KALEIDOSKOP TEORIE ČÍSEL (2. kapitola)

Martin Klazar

Vím, že čísla jsou krásná. A jestliže krásná nejsou, pak není krásné nic.

(Paul Erdős, *Sunday Times Magazine,* 27. listopadu 1988.)

Analogicky prožíval pan Š. číslice.
„Pro mne 2, 4, 6, 5 nejsou pouhá čísla. Mají tvar ...
1 — to je ostré číslo, nezávisle na jeho grafickém vyjádření,
je to něco ukončeného, tvrdého.
2 — to je plošší, čtverhranné, bělavé, bývá trochu našedlé ...
3 — to je zaostřený úlomek a točí se.
4 — to je opět čtvercové, tupé, podobné 2, ale mohutnější, tlusté ...
5 — plné zakončení v podobě kužele, věže, masívní.
6 — to následuje první za „5“, je bělavé.
8 — to je nevinné, modravě mléčné, podobné vápnu.“

(A. R. Lurija, *Malá knížka o velké paměti.*)

Toto je předběžný text 2. kapitoly (diofantické aproximace) skript k mé přednášce *Úvod do teorie čísel*, kterou jsem konal na MFF UK v Praze v zimních semestrech školních roků 1996/97, 1998/99 a 1999/00. Zatím v preprintové řadě KAM-DIMATIA Series vyšla kapitola 1 (základní pojmy a obraty) a budou v ní postupně vydány zbylé kapitoly: kapitola 3 (diofantické rovnice), kapitola 4 (kongruence), kapitola 5 (prvočísla), kapitola 6 (geometrie čísel), kapitola 7 (číselné rozklady), kapitola 8 (medailony matematiků) a kapitola 9 (návody k řešením úloh). Obtížnost úloh je bodována 0 (nejlehčí) až 5 (nejtěžší).

březen 2000 Martin Klazar

Obsah

Kapitola 2

Reálná čísla versus zlomky

Jedním z prvních velkých úspěchů Leonarda Eulera bylo sečtení řady

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots .$$

Řešení, které popsal v r. 1734 Danielu Bernoullimu v dopise, který se nedochoval, mohlo znít následovně.

> Přesvědčím Vás, že hledaná suma je rovna $\pi^2/6$. Snadno se vidí, že součet převrácených hodnot kořenů mnohočlenu se rovná záporně vzatému podílu koeficientů lineárního a absolutního členu. Pro nekonečný mnohočlen $1 - x/3! + x^2/5! - x^3/7! + \cdots$ dostáváme $-(-1/6)/1 = 1/6$. Kořeny tohoto mnohočlenu jsou zjevně kvadráty kořenů $1 - x^2/3! + x^4/5! - x^6/7! + \cdots = \frac{\sin x}{x}$ a tyto jsou $\pm\pi, \pm 2\pi, \pm 3\pi$ a tak dál. Proto
>
> $$\frac{1}{1^2\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2} + \cdots = \frac{1}{6} .$$
>
> Tudíž suma reciprokých hodnot čtverců přirozených čísel je rovna $\pi^2/6$, quod erat demonstrandum.

Řadu se třetími mocninami se však Eulerovi ani přes velké usilí sečíst nepodařilo a uspokojivě to neumíme dodnes. Díky Rogeru Apérymu ale víme, že součet je iracionální číslo.

Druhá kapitola pojednává o diofantických aproximacích, to jest o přibližování reálných čísel zlomky. Úvodní Dirichletova věta říká, že každé iracionální číslo $\alpha \in \mathbf{R}$ se dá přiblížit nekonečně mnoha zlomky p/q s přesností lepší než

$1/q^2$. Závěrečná věta oddílu 2.1, Hurwitzova, zlepšuje $1/q^2$ na $1/\sqrt{5}q^2$ a ukazuje, že obecně se konstanta $\sqrt{5}$ již nedá zvětšit. Racionální aproximace zaručené Dirichletovou větou se dají nalézt pomocí Fareyových zlomků, jejichž definici a základní vlastnosti uvádíme rovněž v 2.1.

Jinou techniku pro hledání racionálních aproximací představují řetězové zlomky, které zavedeme v oddílu 2.2. Kromě základních vlastností dokážeme i Lagrangeovu větu charakterizující periodické řetězové zlomky. V následujícím oddílu 2.3 odvodíme řetězový rozvoj čísla e. Oddíl 2.4 je věnován zmíněnému překvapujícímu výsledku z konce 70. let 20. století, Apéryho důkazu iracionality čísla $1^{-3} + 2^{-3} + 3^{-3} + \cdots$.

V oddílech 2.5–2.7 se zabýváme algebraickými čísly. V 2.5 dokážeme, že mezi ně nepatří ani e ani π. Liouvilleova čísla zavedená v 2.6 jsou iracionální čísla s velmi dobrými racionálními aproximacemi. Dokážeme jednoduchý klasický výsledek: Liouvilleova čísla jsou nutně transcendentní. Jinak řečeno, iracionální algebraická čísla se nedají příliš dobře aproximovat zlomky. V 2.7 to dále zesílíme v Thueho větě: K algebraickému číslu stupně $n \geq 2$ se jen konečně mnoho zlomků p/q přibližuje blíže než na $q^{-n/2-1-\varepsilon}$.

Důkazy jsou elementární a používají nejvýše reálnou analýzu, s výjimkou důkazu transcendence π, kde se používá jednoduchá komplexní integrace. Pozoruhodná je aplikace prvočíselné věty v oddílu 2.4. Oddíly 2.4 a 2.7 jsou obtížnější. Dirichletova a Thueho věta mají významné důsledky v teorii diofantických rovnic, a proto se s nimi znovu setkáme v příští kapitole.

2.1 Dirichletova věta a Fareyovy zlomky

Věta 19 (Dirichlet, 1842). 1. *Buďte dána čísla $\alpha \in \mathbf{R}$ a $Q \in \mathbf{N}, Q \geq 2$. Pro vhodná $p, q \in \mathbf{Z}$ pak platí $1 \leq q < Q$ a*

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

2. *Nechť $\alpha \in \mathbf{R}$ je iracionální. Nerovnost*

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

má nekonečně mnoho řešení $p/q \in \mathbf{Q}$, kde $(p, q) = 1$.

DŮKAZ. **1.** Použijeme holubníkový princip. Holubníky představuje Q intervalů $[0,1/Q),[1/Q,2/Q),\dots,[(Q-1)/Q,1)$. Holuby představuje $Q+1$ čísel $0,1,\{\alpha\},\{2\alpha\},\dots,\{(Q-1)\alpha\}$. Dva holubi musejí být ve stejném holubníku:

$$|(\alpha q_1 - p_1) - (\alpha q_2 - p_2)| \leq 1/Q$$

pro vhodná $p_i, q_i \in \mathbf{Z}$, kde $0 \leq q_2 < q_1 < Q$. Stačí tedy položit $q = q_1 - q_2, p = p_1 - p_2$, a nerovnost

$$|\alpha q - p| \leq 1/Q$$

vydělit q.

2. Všimněme si, že nezáleží na tom, zda se zlomek p/q požaduje v základním tvaru nebo ne. Mějme již řešení $p_1/q_1, p_2/q_2, \dots, p_r/q_r$. Číslo $Q \in \mathbf{N}$ zvolíme tak veliké, že

$$1/Q < \Delta = \min_{i=1\dots r} |\alpha - p_i/q_i| \ .$$

(Nemáme-li dosud ani jedno řešení, volíme Q libovolně. Vzhledem k iracionalitě α je $\Delta > 0$.) Podle části 1 přiblížíme α zlomkem p/q tak, že $1 \leq q < Q$ a

$$|\alpha - p/q| < 1/qQ < 1/q^2 \ .$$

Protože však též $1/qQ \leq 1/Q < \Delta$, platí $p/q \neq p_i/q_i, i = 1\dots r$, a p/q je nové řešení. Takto vytváříme nekonečně mnoho řešení. $\diamondsuit$

Část 1 věty 19 má další pěkné použití.

Věta 20 (Euler, 1747). *Každé prvočíslo p tvaru $4n+1$ je součet dvou čtverců, $p = a^2 + b^2, a, b \in \mathbf{N}$.*

DŮKAZ. Potřebujeme jednoduchý fakt, který dokážeme ve čtvrté kapitole. Pro takové prvočíslo p totiž existuje číslo $c \in \mathbf{N}$ takové, že

$$c^2 \equiv -1 \mod p \ .$$

Položíme $\alpha = c/p$ a $Q = \lceil \sqrt{p}\, \rceil$. Podle 1 věty 19 máme, pro vhodná celá a, b, že $1 \leq b < \sqrt{p}$ a

$$\left|\frac{c}{p} - \frac{a}{b}\right| < \frac{1}{b\sqrt{p}} \ .$$

Odtud plyne, že $0 \leq |cb - pa| < \sqrt{p}$ a $0 < (cb-pa)^2 + b^2 < 2p$. Ovšem číslo $(cb-pa)^2 + b^2$ je dělitelné p (volba c), a tak $(cb-pa)^2 + b^2 = p$. $\diamondsuit$

Jak pro dané iracionální $\alpha \in \mathbf{R}$ aproximace zaručené v 2 věty 19 nalézt? Zkusme následující nápad. Můžeme předpokládat, že $\alpha \in (0,1)$ (pokud ne, nahradíme α číslem $\{\alpha\}$). Fixujeme $n \in \mathbf{N}$ a vezmeme všechny zlomky z intervalu $[0,1]$, které jsou v základním tvaru a mají jmenovatele $\leq n$. Uspořádáme je podle velikosti, $f_0 = 0 < f_1 < \cdots < f_m = 1$, a α sevřeme mezi dva sousední členy seznamu: $f_i < \alpha < f_{i+1}$. Je překvapující, že tento na první pohled naivní postup vede k cíli — pro každé n je f_i nebo f_{i+1} dobrou aproximací α ve smyslu věty 19. Nahlédneme to v poznámce za větou 21.

