > 0$, tj. α racionální, plynulo by z (2) buď $p/q = \alpha$, nebo $1/qq_0 < 1/q^2$ tj. $q < q_0$. Pro racionální α má tedy (2) kromě triviálního případu jen konečně mnoho řešení v celých p, q.

Můžeme tedy říci, že $\Theta(\alpha)$ je pro reálné algebraické α vždy konečné číslo (tj. reálná algebraická čísla lze jen „velmi špatně“ aproximovat racionálními čísly). Abychom nalezli transcendentní číslo, stačí zkonstruovat iracionální číslo α tak, že $\Theta(\alpha) = +\infty$.

Důsledek Liouvillovy věty. Číslo

$$\alpha = \sum_{m=0}^{\infty} \frac{(-1)^m}{2^{m!}} \tag{4}$$

je transcendentní.

Důkaz. Buď $q_m = 2^{m!}$, $m = 0, 1, \ldots$. Potom je

$$\alpha - \sum_{m=0}^{k-1} \frac{(-1)^m}{2^{m!}} = \sum_{m=k}^{\infty} \frac{(-1)^m}{2^{m!}},$$

a tedy pro vhodné celé $p_{k-1}\left(= q_{k-1} \sum_{m=0}^{k-1} (-1)^m/2^{m!}\right)$ máme

$$0 < \left|\alpha - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2^{k!}} = \frac{1}{q_{k-1}^k} \qquad k = 1, 2, \ldots \tag{5}$$

Kdyby bylo $\alpha = a/b$ (a, b celá, $b > 0$) racionální, měli bychom podle (5)

$$\frac{1}{bq_{k-1}} \leqq \left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{q_{k-1}^k},$$

tj. $q_{k-1}^{k-1} \leqq b$ pro $k = 1, 2, \ldots$ což není možné. Z (5) dále plyne, že nerovnost (3) má nekonečně mnoho řešení pro každé $\beta > 0$ (stačí položit $p = p_{k-1}$, $q = q_{k-1}$ pro $k > \beta$), tj. $\Theta = \Theta(\alpha) = +\infty$, a α tedy nemůže být algebraické číslo.

Liouvillovu konstrukci můžeme ovšem zobecnit (např. $\alpha = \sum_{m=0}^{\infty} q^{-n_m}$, kde $q > 1$ a n_m jsou přirozená, $\lim_{m\to\infty} n_{m+1}/n_m = +\infty$) nebo využít podobně řetězových zlomků nebo nekonečných součinů a sestrojit tak i nespočetnou množinu transcendentních čísel. To je ovšem velmi daleko od řešení otázky, rozhodnout o daném čísle, je-li transcendentní nebo algebraické (nebo dokonce, je-li racionální nebo iracionální).

Abychom mohli odhadnout dosah Liouvillovy metody (kterou lze shrnout v tvrzení: je-li pro iracionální α $\Theta(\alpha) = +\infty$, je α transcendentní), podívejme se, „jak mnoho“ je těch iracionálních α, pro něž je $\Theta(\alpha) = +\infty$ (tato čísla nazýváme Liouvillova čísla). Odpověď nám dává

Chinčinova věta (viz [2]). Buď $\beta > 2$ a buď $\mathfrak{M}_\beta$ množina těch iracionálních α, pro něž nerovnost (3) má nekonečně mnoho řešení v celých p, q, $q > 0$. Potom $\mathfrak{M}_\beta$ je množina nulové Lebesguovy míry.

Důkaz. Buď μ Lebesguova míra v E_1. Zřejmě stačí uvažovat množinu $\mathfrak{M} = \mathfrak{M}_\beta \cap \langle 0,1\rangle$. Pro q přirozené buď M_q sjednocení všech intervalů

$$\left(\frac{p}{q} - \frac{1}{q^\beta}, \frac{p}{q} + \frac{1}{q^\beta}\right).$$

kde $0 \leqq p \leqq q$, p celé. Každé číslo $\alpha \in \mathfrak{M}$ musí ležet v nekonečně mnoha množinách M_q, tj. máme

$$\mathfrak{M} \subset \bigcap_{k=1}^{\infty} \bigcup_{q=k}^{\infty} M_q . \tag{6}$$

Míra množiny M_q je zřejmě nejvýše $2(q + 1)/q^\beta$, a tedy máme

$$\mu(\bigcup_{q=k}^{\infty} M_q) \leqq \sum_{q=k}^{\infty} \frac{2(q + 1)}{q^\beta} \leqq 4 \sum_{q=k}^{\infty} \frac{1}{q^{\beta - 1}}$$

pro každé přirozené k. Podle (6) dostaneme pro každé přirozené k

$$\mu(\mathfrak{M}) \leqq 4 \sum_{q=k}^{\infty} \frac{1}{q^{\beta-1}},$$

a tedy ($\beta - 1 > 1$!) $\mu(\mathfrak{M}) = 0$.

Z Chinčinovy věty okamžitě dostaneme, že i množina těch iracionálních α, pro něž je $\Theta(\alpha) > 2$, má Lebesguovu míru nula (stačí ji vyjádřit ve tvaru $\bigcup_{n=1}^{\infty} \mathfrak{M}_{2+1/n}$ a použít Chinčinovy věty), tj. speciálně pro skoro všechna reálná α je $\Theta(\alpha) = 2$ a Liouvillova čísla tvoří množinu Lebesguovy míry nula. Liouvillova metoda důkazu transcendence zahrnuje tedy „velmi málo" čísel.

Největší zájem byl od počátku samozřejmě soustředěn na zkoumání vlastností známých konstant, jako je e, π atp. Již v r. 1766 dokázal Lambert, že číslo π je iracionální, v r. 1815 pak Fourier ukázal iracionalitu čísla e (jeho důkaz viz např. v [5], str. 339). Protože snahy ukázat, že e nebo π jsou algebraická čísla byly neúspěšné, vznikla domněnka (poprvé přesně formulovaná Legendrem v r. 1855), že jsou to čísla transcendentní. Důkaz transcendence čísla e dal poprvé v r. 1873 Hermite, a to úplně novou metodou, jejíž důmyslné zobecnění dovolilo v r. 1882 Lindemannovi dokázat transcendenci čísla π*).

Novost metody spočívala zejména v tom, že se studovala funkce e^x. Z jejích některých vlastností pak bylo možno odvodit transcendenci její hodnoty v bodě $x = 1$, tj. čísla e. Naznačme stručně hlavní myšlenky Hermitova důkazu:

---

*) Odtud vyplývá nemožnost rektifikace kružnice a kvadratury kruhu (viz např. [7], str. 472).

Je-li $f(x)$ polynom m-tého stupně, dostaneme integrací per partes snadno

$$\int_0^x e^{-t} f(t)\, dt = f(0) - f(x)\, e^{-x} + \int_0^x e^{-t} f'(t)\, dt\,.$$

Použijeme-li tuto formuli postupně na polynomy $f(x), f'(x), \ldots, f^{(m-1)}(x)$ a vzniklé vztahy sečteme, obdržíme (po vynásobení e^x) rovnost

$$e^x F(0) - F(x) = e^x \int_0^x e^{-t} f(t)\, dt\,, \tag{7}$$

kde $F(x) = \sum_{k=0}^{m} f^{(k)}(x)$. Poznamenejme, že jsme vlastně využili pouze toho, že funkce e^x je řešením diferenciální rovnice $y' = y$, které v bodě $x = 0$ nabývá hodnoty 1. Vztah (7) můžeme interpretovat také tak, že hodnotu e^x můžeme nahradit zlomkem $F(x)/F(0)$ (je-li $F(0) \neq 0$) s chybou určenou podle (7).

Předpokládejme nyní, že číslo e je algebraické, tj. že je např. kořenem polynomu $a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ s celočíselnými koeficienty, kde $a_0 \neq 0$. Můžeme též bez újmy na obecnosti předpokládat, že $a_n \neq 0$. Dosadíme-li do (7) postupně čísla n, $n - 1, \ldots, 0$ a utvoříme-li lineární kombinaci získaných vztahů po řadě s koeficienty $a_0, a_1, \ldots, a_n$, obdržíme (pomocí rovnosti $\sum_{k=0}^{n} a_k e^{n-k} = 0$) vztah

$$\sum_{k=0}^{n} a_k F(n-k) = -\sum_{k=0}^{n} a_k e^{n-k} \int_0^{n-k} e^{-t} f(t)\, dt\,. \tag{8}$$