Popsaná posloupnost zlomků $\mathcal{F}_n$ se nazývá *Fareyovými zlomky řádu n*. Například $\mathcal{F}_5$ obsahuje zlomky

$$0 = \frac{0}{1} < \frac{1}{5} < \frac{1}{4} < \frac{1}{3} < \frac{2}{5} < \frac{1}{2} < \frac{3}{5} < \frac{2}{3} < \frac{3}{4} < \frac{4}{5} < \frac{1}{1} = 1 \ .$$

Povšimněme si *mediánové vlastnosti* Fareyových zlomků: V trojici po sobě jdoucích členů $\mathcal{F}_n$ se prostřední zlomek rovná podílu součtů čitatelů a jmenovatelů svých sousedů. Například

$$\frac{0+1}{1+4} = \frac{1}{5}, \quad \frac{2+3}{5+5} = \frac{1}{2} \ \text{ a } \ \frac{3+3}{5+4} = \frac{2}{3} \ .$$

I tato vlastnost plyne z následující věty.

Věta 21 (Cauchy, 1816). *Zlomky $a/b < c/d$ buďte sousední položky seznamu $\mathcal{F}_n$. Pak $bc - ad = 1$. Jinak řečeno, rozdíl dvou sousedních Fareyových zlomků řádu n je nejmenší možný (je roven převrácené hodnotě součinu jmenovatelů).*

Důkaz. Protože $a \perp b$, podle tvrzení 4 z 1. kapitoly má rovnice

$$bx - ay = 1 \tag{1}$$

řešení $x, y \in \mathbf{Z}$. Je-li x_0, y_0 řešením, je řešením i $x_0 + ra, y_0 + rb$, kde $r \in \mathbf{Z}$ je libovolné číslo, a proto existuje řešení x_1, y_1 takové, že

$$0 \leq n - b < y_1 \leq n \ . \tag{2}$$

Zřejmě $x_1/y_1 \in \mathcal{F}_n$. Z (1) máme

$$\frac{x_1}{y_1} = \frac{a}{b} + \frac{1}{by_1} > \frac{a}{b} \ . \tag{3}$$

Tudíž $x_1/y_1 \geq c/d$.

Ukážeme, že ostrá nerovnost $x_1/y_1 > c/d$ vede ke sporu. Sečtením nerovností

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

získáme

$$\frac{x_1}{y_1} - \frac{a}{b} \geq \frac{b + y_1}{bdy_1} \ .$$

Ovšem, s pomocí (3) a (2),

$$\frac{1}{by_1} \geq \frac{b + y_1}{bdy_1} > \frac{n}{bdy_1} \ .$$

Tedy $d > n$, což je spor.

Proto platí $x_1 = c, y_1 = d$, a c, d je také řešením (1). To je ovšem, co chceme dokázat. $\diamondsuit$

Teď již umíme dokázat mediánovou vlastnost a vlastnost dobré aproximace. Pro tři po sobě jdoucí zlomky

$$\frac{a}{b} < \frac{c}{d} < \frac{e}{f}$$

z $\mathcal{F}_n$ máme podle předchozí věty $bc - ad = 1$ a $ed - cf = 1$. Odtud plynou vhodnými celočíselnými lineárními kombinacemi rovnosti $c(eb - af) = e + a$ a $d(eb - af) = b + f$. Takže

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

Nyní vlastnost dobré aproximace. Nechť

$$\frac{a}{b} < \alpha < \frac{c}{d} \ ,$$

kde $\alpha \in \mathbf{R}$ je iracionální a $a/b < c/d$ jsou dva sousední zlomky z $\mathcal{F}_n$. Nechť například $b \leq d$. Pak, podle věty 21,

$$\left| \alpha - \frac{a}{b} \right| < \frac{c}{d} - \frac{a}{b} = \frac{1}{bd} \leq \frac{1}{b^2}$$

a a/b je dobrým přiblížením α. Pro $b > d$ je dobrým přiblížením c/d. Snadno se vidí, že pro $n \to \infty$ dostáváme nekonečně mnoho různých dobrých aproximací. Jiným způsobem jsme tak dokázali 2 věty 19.

Tvrzení 22 (o Fareyových zlomcích). *Zlomky $a/b < c/d$ buďte sousední položky seznamu $\mathcal{F}_n$. Nechť $a/b < \alpha < c/d$, kde $\alpha \in \mathbf{R}$ je iracionální. Pak alespoň jeden ze tří zlomků $a/b, c/d, e/f = (a+c)/(b+d)$ splňuje nerovnost*

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

DŮKAZ. Lze předpokládat, že $\alpha > (a+c)/(b+d) = e/f$ (platí-li opačná nerovnost, celý následující postup se zřejmým způsobem upraví). Nechť neplatí ani jedna ze tří nerovností, potom

$$\alpha - \frac{a}{b} \geq \frac{1}{\sqrt{5}b^2} \ , \tag{4}$$

$$\alpha - \frac{e}{f} \geq \frac{1}{\sqrt{5}f^2} \tag{5}$$

a

$$\frac{c}{d} - \alpha \geq \frac{1}{\sqrt{5}d^2} \ . \tag{6}$$

Odvodíme spor.

Sečtením (4) a (6) máme, díky větě 21,

$$\frac{c}{d} - \frac{a}{b} = \frac{1}{bd} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{d^2}\right) .$$

Sečtením (5) a (6) máme, vzhledem k definici e a f a větě 21,

$$\frac{c}{d} - \frac{e}{f} = \frac{1}{df} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{d^2} + \frac{1}{f^2}\right) .$$

Tedy $bd\sqrt{5} \geq b^2 + d^2$ a $df\sqrt{5} \geq d^2 + f^2$. Sečtením získáváme $d\sqrt{5}(b+f) \geq b^2 + 2d^2 + f^2$. Podle definice f to znamená, že $d\sqrt{5}(2b+d) \geq 2b^2 + 3d^2 + 2bd$. Ekvivalentně,

$$\tfrac{1}{2}((\sqrt{5}-1)d - 2b)^2 \leq 0 \ .$$

Musí nastat rovnost, tudíž $\sqrt{5} = 1 + 2b/d \in \mathbf{Q}$. To je spor. $\diamondsuit$

Ukážeme, že konstanta $\sqrt{5}$ ve jmenovateli je největší možná.

Věta 23 (Hurwitz, 1891). *Nechť číslo $\alpha \in \mathbf{R}$ je iracionální. Nerovnost*

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

má nekonečně mnoho řešení $p/q \in \mathbf{Q}$. Tvrzení neplatí, je-li $\sqrt{5}$ nahrazena libovolnou větší konstantou A.

DŮKAZ. První část věty plyne z tvrzení 22. Pro důkaz druhé části položíme $\alpha = \phi - 1 = (\sqrt{5} - 1)/2$. Ukážeme, že toto číslo — vpodstatě zlatý řez! — se špatně aproximuje zlomky. (Nejhůře ze všech iracionálních čísel, zlatý řez je v tomto smyslu „nejiracionálnější" číslo.) Mějme racionální aproximaci α s konstantou $A > \sqrt{5}$:

$$\alpha = \frac{p}{q} + \frac{\delta}{q^2}\ , \tag{7}$$

kde $p/q \in \mathbf{Q}$ a $|\delta| < 1/A < 1/\sqrt{5}$. Tato rovnost a definice α dávají

$$\frac{\delta}{q} - q\frac{\sqrt{5}}{2} = q\alpha - p - q\frac{\sqrt{5}}{2} = \frac{-q}{2} - p\ .$$

Umocněním na druhou a odečtením $5q^2/4$ přejdeme k

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = (q/2 + p)^2 - 5q^2/4 = p^2 - pq + q^2\ .$$

Kdyby bylo možné rovnici (7) splnit nekonečně mnoha zlomky p/q, vede poslední rovnost ke sporu. Její levá strana je totiž pro dostatečně velké q v absolutní hodnotě menší než 1. Pro velké q tedy máme $p^2 - pq + q^2 = 0$, čili $(2p + q)^2 = 5q^2$. To je opět spor s iracionalitou $\sqrt{5}$. $\diamondsuit$

Část 2 věty 19 a věta 23 se dají kompaktně zformulovat pomocí značení $\|\cdots\|$ (vzdálenost k nejbližšímu celému číslu). První věta říká, že pro iracionální α má nerovnost $q\|q\alpha\| < 1$ nekonečně mnoho řešení $q \in \mathbf{N}$. Druhá říká, že ještě i $q\|q\alpha\| < 5^{-1/2}$ má nekonečně mnoho řešení, ale $5^{-1/2}$ se už nedá obecně zmenšit. Viz úlohy 5 a 6.