Abychom z tohoto vztahu odvodili spor, budeme se snažit volit polynom f tak, aby levá strana v (8) byla „velká“, pravá malá. K tomu opět stačí volit f tak, aby levá strana byla celé nenulové číslo a pravá strana pak číslo v absolutní hodnotě menší než jedna. Budeme tedy hledat f tak, aby $F(0), F(1), \ldots, F(n)$ byla celá čísla a $\max_{0 \leqq x \leqq n} |f(x)|$ bylo velmi malé. Volme

$$f(x) = \frac{1}{(p-1)!}\, x^{p-1}(x-1)^p (x-2)^p \ldots (x-n)^p\,, \tag{9}$$

kde p je liché prvočíslo, $p > |a_n|, n$. Snadno zjistíme, že všechny derivace f v bodech $0, 1, \ldots, n$ jsou celá čísla; dokonce $f^{(k)}(0) = 0$ pro $k < p - 1$, $f^{(p-1)}(0) = (-1)^n (n!)^p$ $f^{(k)}(j) = 0$ pro $k < p$, $j = 1, 2, \ldots, n$ a čísla $f^{(k)}(j)$ jsou pro $k \geqq p$ dělitelná p pro $j = 0, 1, \ldots, n$. Odtud plyne, že pro tento polynom f je levá strana v (8) celé číslo *nedělitelné* p, tj. celé nenulové číslo. Díky faktoriálu ve jmenovateli v (9) ihned zjistíme, že pro dostatečně velká p je absolutní hodnota levé strany v (8) menší než jedna a tím dostaneme spor.

Analogickým postupem (i když o mnoho složitějším) lze dokázat následující obecnou větu.

L i n d e m a n n o v a v ě t a. Je-li z nenulové algebraické číslo, je e^z číslo transcendentní.

Transcendentnost čísla e $(= e^1)$ dostaneme okamžitě. Odtud plyne dále ihned transcendentnost čísla π takto: kdyby π bylo algebraické číslo, tj. kořen polynomu $P(x)$ tvaru (1) s celočíselnými koeficienty, bylo by i číslo πi algebraické, neboť je kořenem polynomu $P(ix)\ P(-ix)$ s celými koeficienty. Číslo $e^{\pi i} = -1$ by tedy muselo být transcendentní, což je spor.

V roce 1885 WEIERSTRASS zjednodušil a současně zobecnil Lindemannův postup a ukázal platnost Lindemannovy domněnky touto větou:

L i n d e m a n n o v a - W e i e r s t r a s s o v a v ě t a. Buďte $\beta_1, \beta_2, \ldots, \beta_n$ navzájem různá algebraická čísla, $b_1, b_2, \ldots, b_n$ algebraická čísla, která nejsou všechna rovna nule. Potom

$$b_1 e^{\beta_1} + b_2 e^{\beta_2} + \ldots + b_n e^{\beta_n} \neq 0 \,.^{*)}$$

To jsou zhruba hlavní výsledky výzkumů o tomto problému celého devatenáctého století. Stručně lze shrnout, že byla využita jednak myšlenka aproximace pomocí čísel racionálních, jednak myšlenka využití funkcí, které pro algebraické hodnoty argumentu nabývají zkoumaných hodnot, přičemž bylo podstatně využito toho, že tyto funkce splňují jednoduché lineární diferenciální rovnice. Asi za tohoto stavu našich znalostí formuloval Hilbert svůj sedmý problém (viz [8]):

Je číslo α^β při algebraickém $\alpha \neq 0,1$ a algebraickém iracionálním β –, tj. např. čísla $2^{\sqrt{2}}$ nebo $e^\pi = i^{-2i}$ – vždy transcendentní nebo alespoň iracionální?**)

Výše jsme upozornili, že Hermitova-Lindemannova metoda je v základě umožněna tím, že vyšetřovaná funkce (ať již e^z nebo $e^{\alpha z}$ pro algebraické α) je řešením jednoduché lineární diferenciální rovnice ($y' = y$ nebo $y' = \alpha y$) s algebraickými koeficienty. Další zobecňování této metody (Legendre, HURWITZ, MAIER) vedla světoznámého matematika K. L. SIEGELA v r. 1929 k vypracování velmi obecné metody. Dalekosáhlé její zdokonalení přísluší sovětskému matematikovi A. B. ŠIDLOVSKÉMU. Pro ilustraci uveďme jeden z jeho nejlepších výsledků z r. 1954 (pro jednoduchost ve speciálním tvaru).