2.2 Řetězové zlomky

Zkusíme jinou ideu, jak pro dané iracionální číslo $\alpha \in \mathbf{R}$ nalézt jeho dobré aproximace zlomky. Aproximace celým číslem zdola je jasná, je to $a_0 = \lfloor \alpha \rfloor \in$

Z. Rozdíl $\zeta_0 = \alpha - a_0 = \{\alpha\} \in [0,1)$ aproximujeme podobně — pokud $\zeta_0 \neq 0$, vyjádříme $1/\zeta_0$ jako

$$1/\zeta_0 = a_1 + \zeta_1,\ a_1 = \lfloor 1/\zeta_0 \rfloor \in \mathbf{N},\ \zeta_1 = \{1/\zeta_0\} \in [0,1)\ .$$

Pokud $\zeta_1 \neq 0$, vyjádříme opět

$$1/\zeta_1 = a_2 + \zeta_2,\ a_2 = \lfloor 1/\zeta_1 \rfloor \in \mathbf{N},\ \zeta_2 = \{1/\zeta_1\} \in [0,1)\ .$$

Obdobně definujeme další $a_i \in \mathbf{N}$ a $\zeta_i \in [0,1)$. Dostáváme rovnosti

$$\begin{aligned}\alpha &= a_0 + \zeta_0 = a_0 + \cfrac{1}{a_1 + \zeta_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \zeta_2}} = \cdots \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\begin{matrix}\ddots \\ a_{n-1} + \cfrac{1}{a_n + \zeta_n}\end{matrix}}}} = \cdots\ . \end{aligned} \tag{8}$$

Číslo α určuje čísla a_i a ζ_i jednoznačně. Idea je postupně pro $i = 0, 1, \ldots$ nahrazovat ζ_i nulou. Skutečně se tak dostanou dobré aproximace ve smyslu 2 věty 19. Dokážeme to v tvrzení 26.

Posloupnost čísel a_i — připomínáme, že $a_0 \in \mathbf{Z}$ a $a_i \in \mathbf{N}$ pro $i > 0$ — značíme $//a_0, a_1, \ldots, a_n//$, popř. $//a_0, a_1, \ldots//$ (je-li nekonečná), a nazýváme *řetězovým rozvojem (zlomkem)* čísla α. Jeho n-tým *sblíženým zlomkem* rozumíme racionální číslo, které vznikne z výrazu (8) záměnou ζ_n za 0. Číslům a_i se říká *členy rozvoje*. Uvádíme tři příklady řetězových rozvojů.

Příklad 1. Rozvineme zlomek $-119/27$:

$$\begin{aligned}\frac{-119}{27} &= -5 + \frac{16}{27} = -5 + \cfrac{1}{1 + \cfrac{11}{16}} = -5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{5}{11}}} \\ &= -5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{5}}}} = //-5, 1, 1, 2, 5//\ .\end{aligned}$$

Sblížené zlomky čísla $-119/27$ jsou $-5/1, -4/1, -9/2, -22/5$ a $-119/27$.

Příklad 2. Nalezneme řetězový rozvoj čísla $\alpha = \sqrt{7}$. Protože

$$\sqrt{7} = 2 + (\sqrt{7} - 2)$$

a $\sqrt{7} - 2 \in [0,1)$, máme $a_0 = 2, \zeta_0 = \sqrt{7} - 2$. Protože

$$1/\zeta_0 = 1/(\sqrt{7} - 2) = (\sqrt{7} + 2)/3 = 1 + (\sqrt{7} - 1)/3$$

a $(\sqrt{7} - 1)/3 \in [0,1)$, máme $a_1 = 1, \zeta_1 = (\sqrt{7} - 1)/3$. Protože

$$1/\zeta_1 = 3/(\sqrt{7} - 1) = (\sqrt{7} + 1)/2 = 1 + (\sqrt{7} - 1)/2\ ,$$

máme $a_2 = 1, \zeta_2 = (\sqrt{7} - 1)/2$. Protože

$$1/\zeta_2 = 2/(\sqrt{7} - 1) = (\sqrt{7} + 1)/3 = 1 + (\sqrt{7} - 2)/3\ ,$$

máme $a_3 = 1, \zeta_3 = (\sqrt{7} - 2)/3$. Protože

$$1/\zeta_3 = 3/(\sqrt{7} - 2) = \sqrt{7} + 2 = 4 + (\sqrt{7} - 2)\ ,$$

máme $a_4 = 4, \zeta_4 = \sqrt{7} - 2$ a jsme ve stejné situaci, jako když jsme měli počítat a_1. Sekvence $1, 1, 1, 4$ členů rozvoje se stále opakuje. Dostáváme řetězový rozvoj

$$\sqrt{7} = //2, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots //\ .$$

V jakém smyslu se číslo $\sqrt{7}$ rovná svému řetězovému rozvoji objasníme v tvrzení 26. Posloupnost sblížených zlomků čísla $\sqrt{7}$ začíná $2/1, 3/1, 5/2, 8/3, 13/5, 45/17, 82/31, \ldots$

Příklad 3. Do třetice se podíváme na zlatý řez. Protože

$$(1 + \sqrt{5})/2 = 1 + (\sqrt{5} - 1)/2$$

a $(\sqrt{5} - 1)/2 \in [0,1)$, máme $a_0 = 1, \zeta_0 = (\sqrt{5} - 1)/2$. Dále

$$1/\zeta_0 = 2/(\sqrt{5} - 1) = (1 + \sqrt{5})/2$$

a jsme zase na začátku. Vidíme, že zlatý řez má velmi jednoduchý řetězový rozvoj

$$\phi = \frac{1 + \sqrt{5}}{2} = //1, 1, 1, 1, \ldots //\ .$$

Z hlediska řetězových rozvojů je ϕ nejjednodušším iracionálním číslem. Posloupnost jeho sblížených zlomků začíná zlomky $1/1, 2/1, 3/2, 5/3, \ldots$. Snadno se vidí, že n-tý sblížený zlomek je F_{n+1}/F_n, kde $F_n, n \geq 0$, je posloupnost *Fibonacciových čísel* $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ splňující rekurenci $F_{n+1} = F_n + F_{n-1}$.

Zavedeme abstraktnější pojetí řetězových zlomků. Nechť $x_0, x_1, \ldots, x_n, \ldots$ jsou různé proměnné. *Řetězovým zlomkem* rozumíme též racionální funkci

$$//x_0, x_1, \ldots, x_n// = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\begin{array}{c}\vdots\\ x_{n-1} + \cfrac{1}{x_n}\end{array}}}} .$$

Sblíženým zlomkem p_n/q_n rozumíme vyjádření $//x_0, x_1, \ldots, x_n//$ jako podílu dvou polynomů $p_n(x_0, x_1, \ldots, x_n)$ a $q_n(x_0, x_1, \ldots, x_n)$, které vznikne úpravou složeného zlomku na kanonický tvar.

Vztah mezi n-tým sblíženým zlomkem $r \in \mathbf{Q}$ čísla $\alpha \in \mathbf{R}$ a n-tým sblíženým zlomkem p_n/q_n chápaným jako racionální funkce v x_i je jednoduchý: $r = p_n(a_0, a_1, \ldots, a_n)/q_n(a_0, a_1, \ldots, a_n)$, kde jsme za proměnné x_i dosadili příslušné členy řetězového rozvoje. V následujících dvou lemmatech pracujeme se sblíženými zlomky ve smyslu druhé definice, vše ale samozřejmě platí i pro čísla, stačí psát a_i místo x_i.