Š i d l o v s k é h o v ě t a. Nechť Siegelova E-funkce $f(z)$ je transcendentní a je řešením lineární diferenciální rovnice

$$P_1 y' + P_0 y = Q\,,$$

*) Volíme-li $n = 2$, $b_1 = 1$, $\beta_1 = z$, $\beta_2 = 0$, dostaneme ihned Lindemannovu větu.

**) Hilbert speciálně ještě klade otázku, zda v rovnoramenném trojúhelníku je podíl základny a ramene číslo transcendentní, je-li podíl úhlu při základně a úhlu při vrcholu číslo algebraické. Tato úloha vede k důkazu transcendence čísla $i^{-2i\alpha}$ pro reálné algebraické α. Poznamenejme ještě, že výrazem α^β pro komplexní α, β rozumíme libovolnou hodnotu této obecné mocniny.

kde P_0, P_1, Q jsou polynomy s algebraickými koeficienty a nechť α je algebraické číslo, které není kořenem polynomu $zP_1(z)$. Potom $f(\alpha)$ je transcendentní.

Pro objasnění uveďme, že funkci f nazveme transcendentní, jestliže nesplňuje žádnou rovnici tvaru

$$A_0(z)f^n(z) + \ldots + A_n(z) = 0\,,$$

kde $A_0, \ldots, A_n$ jsou polynomy (ne všechny nulové). Siegelovou E-funkcí je např. každá funkce tvaru

$$f(z) = \sum_{n=0}^{\infty} C_n \frac{z^n}{n!}\,,$$

kde C_n jsou celá a platí, že pro každé $\varepsilon < 0$ je posloupnost $C_n n^{-\varepsilon n}$ omezená.

Odtud je patrné, že další zobecňování Lindemannovy metody nemohlo příliš přispět k řešení Hilbertova problému, neboť tam jde o hodnoty funkce $\alpha^z = e^{z \log \alpha}$, přičemž číslo $\log \alpha$ bude ve zkoumaném případě transcendentní. Tato funkce splňuje diferenciální rovnice s transcendentními koeficienty a koeficienty jejího rozvoje v řadu jsou opět transcendentní. K řešení Hilbertova problému bylo třeba vypracovat novou účinnou metodu.

V roce 1929 vypracoval A. O. Gelfond metodu, s jejíž pomocí se mu podařilo dokázat jistý speciální výsledek: Je-li $\alpha \neq 0,1$ algebraické číslo, q přirozené a $\sqrt{q}$ iracionální, je číslo $\alpha^{i\sqrt{q}}$ transcendentní. V r. 1930 R. O. Kuzmin ukázal za stejných předpokladů transcencenci čísla $\alpha^{\sqrt{q}}$. Úplné řešení sedmého Hilbertova problému se A. O. Geľfondovi podařilo v r. 1934 vypracováním další metody touto větou:*)

Geľfondova věta. Buďte α, β algebraická čísla a $\alpha, \beta \neq 0,1$. Potom číslo $\log \alpha / \log \beta$ je buď racionální, nebo transcendentní.

Odtud speciálně plyne (položíme-li $\beta = 10$), že dekadické logaritmy algebraických čísel jsou buď čísla racionální, nebo transcendentní. Důsledkem je i řešení Hilbertova problému: jsou-li a a b algebraická čísla, $a \neq 0,1$ a b iracionální, platí pro číslo $a^b = c$ vztah $b \log a = \log c$. Kdyby bylo c algebraické (a nutně je $c \neq 0,1$), bylo by číslo $b = \log c / \log a$ podle Geľfondovy věty buď racionální, nebo transcendentní, což dává spor s předpokladem.

Není možné v tomto článku popsat podrobně některou z obou Geľfondových metod. Pokusíme se alespoň naznačit hlavní myšlenky; omezíme se přitom na účinnější druhou metodu. Velmi zhruba lze říci, že Geľfondova metoda je skloubení metody Liouvillovy i Hermitovy: využívá vlastností algebraických čísel vzhledem k aproximaci čísly racionálními i vlastností funkcí, jejichž hodnotami v algebraických bodech zkoumaná čísla jsou.