Lemma 24. *Čitatele a jmenovatele sblížených zlomků p_n/q_n splňují rekurence*

$$\begin{array}{rclrclrcl} p_0 & = & x_0 \ , & p_1 & = & x_0 x_1 + 1 \ , & p_n & = & x_n p_{n-1} + p_{n-2} \\ q_0 & = & 1 \ , & q_1 & = & x_1 \ , & q_n & = & x_n q_{n-1} + q_{n-2} \ . \end{array}$$

Důkaz. Indukcí podle n. Pro $n = 0, 1$ lemma platí. Předpokládejme platnost rekurence pro n-tý sblížený zlomek. Pro $(n+1)$-tý pak máme

$$\begin{aligned} \frac{p_{n+1}}{q_{n+1}} &= //x_0, x_1, \ldots, x_{n+1}// = //x_0, x_1, \ldots, x_{n-1}, x_n + 1/x_{n+1}// \\ &= \frac{(x_n + 1/x_{n+1})p_{n-1} + p_{n-2}}{(x_n + 1/x_{n+1})q_{n-1} + q_{n-2}} \end{aligned}$$

$$
\begin{aligned}
&= \frac{x_{n+1}(x_n p_{n-1} + p_{n-2}) + p_{n-1}}{x_{n+1}(x_n q_{n-1} + q_{n-2}) + q_{n-1}} \\
&= \frac{x_{n+1} p_n + p_{n-1}}{x_{n+1} q_n + q_{n-1}} \; .
\end{aligned}
$$

Při přechodu na druhý a čtvrtý řádek jsme použili indukční předpoklad. $\diamondsuit$

Lemma 25. *Sblížené zlomky splňují vztahy*

$$
\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1} q_n} \quad a \quad \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n x_n}{q_{n-2} q_n} \; .
$$

DŮKAZ. Opakovaným použitím předchozího lemmatu postupně dostáváme

$$
\begin{aligned}
p_n q_{n-1} - q_n p_{n-1} &= (x_n p_{n-1} + p_{n-2}) q_{n-1} - (x_n q_{n-1} + q_{n-2}) p_{n-1} \\
&= -(p_{n-1} q_{n-2} - q_{n-1} q_{n-2}) \\
&\vdots \\
&= (-1)^{n-1} (p_1 q_0 - q_1 p_0) \\
&= (-1)^{n-1} \; .
\end{aligned}
$$

Pomocí předchozího lemmatu a právě odvozeného vztahu máme

$$
\begin{aligned}
p_n q_{n-2} - q_n p_{n-2} &= (x_n p_{n-1} + p_{n-2}) q_{n-2} - (x_n q_{n-1} + q_{n-2}) p_{n-2} \\
&= x_n (p_{n-1} q_{n-2} - q_{n-1} p_{n-2}) \\
&= (-1)^n x_n \; .
\end{aligned}
$$

$\diamondsuit$

Tvrzení 26 (shrnutí). *Zlomek $p_n/q_n \in \mathbf{Q}$ buď n-tý sblížený zlomek řetězového rozvoje čísla $\alpha \in \mathbf{R}$, čísla a_i buďte členy řetězového rozvoje α.*

1. *p_n/q_n je v základním tvaru. (To jest, čísla p_n a q_n vypočtená z a_i pomocí rekurencí jsou nesoudělná.)*

2. *$p_{2n}/q_{2n} \leq \alpha \leq p_{2n+1}/q_{2n+1}$.*

3. *Rozvoj $//a_0, a_1, \ldots //$ je konečný, právě když α je racionální.*

4. *Racionální α se rovná svému řetězovému rozvoji.*

5. *Pro iracionální α posloupnosti sblížených zlomků*

$$p_0/q_0 < p_2/q_2 < p_4/q_4 < \cdots < \alpha$$

a

$$\alpha < \cdots < p_5/q_5 < p_3/q_3 < p_1/q_1$$

konvergují k α.

6. *Každý sblížený zlomek α je jeho dobrým přiblížením ve smyslu 2 věty 19.*

DŮKAZ. Část 1 plyne z předešlého lemmatu, protože $p_n q_{n-1} - q_n p_{n-1} = \pm 1$. Část 2 vyplývá z rovnosti (8): Nahradíme-li v ní ζ_n nulou, výraz se zmenší pro sudé n a zvětší pro n liché. V 3 je zřejmé, že iracionální α má nekonečný řetězový rozvoj. Nechť nyní $\alpha = p/q \in \mathbf{Q}$. Zřejmě $p/q = \lfloor p/q \rfloor + r_0/q$, kde r_0 je zbytek při dělení p číslem q. Dále $1/\zeta_0 = \lfloor q/r_0 \rfloor + r_1/r_0$, kde r_1 je zbytek při dělení q číslem r_0. A tak dále. Vytváření řetězového rozvoje zlomku p/q je tedy jen jiným popisem Euklidova algoritmu pro hledání (p, q) (viz oddíl 1.1). Odtud je konečnost zřejmá. Rovnost 4 je očividná — jakmile $\zeta_n = 0$, $\alpha = p/q$ se rovná svému řetězovému rozvoji. Část 5 plyne z 2 a z obou vztahů předchozího lemmatu. Část 6 plyne z první rovnosti tohoto lemmatu a z monotonie $q_{n-1} \le q_n$. Dostáváme tak již třetí důkaz 2 věty 19. ◇

Lemma 27. *Sblížené zlomky $p_n/q_n \in \mathbf{Q}$ čísla $\alpha \in \mathbf{R}$ splňují nerovnosti*

$$|\alpha q_0 - p_0| > |\alpha q_1 - p_1| > |\alpha q_2 - p_2| > \cdots \ .$$

DŮKAZ. Nechť $\alpha = //a_0, a_1, \ldots //$ (řetězový rozvoj α může být i konečný). Definujeme reálná čísla β_n a α_n jako $\beta_n = //a_0, a_1, \ldots, a_n//$ a $\alpha_n = //a_n, a_{n+1}, \ldots //$. Podle lemmat 24 a 25 máme

$$q_n \beta_{n+1} - p_n = q_n \frac{p_{n+1}}{q_{n+1}} - p_n = \frac{p_{n+1} q_n - q_{n+1} p_n}{q_{n+1}} = \frac{(-1)^n}{a_{n+1} q_n + q_{n-1}} \ .$$

To platí i tehdy, chápeme-li a_i jako proměnné. Za a_{n+1} v β_{n+1} dosadíme α_{n+1} a máme ($\alpha_{n+1} \ge 1$)

$$|\alpha q_n - p_n| = \frac{1}{\alpha_{n+1} q_n + q_{n-1}} \le \frac{1}{q_n + q_{n-1}} \ .$$

Z druhé strany ($\alpha_n < a_n + 1$), s použitím lemmatu 24 v závěrečné rovnosti,

$$|\alpha q_{n-1} - p_{n-1}| = \frac{1}{\alpha_n q_{n-1} + q_{n-2}} > \frac{1}{(a_n+1)q_{n-1} + q_{n-2}} = \frac{1}{q_n + q_{n-1}} \ .$$

Tím je lemma dokázáno. $\diamondsuit$

Je-li α reálné a čísla $p \in \mathbf{Z}$ a $q \in \mathbf{N}$ jsou taková, že $\|q\alpha\| = |q\alpha - p| < \|r\alpha\|$ pro všechna přirozená čísla r menší než q, nazývá se zlomek p/q *nejlepší aproximací* čísla α.

Věta 28 (Lagrange, 1770). *Nejlepší aproximace $\alpha \in \mathbf{R}$ jsou právě jeho sblížené zlomky.*

DŮKAZ. Nechť $\alpha = //a_0, a_1, \ldots //$ má sblížené zlomky $p_n/q_n \in \mathbf{Q}$. Ukážeme nejprve, že nejlepší aproximace $a/b \in \mathbf{Q}, a \perp b$, se rovná některému z nich. Nerovnost $a/b < p_0/q_0 = a_0 = \lfloor \alpha \rfloor$ je nemožná, plyne z ní totiž

$$|\alpha - a_0| = \alpha - a_0 < \alpha - a/b \le b|\alpha - a/b| = |b\alpha - a| \ ,$$

což je ve sporu s definicí nejlepší aproximace. Podobně je nemožná i nerovnost $a/b > p_1/q_1$, protože implikuje

$$|a/b - \alpha| = a/b - \alpha > a/b - p_1/q_1 \ge 1/bq_1 \ ,$$

což dává opět spor $|b\alpha - a| > 1/q_1 = 1/a_1 \ge |\alpha - a_0|$. Takže $p_0/q_0 \le \alpha \le p_1/q_1$. Kdyby a/b nebyl roven žádnému sblíženému zlomku, ležel by ostře mezi p_{n-1}/q_{n-1} a p_{n+1}/q_{n+1} pro nějaké $n \in \mathbf{N}$. Podle lemmatu 25

$$\frac{1}{bq_{n-1}} \le \left| \frac{a}{b} - \frac{p_{n-1}}{q_{n-1}} \right| < \left| \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \right| = \frac{1}{q_n q_{n-1}} \ .$$

Tedy $q_n < b$. Na druhé straně, podle části 5 tvrzení 26,

$$\frac{1}{bq_{n+1}} \le \left| \frac{p_{n+1}}{q_{n+1}} - \frac{a}{b} \right| \le \left| \alpha - \frac{a}{b} \right| \ .$$

Odtud máme $|q_n\alpha - p_n| < 1/q_{n+1} \le |b\alpha - a|$. Zlomek a/b není nejlepší aproximací α, což je spor. Dokázali jsme první polovinu věty.

Zbývá dokázat, že každý sblížený zlomek je nejlepší aproximací. Postupujeme indukcí podle n. Pro $n = 0$ je p_0/q_0 nejlepší aproximací, protože neexistuje $q \in \mathbf{N}$, $1 \leq q < q_0 = 1$. Nechť již bylo dokázáno, že p_n/q_n je nejlepší aproximace. Jako q označíme první celé číslo větší než q_n, pro něž platí $\|q\alpha\| < \|q_n\alpha\|$. Číslo $p \in \mathbf{Z}$ je určeno z $\|q\alpha\| = |q\alpha - p|$. Podle indukčního předpokladu a definice nejlepší aproximace je jasné, že p/q je nejlepší aproximace α. Podle první části a předchozího lemmatu je jasné, že $q = q_{n+1}$ a $p = p_{n+1}$. $\diamondsuit$

Následující výsledek dokázal A. M. Legendre.

Tvrzení 29 (blízko se dostanou jen řetězové zlomky). *Pokud $\alpha \in \mathbf{R}$, $p/q \in \mathbf{Q}$ a $|\alpha - p/q| < 1/2q^2$, je p/q sblíženým zlomkem čísla α.*

Důkaz. Podle předešlé věty stačí ukázat, že p/q je nejlepší aproximací α. Abychom to ověřili, uvážíme libovolný zlomek a/b různý od p/q, pro nějž platí

$$|b\alpha - a| \leq |q\alpha - p| < 1/2q \ .$$

Tudíž

$$\frac{1}{bq} \leq \left|\frac{a}{b} - \frac{p}{q}\right| \leq \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{p}{q}\right| < \frac{1}{2bq} + \frac{1}{2q^2} = \frac{b+q}{2bq^2} \ .$$

Odtud plyne $q < b$. Číslo p/q je opravdu nejlepší aproximace a tedy sblížený zlomek čísla α. $\diamondsuit$

Věta 30 (Lagrange, 1770). *Číslo $\alpha \in \mathbf{R}$ buď iracionální. Jeho řetězový rozvoj $\alpha = //a_0, a_1, \ldots//$ je od určitého místa periodický, právě když α je kvadratickou iracionalitou.*

Důkaz. Nechť

$$\alpha = //a_0, a_1, \ldots//$$

je periodický rozvoj s předperiodou délky l a periodou délky k. Položíme-li $\alpha_l = //a_l, a_{l+1}, \ldots//$, máme

$$\alpha_l = //a_l, a_{l+1}, \ldots, a_{l+k-1}, \alpha_l// \ .$$

Odtud

$$\alpha_l = \frac{p\alpha_l + p'}{q\alpha_l + q'} \ , \tag{9}$$

kde p/q a p'/q' jsou poslední a předposlední sblížený zlomek čísla $//a_l, \ldots, a_{l+k-1}//$. Pro číslo α platí

$$\alpha = \frac{\alpha_l p_{l-1} + p_{l-2}}{\alpha_l q_{l-1} + q_{l-2}} \tag{10}$$

(p_l/q_l je jeho l-tý sblížený zlomek). Eliminací α_l z (9) a (10) dostáváme pro α kvadratickou rovnici s celočíselnými koeficienty.

Opačná implikace je zajímavější. Nechť iracionální $\alpha \in \mathbf{R}$ splňuje rovnici $a\alpha^2 + b\alpha + c = 0$, kde $a, b, c \in \mathbf{Z}$ a $a \neq 0$. Dokážeme periodičnost řetězového rozvoje $\alpha = //a_0, a_1, \ldots//$. Opět vezmeme čísla

$$\alpha_n = //a_n, a_{n+1}, \ldots// \ .$$

Platí

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \ ,$$

kde p_n/q_n je n-tý sblížený zlomek α. Dosadíme to do rovnice pro α a po úpravách dostaneme

$$A_n \alpha_n^2 + B_n \alpha_n + C_n = 0 \ ,$$

kde

$$\begin{aligned}
A_n &= a p_{n-1}^2 + b p_{n-1} q_{n-1} + c q_{n-1}^2 \ , \\
B_n &= 2a p_{n-1} p_{n-2} + b(p_{n-1} q_{n-2} + q_{n-1} p_{n-2}) + 2c q_{n-1} q_{n-2} \quad \text{a} \\
C_n &= a p_{n-2}^2 + b p_{n-2} q_{n-2} + c q_{n-2}^2 \ .
\end{aligned}$$

Odtud okamžitě plyne, že $C_n = A_{n-1}$. S pomocí lemmatu 25 dostáváme, že

$$B_n^2 - 4A_n C_n = b^2 - 4ac \ .$$

Číslo α se pomocí sblíženého zlomku vyjádří jako $\alpha = \delta/q_{n-1}^2 + p_{n-1}/q_{n-1}$, kde $|\delta| < 1$. Tedy

$$\begin{aligned}
A_n &= a(\alpha q_{n-1} + \delta/q_{n-1})^2 + b(\alpha q_{n-1} + \delta/q_{n-1})q_{n-1} + c q_{n-1}^2 \\
&= q_{n-1}^2(a\alpha^2 + b\alpha + c) + 2a\alpha\delta + a\left(\frac{\delta}{q_{n-1}}\right)^2 + b\delta \\
&= 2a\alpha\delta + a\left(\frac{\delta}{q_{n-1}}\right)^2 + b\delta \ .
\end{aligned}$$

$|A_n|$ proto lze omezit konstantou nezávislou na n. Díky $C_n = A_{n-1}$ a relaci svazující A_n, B_n a C_n totéž platí i pro B_n a C_n. Pro hodnoty veličin A_n, B_n, C_n tedy máme s n probíhajícím přirozená čísla jen konečně mnoho možností. Proto existují (holubníkový princip) tři celá čísla A, B a C a takové tři indexy $n_1 < n_2 < n_3$, že $A_{n_i} = A, B_{n_i} = B$ a $C_{n_i} = C$, $i = 1, 2, 3$. Dostáváme, že čísla α_{n_i} jsou řešením jediné kvadratické rovnice $Ax^2 + Bx + C = 0$. Některá dvě se proto nutně rovnají, například $\alpha_{n_1} = \alpha_{n_3}$. Rozvoj α je tudíž od určitého místa periodický. $\diamondsuit$

O řetězových rozvojích algebraických iracionalit stupně > 2 není téměř nic známo. Například není známo, zda členy řetězového rozvoje $\sqrt[3]{2}$ jsou omezené.

2.3 Řetězový rozvoj čísla e

Ikdyž (jak dokážeme v 2.5) je Eulerovo číslo e transcendentní a jeho řetězový zlomek proto není periodický, řídí se jednoduchým pravidlem.

Věta 31 (Euler, 1737). *Číslo* $\mathrm{e} = 2.71828\ldots$ *má řetězový rozvoj složený z počátečního úseku* $2, 1$ *a z úseků* $2n, 1, 1$, *kde* n *probíhá* $\mathbf{N}$, *to jest*

$$\mathrm{e} = //2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, \ldots// \ .$$

DŮKAZ. Nechť $c \in \mathbf{R}$, kde $c \neq 0, -1, -2, \ldots$. Budeme pracovat s funkcí

$$F(c, x) = \sum_{n=0}^{\infty} \frac{x^n}{c(c+1)\cdots(c+n-1)\cdot n!} \ .$$

Sčítanec s $n = 0$ se definuje jako 1. Pro každé pevné c z uvedeného oboru řada definující $F(c, x)$ konverguje pro všechny argumenty $x \in \mathbf{R}$.

Porovnáním koeficientů u x^n se ujistíme o platnosti identity

$$F(c, x) = F(c+1, x) + \frac{x}{c(c+1)} F(c+2, x) \ .$$

Úpravou z ní odvodíme vztah

$$\frac{F(c+1, x)}{F(c, x)} = \frac{1}{1 + \dfrac{x}{c(c+1)} \cdot \dfrac{F(c+2, x)}{F(c+1, x)}} \ .$$

Položíme $x = z^2$ a upravujeme dále:

$$\frac{z}{c} \cdot \frac{F(c+1, z^2)}{F(c, z^2)} = \cfrac{1}{\cfrac{c}{z} + \cfrac{z}{c+1} \cfrac{F(c+2, z^2)}{F(c+1, z^2)}} \ .$$

Opakováním této transformace získáme řetězový rozvoj

$$\begin{aligned} \frac{z}{c} \cdot \frac{F(c+1, z^2)}{F(c, z^2)} &= //0, \tfrac{c}{z}, \tfrac{c+1}{z}, \ldots \\ &\quad \ldots, \tfrac{c+n}{z}, \tfrac{c+n+1}{z} \cdot \tfrac{F(c+n+1, z^2)}{F(c+n+2, z^2)}// \ . \end{aligned}$$

V dalším bude $c = 1/2$ a $z = 1/2y$, kde $y \in \mathbf{N}$. Pak $(c+n)/z \in \mathbf{N}$ pro všechna $n \in \mathbf{N}_0$. Protože $F(c+n+1, z^2)/F(c+n+2, z^2) > 1$, je

$$\frac{c+n+1}{z} \cdot \frac{F(c+n+1, z^2)}{F(c+n+2, z^2)} > 1$$

a můžeme rozvíjet donekonečna:

$$\frac{z}{c} \cdot \frac{F(c+1, z^2)}{F(c, z^2)} = //0, \tfrac{c}{z}, \tfrac{c+1}{z}, \tfrac{c+2}{z}, \ldots // \ . \tag{12}$$

Z mocninného rozvoje exponenciální funkce

$$\mathrm{e}^w = \sum_{n=0}^{\infty} \frac{w^n}{n!}$$

a z definice $F(c, x)$ plynou identity

$$\begin{aligned} \mathrm{e}^w - \mathrm{e}^{-w} &= 2w \sum_{n=0}^{\infty} \frac{(w^2)^n}{(2n+1)!} &= 2wF(3/2, w^2/4) \ \text{ a} \\ \mathrm{e}^w + \mathrm{e}^{-w} &= 2 \sum_{n=0}^{\infty} \frac{(w^2)^n}{(2n)!} &= 2F(1/2, w^2/4) \ . \end{aligned}$$