---

*) O několik měsíců později podal poněkud jiný důkaz této věty Siegelův žák, německý matematik T. Schneider.

Liouvillovu větu můžeme formulovat také takto: Je-li $P(x) = a_0 x + a_1$ polynom stupně nejvýše prvého, $|a_j| \leqq A$, $j = 0,1$, a_0, a_1 celá a je-li α algebraické číslo, je buď $P(\alpha) = 0$, nebo pro jistou konstantu Θ, závislou jen na α, je $|P(\alpha)| \geqq A^{-\Theta}$. Máme-li polynom $P(x_1, \ldots, x_n)$ s celočíselnými koeficienty stupně nejvýše N a jsou-li $\alpha_1, \ldots, \alpha_n$ racionální čísla, je zřejmě buď $P(\alpha_1, \ldots, \alpha_n) = 0$, nebo $|P(\alpha_1, \ldots, \alpha_n)| \geqq q^{-N}$, kde q je přirozené číslo, závislé jen na $\alpha_1, \ldots, \alpha_n$. Obecně lze ukázat tuto obecnou vlastnost algebraických čísel:

Buď $P(x_1, \ldots, x_n)$ polynom stupně nejvýše N s celočíselnými koeficienty, které jsou v absolutní hodnotě nejvýše H, $\alpha_1, \ldots, \alpha_n$ algebraická čísla. Potom je buď $P(\alpha_1, \ldots, \alpha_n) = 0$, nebo

$$|P(\alpha_1, \ldots, \alpha_n)| > H^{-\Theta_1} e^{-\Theta_2 N},$$

kde Θ_1 a Θ_2 jsou kladná čísla, která závisí jen na $\alpha_1, \ldots, \alpha_n$.

Druhá vlastnost algebraických čísel, která je využívána, je bezprostředním důsledkem definice. Je-li α algebraické číslo, existuje polynom tvaru (1) s celočíselnými koeficienty, $a_0 \neq 0$ tak, že $P(\alpha) = 0$. Lze tedy číslo α^n vyjádřit lineární kombinací čísel $\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1$ s racionálními koeficienty a to platí i pro každou vyšší mocninu čísla α, jak ihned zjistíme. Je přitom důležité, že koeficienty této lineární kombinace nejsou příliš velká čísla. Přesně: Je-li $N \geqq n$, lze psát

$$\alpha^N = d^{-N} \sum_{k=0}^{n-1} a_{k,N} (d\alpha)^k,$$

kde d je přirozené a kde $a_{k,N}$ jsou celá $|a_{k,N}| \leqq e^{\Theta N}$, $k = 0,1 \ldots, n-1$, kde Θ závisí jen na α.

Třetí myšlenka, používaná Gel'fondem, je velmi jednoduchá. Uvažujme vztahy

$$\sum_{k=1}^{q} b_{jk} x_k = 0, \quad j = 1, \ldots, p$$

s celočíselnými b_{jk}, $|b_{j,k}| \leqq B$, $j = 1, \ldots p$, $k = 1, \ldots, q$. Tato soustava lineárních rovnic má jistě netriviální řešení, je-li $q > p$. Lze poměrně snadno ukázat, že pro dosti velké q ($q \geqq 2p$) existuje dokonce její celočíselné řešení (netriviální) $x_1, \ldots, x_q$ a ne příliš velké ($|x_k| \leqq 3Bq$).

Načrtneme nyní Gel'fondův důkaz jeho věty.

Uvažujme funkci

$$f(x) = \sum_{k=0}^{p} \sum_{k=0}^{p} C_{k,n} a^{kx} b^{nx}, \quad *) \tag{10}$$

*) Původní Gel'fondův důkaz používá teorii funkcí komplexní proměnné, tj. (10) je funkce komplexní proměnné x. V r. 1962 (viz [4]) publikoval Gel'fond „reálnou", i když ne tak účinnou variantu. Pro jednoduchost se omezíme na tuto zjednodušenou verzi, tj. a, b v Gel'fondově větě budou reálná čísla.