Položíme $w = 1/y, y \in \mathbf{N}$, a utvoříme podíl obou rovností. S použitím (12) dostáváme podivuhodnou identitu

$$\frac{\mathrm{e}^{1/y} - \mathrm{e}^{-1/y}}{\mathrm{e}^{1/y} + \mathrm{e}^{-1/y}} = //0, y, 3y, 5y, 7y, \ldots // \ .$$

Volba $y = 2$ vede k rovnosti

$$\frac{\mathrm{e}-1}{\mathrm{e}+1} = //0, 2, 6, 10, 14, \dots// \ .$$

Hledaný rozvoj e odtud odvodíme hrubou silou. Položíme

$$\alpha = \frac{\mathrm{e}+1}{\mathrm{e}-1} \ .$$

Je to reciproká hodnota právě uvažovaného čísla, a tak

$$\alpha = //2, 6, 10, 14, 18, \dots// \ .$$

Nechť r_n/s_n je n-tý sblížený zlomek α. Ukážeme, že reálné číslo

$$\xi = //2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \dots//$$

se rovná číslu

$$\mathrm{e} = \frac{\alpha+1}{\alpha-1} \ .$$

Nechť p_n/q_n je n-tý sblížený zlomek ξ.

Pro každé celé $n \geq 0$ dokážeme platnost rovností

$$p_{3n+1} = r_n + s_n \quad \text{a} \quad q_{3n+1} = r_n - s_n \ . \tag{13}$$

Pro $n = 0, 1$ tyto rovnosti platí, přímý výpočet rekurentními vztahy totiž ukazuje, že $p_1 = 3, q_1 = 1, r_0 = 2, s_0 = 1$ a $p_4 = 19, q_4 = 7, r_1 = 13, s_1 = 6$. Pro $n > 1$ užijeme indukci. Nechť (13) platí pro $n - 1$. Lemma 24 dává pro r_n a s_n vztahy

$$r_n = (2+4n)r_{n-1} + r_{n-2} \quad \text{a} \quad s_n = (2+4n)s_{n-1} + s_{n-2} \ . \tag{14}$$

Pro p_n, jakož i pro q_n, máme rekurence

$$\begin{array}{lcll}
p_{3n-3} & = & p_{3n-4} + p_{3n-5} & \quad 1 \\
p_{3n-2} & = & p_{3n-3} + p_{3n-4} & \quad -1 \\
p_{3n-1} & = & 2np_{3n-2} + p_{3n-3} & \quad 2 \\
p_{3n} & = & p_{3n-1} + p_{3n-2} & \quad 1 \\
p_{3n+1} & = & p_{3n} + p_{3n-1} & \quad 1
\end{array}$$

Lineární kombinací užívající koeficientů uvedených vpravo dostáváme

$$p_{3n+1} = (4n+2)p_{3n-2} + p_{3n-5} \quad \text{a} \quad q_{3n+1} = (4n+2)q_{3n-2} + q_{3n-5} \ .$$

S pomocí rovnic (14) plynou rovnice (13) indukcí.

Vztah (13) je dokázán, platí tedy

$$\frac{p_{3n+1}}{q_{3n+1}} = \frac{r_n + s_n}{r_n - s_n} = \frac{r_n/s_n + 1}{r_n/s_n - 1} .$$

Limitním přechodem, $n \to \infty$, plyne kýžená rovnost

$$\xi = \frac{\alpha + 1}{\alpha - 1} = \mathrm{e} .$$

$\diamondsuit$

2.4 Iracionalita čísla $\zeta(3)$

Věta 32 (Apéry, 1979). *Číslo*

$$\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3} = \frac{1}{1} + \frac{1}{8} + \frac{1}{27} + \cdots = 1.20205\ldots$$

je iracionální.

Zda jsou i jiné hodnoty $\zeta(2k+1)$ funkce $\zeta(s)$ v lichých číslech iracionální není známo. Hodnoty $\zeta(2k)$ jsou racionální násobky mocnin čísla π a jsou tedy transcendentní (úloha 12.)

Začneme serií lemmat. Důkaz používá reálnou analýzu, v závěru budeme potřebovat prvočíselnou větu z kapitoly 5. Začíná analytická magie.

Pro čísla $r, s \in \mathbf{N}_0$ a $\sigma \in \mathbf{R}, \sigma \geq 0$, máme identity

$$\begin{aligned}
\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1 - xy}\, dx\, dy &= \sum_{k=0}^{\infty} \frac{1}{(k+r+\sigma+1)(k+s+\sigma+1)} \\
&= \sum_{k=0}^{\infty} \frac{1}{r-s} \left(\frac{1}{k+s+\sigma+1} - \frac{1}{k+r+\sigma+1} \right) \\
&= \frac{1}{r-s} \left(\frac{1}{s+1+\sigma} + \frac{1}{s+2+\sigma} + \cdots + \frac{1}{r+\sigma} \right) .
\end{aligned}$$

První řádek plyne rozvinutím $1/(1-xy)$ do geometrické řady a záměnou pořadí integrace a sumace. Druhý řádek představuje elementární úpravu platnou pro $r \neq s$. Na třetím řádku předpokládáme navíc, že $r > s$.

Nechť $V(r) = [1, 2, \ldots, r]$ je nejmenší společný násobek čísel $1, 2, \ldots, r$.

Lemma 33. *Pro $r, s \in \mathbf{N}_0$, $r > s$, máme*

$$\int_0^1 \int_0^1 \frac{\log(xy)}{1-xy} x^r y^s \, dx \, dy = \frac{a}{b} \in \mathbf{Q} \ ,$$

kde $a \perp b$ a jmenovatel b dělí $V(r)^3$.

Důkaz. Hořejší identitu

$$\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1-xy} \, dx \, dy = \frac{1}{r-s} \left(\frac{1}{s+1+\sigma} + \frac{1}{s+2+\sigma} + \cdots + \frac{1}{r+\sigma} \right)$$

derivujeme nejprve podle σ (záměna pořadí derivování a integrace) a pak položíme $\sigma = 0$. Dostaneme

$$\int_0^1 \int_0^1 \frac{\log(xy)}{1-xy} x^r y^s \, dx \, dy = \frac{-1}{r-s} \left(\frac{1}{(s+1)^2} + \frac{1}{(s+2)^2} + \cdots + \frac{1}{r^2} \right)$$

a vše je jasné. ◊

Lemma 34. *Pro $r \in \mathbf{N}_0$ máme*

$$\int_0^1 \int_0^1 \frac{\log(xy)}{1-xy} (xy)^r \, dx \, dy = -2 \left(\zeta(3) - \frac{1}{1^3} - \frac{1}{2^3} - \cdots - \frac{1}{r^3} \right) .$$

Důkaz. Hořejší identitu

$$\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1-xy} \, dx \, dy = \sum_{k=0}^{\infty} \frac{1}{r-s} \left(\frac{1}{k+s+\sigma+1} - \frac{1}{k+r+\sigma+1} \right)$$

nejprve derivujeme podle σ (záměna pořadí derivování a integrace, derivování a sumace) a pak položíme $r = s$ a $\sigma = 0$. Dostaneme

$$\int_0^1 \int_0^1 \frac{\log(xy)}{1-xy} (xy)^r \, dx \, dy = \sum_{k=0}^{\infty} \frac{-2}{(k+r+1)^3}$$

a vše je jasné. ◊

Zavedeme celočíselný polynom

$$P_n(x) = \frac{1}{n!} \left(\frac{d}{dx} \right)^n (x^n (1-x)^n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n+k}{n} x^k \ .$$

Lemma 35. *Pro každé číslo $n \in \mathbf{N}$ máme vztah*

$$\int_0^1 \int_0^1 \frac{-\log(xy)}{1-xy} P_n(x) P_n(y)\, dx\, dy = \frac{a_n \zeta(3) + b_n}{V(n)^3} \ ,$$

kde $a_n, b_n \in \mathbf{Z}$.