kde $C_{k,n}$ jsou celá čísla a p dostatečně velké. Položíme-li $\omega = \ln b/\ln a$, vidíme, že

$$f^{(\nu)}(x) \ln^{-\nu} a = \sum_{k=0}^{p} \sum_{k=0}^{p} C_{k,n} a^{kx} b^{nx} (k + n\omega)^{\nu},$$

tj. pro celočíselná x dostaneme polynom s celočíselnými koeficienty v a, b a ω. Pomocí výše uvedené vlastnosti algebraických čísel lze tento výraz upravit tak, že obsahuje (nezávisle na volbě x, ν a p) pevné mocniny s, b i ω, tj. přesněji existuje přirozené číslo d tak, že pro x celé je

$$d^{p^2} f^{(\nu)}(x) \ln^{-\nu} a = \sum_{\nu_1=0}^{r_1-1} \sum_{\nu_2=0}^{r_2-1} \sum_{\nu_3=0}^{r_3-1} D^{(k,n)}_{\nu_1,\nu_2,\nu_3}(x) (da)^{\nu_1} (db)^{\nu_2} (d\omega)^{\nu_3}, \tag{11}$$

kde $D^{(k,n)}_{\nu_1,\nu_2,\nu_3}(x)$ jsou celočíselné lineární kombinace čísel $C_{k,n}$. Nyní využijeme uvedené třetí myšlenky: Omezíme-li se na vhodný počet ν, x ($0 \leqq \nu \leqq p^2/\ln p$, $0 \leqq x \leqq \ln^2 p$, x celé) lze zvolit $C_{k,n}$ ne všechna rovna nule, $|C_{k,n}| \leqq e^{\Theta p^2}$, Θ nezávisí na p, tak, že koeficienty D v (11) jsou nulové, tj.

$$f^{(\nu)}(x) = 0 \quad \text{pro} \quad 0 \leqq \nu \leqq \frac{p^2}{\ln p}, \quad 0 \leqq x \leqq \frac{\ln p}{2r_1 r_2 r_3}, \quad x \text{ celé}. \tag{12}$$

Nyní nastupuje základní hybná myšlenka důkazu. Vztah (12) ukazuje, že funkce f má hodně nulových bodů (každý počítán se svou násobností). Odtud lze odvodit (a to je vlastně jediná skutečně analytická část důkazu), že $f^{(\nu)}(x)$ musí být „velmi malé" pro více hodnot x, přesně

$$|f^{(\nu)}(x)| < e^{-(1/5r_1r_2r_3)p^2 \log p} \tag{13}$$

pro $0 \leqq \nu \leqq p^2/\ln p$, $0 \leqq x \leqq \ln^2 p$, x celé. Protože $f^{(\nu)}(x)$ pro toto ν a x jsou polynomy s celočíselnými koeficienty v a, b, ω, jsou to podle výše uvedeného buď nuly, nebo čísla ne příliš malá (přesněji $|f^{(\nu)}(x)| > e^{-\Theta p^2}$, kde Θ na p nezávisí), což spolu s (13) dává, že

$$f^{(\nu)}(x) = 0, \quad 0 \leqq \nu \leqq \frac{p^2}{\ln p}, \quad 0 \leqq x \leqq \ln^2 p, \quad x \text{ celé},$$

tj. funkce f má alespoň $p^2 \ln p > (p + 1)^2$ (pro velmi velké p) kořenů. Nyní buď můžeme s trochou námahy celý postup opakovat a nakonec ukázat, že $f^{(\nu)}(0) = 0$ pro $\nu = 0,1 \ldots (p + 1)^2$. Odtud plyne ihned spor, neboť to znamená, že

$$f^{(\nu)}(0) \ln^{-\nu} a = \sum_{k=0}^{p} \sum_{n=0}^{p} C_{k,n}(k + \omega n)^{\nu} = 0, \quad \nu = 1, 2, \ldots, (p + 1)^2 - 1$$

což je soustava $(p + 1)^2$ rovnic o $(p + 1)^2$ neznámých, jejíž determinant je Vandermondův determinant čísel $k + \omega n$, k, $n = 0, \ldots, p$, který je nenulový, neboť ω je podle předpokladu iracionální, a tedy jsou to čísla navzájem různá.*) Druhá možnost je ukázat přímo použitím Rollovy věty, že funkce $f(x)$ má nejvýše $(p + 1)^2$ kořenů.**)

Naznačili jsme doposud v hrubých rysech tři základní směry, kterými se vyvíjela teorie transcendentních čísel. Jsou to v podstatě tři metody vzniklé zobecněním a dalším zdokonalováním důkazů věty Liouvillovy, Lindenmannovy a Geľfondovy. Obraťme se závěrem k některým zajímavým výsledkům a neřešeným problémům v jednotlivých těchto směrech, i když se ovšem metody dají kombinovat. Budeme se přitom zmiňovat o důsledcích, které odtud většinou vyplynou pro teorii diofantických rovnic, kterých se týká desátý Hilbertův problém. Čtenáře, který se chce s touto problematikou podrobněji seznámit, odkazujeme na původní monografie [2], [3] a [9] a na přehledné články [1] a [10], případně na další literaturu v nich doporučenou.

Jak jsme viděli, dává Liouvillova věta poměrně jednoduchý prostředek k důkazu transcendence řady čísel. Je tedy nasnadě otázka, je-li její tvrzení definitivní. V roce 1908 se THUEMU podařilo ukázat, že je-li α iracionální kořen mnohočlenu (1) s celými koeficienty, je $\Theta(\alpha) \leqq (n/2) + 1$. Tento výsledek byl postupně stále zlepšován (Siegel, Geľfond, DYSON atd.), ale až v r. 1955 dokázal ROTH definitivní větu.

Rothova věta. Je-li α iracionální algebraické číslo, je $\Theta(\alpha) = 2$.

Ihned vidíme, že Rothova věta dává vydatný důkazový prostředek i metodu konstrukce dalších transcendentních čísel. Tak např. lze ukázat, že číslo

$$\alpha = 0{,}1234567891011\ldots$$

je transcendentní číslo, které není číslo Liouvillovo (MAHLER).

Zmínili jsme se již, že Siegelovo a Šidlovského zobecnění Lindemannovy metody dává prostředky k důkazu transcendence hodnot řešení jistých lineárních diferenciálních rovnic pro algebraické hodnoty argumentu. Speciálně např. platí:

Siegelova věta. Pro λ racionální, $\lambda \neq \pm\frac{1}{2}, -1, \pm\frac{3}{2}, \ldots$ buď

$$K_\lambda(z) = \sum_{n=0} \frac{(-1)^n}{n!(\lambda + 1)\ldots(\lambda + n)} \left(\frac{z}{2}\right)^{2n}$$

tj. pro Besselovu funkci $J_\lambda(z)$ máme $J_\lambda(z) = K_\lambda(z)\,(z/2)^\lambda/\Gamma(\lambda + 1))$. Potom pro každé nenulové algebraické α jsou čísla $K_\lambda(\alpha)$ i $K'_\lambda(\alpha)$ transcendentní (dokonce pro žádný nenulový polynom $f(x, y)$ s celočíselnými koeficienty neplatí $f(K_\lambda(\alpha), K'_\lambda(\alpha)) = 0$, tj. jsou to čísla tzv. *algebraicky nezávislá*).

*) Tento postup se hodí i pro úvahy s komplexními a, b.

**) Funkce f tvaru $\sum_{j=1}^{N} c_j \mathrm{e}^{\gamma_j x}$, kde c jsou nenulová a γ_j navzájem různá. Kdyby funkce f měla $N + 1$ kořenů, měla by podle Rollovy věty funkce $\mathrm{d}/\mathrm{d}x(\mathrm{e}^{-\gamma_1 x} f(x))$ alespoň N kořenů (každý počítán se svou násobností) atd. a funkce $\mathrm{e}^{(\gamma_N - \gamma_{N-1})x}$ by měla mít alespoň jeden kořen, což je spor.

Šidlovského věta. Buď α nenulové algebraické číslo, p racionální, $p > 0$,

$$\Phi(z) = \int_0^z e^{-t^2}\,dt\,, \qquad F(z) = \int_0^z t^{p-1}\,e^{-t}\,dt\,.$$

Potom čísla $\Phi(\alpha)$ i $F(\alpha)$ jsou transcendentní (dokonce čísla e^{α^2}, $\Phi(\alpha)$, resp. e^{α}, $F(\alpha)$ jsou algebraicky nezávislá.