Důkaz. Plyne z obou předchozích lemmat. $\diamondsuit$

Lemma 36 *Platí*

$$\int_0^1 \int_0^1 \frac{-\log(xy)}{1-xy} P_n(x) P_n(y)\, dx\, dy =$$
$$= \int_0^1 \int_0^1 \int_0^1 \frac{(x(1-x)y(1-y)w(1-w))^n}{(1-(1-xy)w)^{n+1}}\, dx\, dy\, dw > 0 \ .$$

Důkaz. Pomocí

$$\frac{-\log(xy)}{1-xy} = \int_0^1 \frac{dz}{1-(1-xy)z}$$

nahradíme dvojitý integrál na levé straně trojitým integrálem

$$\int_0^1 \int_0^1 \int_0^1 \frac{P_n(x) P_n(y)}{1-(1-xy)z}\, dx\, dy\, dz \ .$$

Ten pomocí definice $P_n(x)$ proměníme n-násobnou integrací per partes podle x v integrál

$$\int_0^1 \int_0^1 \int_0^1 \frac{(xyz)^n (1-x)^n P_n(y)}{(1-(1-xy)z)^{n+1}}\, dx\, dy\, dz \ .$$

Užijeme substituci

$$w = w(z) = \frac{1-z}{1-(1-xy)z},\ dz = \frac{1-(1-xy)z}{w(1-xy)-1} dw \ .$$

Ve výsledném integrálu (nepřehlédněme, že w probíhá $[0,1]$ v opačném smyslu, než z)

$$\int_0^1 \int_0^1 \int_0^1 (1-x)^n (1-w)^n \frac{P_n(y)}{1-(1-xy)w}\, dx\, dy\, dw$$

integrujeme n krát per partes podle y. Dostaneme

$$\int_0^1 \int_0^1 \int_0^1 \frac{x^n (1-x)^n y^n (1-y)^n w^n (1-w)^n}{(1-(1-xy)w)^{n+1}}\, dx\, dy\, dw \ .$$

Tento integrál je navíc bezpochyby kladný, protože jeho integrand je v daném oboru kladný. $\diamondsuit$

Lemma 37. *Jako I označíme otevřený jednotkový interval* $(0,1)$. *Pak*

$$\max_{x,y,w\in I} \frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w} = (\sqrt{2}-1)^4.$$

Důkaz. Nejprve pro pevné $x, y \in I$ najdeme maximum

$$M(\alpha) = \max_{w\in I} \frac{w(1-w)}{1-\alpha w}\ ,$$

kde $\alpha = 1 - xy$. Standardním postupem („derivaci polož rovnu nule") se zjistí, že

$$M(\alpha) = \left(\frac{1-\sqrt{1-\alpha}}{\alpha}\right)^2$$

a nabývá se v $w = (1-\sqrt{1-\alpha})/\alpha$. Nyní zmaximalizujeme výraz

$$x(1-x)y(1-y)M(\alpha) = \frac{x(1-x)y(1-y)}{(1+\sqrt{xy})^2}\ ,$$

přičemž $xy = \beta^2$ bude konstanta a x, y leží v I. Hledáme tedy maximum výrazu

$$\frac{\beta^2(1+\beta^2-(x+\beta^2/x))}{(1+\beta)^2}$$

pro $x \in I$. To znamená minimalizovat $x + \beta^2/x$. Hned se vidí, že minimum 2β se nabývá pro $x = \beta$. Dostáváme maximum

$$\left(\frac{\beta(1-\beta)}{1+\beta}\right)^2.$$

Funkce $\beta(1-\beta)/(1+\beta)$ nabývá na I maxima $(\sqrt{2}-1)^2$ a to pro $\beta = \sqrt{2}-1$. Celkové maximum je tedy $(\sqrt{2}-1)^4$ a nabývá se v $x = y = \beta = \sqrt{2}-1$ a $w = 1/(1+\beta) = \sqrt{2}/2$. $\diamondsuit$

DŮKAZ VĚTY 32. Podle lemmat 35, 36, 37 a 34 pro každé číslo $n \in \mathbf{N}$ existují celá čísla $a_n, b_n \in \mathbf{Z}$ taková, že

$$\begin{aligned} 0 < |a_n\zeta(3) + b_n| &\leq V(n)^3(\sqrt{2}-1)^{4n} \int_0^1 \int_0^1 \int_0^1 \frac{dx\, dy\, dw}{1-(1-xy)w} \\ &= V(n)^3(\sqrt{2}-1)^{4n} \int_0^1 \int_0^1 \frac{-\log(xy)}{1-xy}\, dx\, dy \\ &= 2\zeta(3)V(n)^3(\sqrt{2}-1)^{4n}. \end{aligned}$$

Pro velká n platí odhad

$$V(n) \leq n^{\pi(n)} < 3^n,$$

neboť $V(n)$ je součinem $\pi(n)$ mocnin prvočísel, z nichž žádná nepřesahuje n, a $\pi(n) \sim n/\log n$ podle prvočíselné věty (věta **??** z páté kapitoly). Pro všechna $n > n_0$ tak platí odhad

$$0 < |a_n\zeta(3) + b_n| < 2\zeta(3) \cdot 27^n \cdot (\sqrt{2}-1)^{4n} < (4/5)^n.$$

Pokud $\zeta(3) = c/d \in \mathbf{Q}$, jsou tyto nerovnosti sporné. Podle první z nich je $|a_n\zeta(3) + b_n| \geq 1/d$ pro všechna $n \in \mathbf{N}$, zatímco podle poslední má pro $n \to \infty$ daná veličina jít k nule.

2.5 Transcendence čísel e a π

Uvádíme dva klasické výsledky z teorie transcendentních čísel. Důsledkem druhého z nich je nemožnost kvadratury kruhu: Pomocí pravítka a kružítka nelze k danému kruhu sestrojit rovnoplochý čtverec.

Věta 38 (Hermite, 1873). *Číslo* $\mathrm{e} = 2.71828\ldots$ *je transcendentní.*

DŮKAZ. **(Hilbert, 1893.)** Integrací per partes se pro každé $k \in \mathbf{N}$ snadno spočte, že

$$\int_0^\infty x^k \mathrm{e}^{-x} dx = k!\ .$$

Pro každý celočíselný polynom $p(x) \in \mathbf{Z}[x]$ je proto následující integrál rovný celému číslu a navíc

$$\int_0^\infty x^k p(x) \mathrm{e}^{-x} dx \equiv p(0)k! \bmod (k+1)!\ . \tag{15}$$

Nechť je číslo e algebraické stupně n a splňuje rovnici

$$a_0 + a_1\mathrm{e} + \cdots + a_n\mathrm{e}^n = 0 \ , \tag{16}$$

kde $a_i \in \mathbf{Z}$ a $a_0 \neq 0$. (Nenulovost konstantního členu se dá vždy dosáhnout zkrácením mocniny x.) Tuto rovnost přivedeme ke sporu.

Pro $r \in \mathbf{N}$ a reálná čísla $b \leq c \leq \infty$ definujeme zkratku

$$\int_b^c = \int_b^c x^r((x-1)(x-2)\cdots(x-n))^{r+1}\mathrm{e}^{-x}dx \ .$$

Rovnici (16) vynásobíme $\int_0^\infty$ a vzniklý součet $n+1$ integrálů rozložíme na

$$P_1 + P_2 = 0 \ ,$$

kde

$$\begin{aligned} P_1 &= a_0\int_0^\infty + a_1\mathrm{e}\int_1^\infty + \cdots + a_n\mathrm{e}^n\int_n^\infty \quad \text{a} \\ P_2 &= a_1\mathrm{e}\int_0^1 + a_2\mathrm{e}^2\int_0^2 + \cdots + a_n\mathrm{e}^n\int_0^n \ . \end{aligned}$$

Pomocí substituce $y = x - k$ vypočteme

$$\begin{aligned} a_k\mathrm{e}^k\int_k^\infty &= a_k\int_k^\infty x^r((x-1)\cdots(x-n))^{r+1}\mathrm{e}^{-(x-k)}dx \\ &= a_k\int_0^\infty (y+k)^r((y+k-1)\cdots(y+k-n))^{r+1}\mathrm{e}^{-y}dy \\ &= \begin{cases} a_0\int_0^\infty y^r p_0(y)\mathrm{e}^{-y}dy & \text{pro } k=0 \text{ a} \\ \\ a_k\int_0^\infty y^{r+1}p_k(y)\mathrm{e}^{-y}dy & \text{pro } 0 < k \leq n \ , \end{cases} \end{aligned}$$

kde $p_i(y) \in \mathbf{Z}[y]$ je jistý polynom. Podle (15) dostáváme

$$P_1 \equiv a_0p_0(0)r! \equiv a_0(-1)^{n(r+1)}(n!)^{r+1}r! \bmod (r+1)! \ .$$

Pro $(r+1) \perp a_0n!$ je P_1 nenulové celé číslo dělitelné $r!$ (teď potřebujeme, že $a_0 \neq 0$). Nechť M a N jsou maxima funkcí $|x(x-1)\cdots(x-n)|$ a $|x(x-1)\cdots(x-n)\mathrm{e}^{-x}|$ na intervalu $[0,n]$. Pro $1 \leq k \leq n$ máme

$$\left|a_k\int_0^k\right| \leq |a_k|\int_0^k M^rNdx = k|a_k|M^rN \ ,$$

a proto
$$|P_2| \le (|a_1|\mathrm{e} + 2|a_2|\mathrm{e}^2 + \cdots + n|a_n|\mathrm{e}^n)M^r N \ .$$
Pro $r \to \infty$ je tedy $P_2 = o(r!)$. Protože máme nekonečně hodnot $r \in \mathbf{N}$, pro něž je P_1 nenulový násobek $r!$, a přitom vždy platí rovnost $P_1 + P_2 = 0$, dostáváme spor. $\diamondsuit$

Věta 39 (Lindemann, 1882). *Číslo $\pi = 3.14159\ldots$ je transcendentní.*

DŮKAZ. **(Hilbert, 1893.)** Nechť je číslo π algebraické. Pak, podle tvrzení 14 z 1. kapitoly, je algebraické i číslo $i\pi$, kde $i = \sqrt{-1}$. Nechť $\alpha_1 = i\pi, \alpha_2, \ldots, \alpha_n$ jsou všechny kořeny celočíselného polynomu, který se anuluje na $i\pi$. Potom
$$(1 + \mathrm{e}^{\alpha_1})(1 + \mathrm{e}^{\alpha_2}) \cdots (1 + \mathrm{e}^{\alpha_n}) = 1 + \mathrm{e}^{\beta_1} + \cdots + \mathrm{e}^{\beta_m} = 0 \ ,$$
protože $1 + \mathrm{e}^{i\pi} = 0$. Čísla $\beta_1, \ldots, \beta_m$, jichž je $m = 2^n - 1$, jsou rovněž algebraická, jsou to totiž všechny možné součty vytvořené z čísel α_i. Tvrzení 14 nám dává ještě více — stejně jako v jeho důkazu se dostane, že β_j jsou kořeny celočíselného polynomu $h(x)$ stupně m.