Podobné výsledky lze dokázat i o hodnotách funkcí

$$\int_0^z \frac{\sin t}{t}\,dt\,, \quad \int_0^z \sin t^2\,dt \quad \text{atp.}$$

Řadu krásných výsledků dostaneme využitím metody A. O. Geľfonda. Tak např. (Schneider 1941) hodnoty

$$B(p, q) = \int_0^1 x^{p-1}(1 - x)^{q-1}\,dx$$

jsou transcendentní pro každou dvojici kladných racionálních čísel p, q intervalu $(0,1)$ nebo (Geľfond 1949): je-li $\alpha \neq 0,1$ algebraické číslo, $\nu \neq 0$ číslo racionální, je alespoň jedno z čísel

$$\alpha^{e^{\nu}},\ \alpha^{e^{2\nu}},\ \alpha^{e^{3\nu}},\ \alpha^{e^{\nu 4}}$$

transcendentní.

Zhruba před šesti lety se podařilo mladému anglickému matematikovi A. BAKEROVI*) podstatně zdokonalit Geľfondovu metodu. Jádro jeho postupu lze formulovat poměrně snadno: tam, kde Geľfond konstruuje jistou funkci jedné proněnné, bere Baker funkci více proměnných. Velmi zhruba řečeno získává tím větší volnost, ale na druhé straně musí vynaložit mnohem větší námahu na její vyšetření. Ostatní postup odpovídá původní Geľfondově metodě (funkce se sestrojí tak, aby měla hodně nulových bodů, ale ne identicky rovna nule a z předpokladu algebraičnosti příslušných čísel ukážeme, že nulových bodů musí být „ještě více" a tím dojdeme ke sporu). Pro podrobnější výklad odkazujeme na článek [1] i literaturu tam uvedenou. Uveďme jen pro ilustraci jeden z Bakerových výsledků:

Bakerova věta. Jsou-li $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n$ nenulová algebraická čísla, je číslo

$$e^{\beta_0}\alpha_1^{\beta_1}, \ldots, \alpha_n^{\beta_n}$$

transcendentní.

Nebudeme se zmiňovat o dalším přínosu Bakerových prací a uvedeme na závěr některé neřešené problémy. Doposud není nic známo o algebraické závislosti čísel e

---

*) Práce A. Bakera byly v r. 1970 na Mezinárodním kongresu matematiků v Nice oceněny Fieldsovou medailí.

a π*). Skoro nic není známo o charakteru Eulerovy konstanty

$$C = \lim_{m \to \infty} \left(\sum_{n=1}^{m} \frac{1}{n} - \ln m \right) = \Gamma'(1)$$

a asi stejné jsou naše znalosti o hodnotách Riemannovy ζ-funkce v lichých číslech, tj. o číslech

$$\zeta(2n + 1) = \sum_{k=1}^{\infty} \frac{1}{k^{2n+1}}, \quad n = 1, 2, \ldots$$

a mohli bychom formulovat celou dlouhou řadu problémů.

Celkově lze říci, že i když v teorii transcendentních čísel se dosáhlo celé řady zásadních výsledků, sedmý Hilbertův problém byl poměrně brzy rozřešen a existující metody byly řadou autorů podstatně zdokonaleny, bude další pokrok zřejmě vázán na vznik nových myšlenek, které by podstatněji rozšířily naše znalosti o transcendentních číslech.

Literatura

[1] A. Baker, Effective methods in Diophantine problems, Proc. Symposia Pure Mathematics (American Math. Soc.), *20* (1971), 195—205.

[2] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge 1957.

[3] A. O. Gelfond, *Algebraičeskije i transcendentnyje čisla*, Moskva 1952.

[4] A. O. Gelfond, Ju. V. Linnik, *Elementarnyje metody v analitičeskoj teorii čisel*, Moskva 1962.

[5] V. Jarník, *Diferenciální počet I*, NČSAV Praha 1955.

[6] V. Jarník, *Diferenciální počet II*, NČSAV Praha 1956.

[7] V. Kořínek, *Základy algebry*, NČSAV Praha 1956.

[8] *Problémy Gil'berta* (sborník), Moskva 1969.

[9] T. Schneider, *Einführung in die transzendenten Zahlen*, Springer 1957.

[10] A. B. Šidlovskij, N. I. Fel'dman, Razvitije i sovreměnnoje sostojanije teoriji transcendentnych čisel, Uspěchi mat. nauk *22* (1967), No 3, 1—81.

*) Snadno (tj. sporem) nahlédneme např., že mezi čísly e $+ r\pi$, r racionální, je nejvýše jedno algebraické. Více však nevíme.