Lze předpokládat, že nulová β_j jsou čísla $\beta_m = \beta_{m-1} = \cdots = \beta_{m-a+1} = 0$. Takže
$$(1 + a) + \mathrm{e}^{\beta_1} + \cdots + \mathrm{e}^{\beta_{m-a}} = 0 \ , \tag{17}$$
kde $a \in \mathbf{N}_0$ a $\beta_1, \ldots, \beta_{m-a} \in \mathbf{C}^{\,\mathrm{alg}}$ jsou nenulová čísla. Tuto rovnost přivedeme ke sporu.

Čísla $\beta_1, \ldots, \beta_{m-a}$ jsou kořeny celočíselného polynomu
$$f(x) = h(x)/x^a = bx^l + b_1 x^{l-1} + \cdots + b_l \ ,$$
kde $l = m - a$ a celá čísla b, b_l nejsou nulová.

Rovnost (17) vynásobíme integrálem
$$\int_0^\infty = \int_0^\infty x^r (b^l f(x))^{r+1} \mathrm{e}^{-x} dx \ ,$$
kde $r \in \mathbf{N}$ je parametr, který vhodně zvolíme později. Opět máme rozklad
$$P_1 + P_2 = 0 \ ,$$

kde

$$\begin{aligned}P_1 &= (a+1)\int_0^\infty + \mathrm{e}^{\beta_1}\int_{\beta_1}^\infty + \cdots + \mathrm{e}^{\beta_l}\int_{\beta_l}^\infty \quad \text{a}\\ P_2 &= \mathrm{e}^{\beta_1}\int_0^{\beta_1} + \mathrm{e}^{\beta_2}\int_0^{\beta_2} + \cdots + \mathrm{e}^{\beta_l}\int_0^{\beta_l} .\end{aligned}$$

Integrály v P_1 jsou přes polopřímku rovnoběžnou s reálnou osou a běžící z β_j do ∞. Integrály v P_2 jsou přes příslušnou úsečku.

Po rozvinutí Taylorovou řadou vidíme, že $(y+\beta_j)^r(b^l f(y+\beta_j))^{r+1}$ jako polynom v y má nejnižší mocninu y^{r+1}, protože $f(\beta_j)=0$. Po jejím vytknutí zbývá polynom v y stupně $l(r+1)-1$, jehož koeficienty (polynomy ze $\mathbf{Z}[\beta_j]$) mají koeficienty dělitelné $b^{l(r+1)}$. Proto s pomocí substituce $y = x - \beta_j$ a kongruence (15) dostáváme

$$\begin{aligned}\mathrm{e}^{\beta_j}\int_{\beta_j}^\infty &= \int_0^\infty (y+\beta_j)^r(b^l f(y+\beta_j))^{r+1}\mathrm{e}^{-y}dy\\ &= (r+1)!G(b\beta_j) ,\end{aligned}$$

kde $G(x) \in \mathbf{Z}[x]$ je jistý polynom.

Jak víme, $b\beta_1, \dots, b\beta_l \in \mathbf{C}^{\,\mathrm{calg}}$, neboť jde o kořeny monického polynomu $g(y) \in \mathbf{Z}[y]$, kde $y = bx$ a $g(y) = b^{l-1}f(x)$. Tudíž

$$G(b\beta_1) + \cdots + G(b\beta_l) \in \mathbf{Z} ,$$

protože podle věty 13 a Viètových vztahů je tato suma rovna hodnotě jistého celočíselného polynomu na koeficientech $g(y)$.

V P_1 tak posledních l sčítanců dává dohromady celočíselný násobek $(r+1)!$. Co se týče prvního sčítance, podle kongruence (15) máme

$$\int_0^\infty \equiv r! b^{rl+l} b_l^{r+1} \bmod (r+1)! .$$

Takže $P_1 \in \mathbf{Z}$ a

$$P_1 \equiv r!(a+1)b^{rl+l}b_l^{r+1} \bmod (r+1)! .$$

Člen P_2 se odhadne jako v předchozí větě. Vyjde odhad

$$|P_2| \ll M^r,$$

kde M je vhodná konstanta. Rovnost $P_1 + P_2 = 0$ je tak opět nemožná — pro nekonečně mnoho $r \in \mathbf{N}$ je P_1 nenulový násobek $r!$ (protože $bb_l \neq 0$, stačí vzít r tak, že $(r+1) \perp (a+1)bb_l$) a současně $P_2 = o(r!)$. $\diamondsuit$

2.6 Liouvilleova nerovnost

Oba předchozí důkazy jsou docela rafinované. Mnohem jednodušší důkazy transcendence řady čísel poskytuje Liouvilleova věta.

Věta 40 (Liouville, 1844). *Je-li $\alpha \in \mathbf{R}$ algebraické číslo stupně $n \geq 2$, existuje konstanta $c > 0$ závisející jen na α taková, že*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n} \tag{18}$$

pro všechny zlomky $p/q \in \mathbf{Q}$.

Důkaz. Nechť $P(x) \in \mathbf{Z}[x]$ je celočíselný polynom stupně n s kořenem α. Jako I označíme interval $[\alpha - 1, \alpha + 1]$. Konstantu d zavedeme vztahem

$$d = \max_{x \in I} |P'(x)| \ .$$

Ukážeme, že (18) platí s konstantou $c = \min(1, 1/d)$. Pro zlomek $p/q \notin I$ platí (18) triviálně. Pokud $p/q \in I$, použijeme Lagrangeovu větu o střední hodnotě:

$$\frac{P(p/q)}{p/q - \alpha} = \frac{P(p/q) - P(\alpha)}{p/q - \alpha} = P'(y) \ , \tag{19}$$

kde $y \in \mathbf{R}$ leží mezi α a p/q. Jistě $P(p/q) \neq 0$, jinak by $P(x)/(x - p/q)$ byl (racionální) polynom s kořenem α a stupněm menším než má $P(x)$. Navíc je $P(p/q)$ zlomek se jmenovatelem nepřesahujícím q^n. Proto

$$|P(p/q)| \geq \frac{1}{q^n} \ . \tag{20}$$

Z (19) a (20) ihned máme

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{P(p/q)}{P'(y)}\right| \geq \frac{1}{dq^n} \geq \frac{c}{q^n} \ .$$

$\diamondsuit$

(Alternativní důkaz je naznačen v úloze 19.) Věta má následující praktický korolár.

Tvrzení 41 (příznak transcendence). *Každé reálné iracionální číslo α, pro něž má pro každé $n \in \mathbf{N}$ nerovnost*

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

řešení $p/q \in \mathbf{Q}$ s $q > 1$, je transcendentní.

Proto je například číslo

$$\beta = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.110001000000000000000001 0\ldots$$

transcendentní (úloha 20). Reálná iracionální čísla splňující podmínku tvrzení 41 se nazývají *Liouvilleova*.

Z 2 věty 19 plyne, že pro algebraické číslo $\alpha \in \mathbf{R}$ stupně 2 je exponent $n = 2$ v (18) nejlepší (tj. nejmenší) možný. Víme dokonce (věta 23), že pak $c < 1/\sqrt{5}$.

2.7 Thueho věta

Pro čísla $\alpha \in \mathbf{R} \cap \mathbf{C}^{\,\mathrm{alg}}$ stupně $n \geq 3$ se dá exponent n v Liouvilleově nerovnosti snížit. Toto snížení má dalekosáhlé důsledky pro řešení diofantických rovnic a je hlubokým výsledkem o algebraických číslech.

Věta 42 (Thue, 1909). *Nechť $\alpha \in \mathbf{R}$ je algebraické číslo stupně $n \geq 2$ a číslo $\varepsilon > 0$ je pevné. Nerovnost*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{n/2+1+\varepsilon}} \tag{21}$$

má jen konečně mnoho řešení $p/q \in \mathbf{Q}$.

Všimněme si, že pro $n = 2$ jde o tvrzení slabší než Liouvilleova věta.

Bez újmy na obecnosti můžeme předpokládat, že $p \perp q$. Další zjednodušení je, že Thueho větu stačí dokázat pro celá algebraická čísla. Skutečně, pro $\alpha \in \mathbf{C}^{\,\mathrm{alg}}$ existuje $b \in \mathbf{Z}$, že $\beta = b\alpha \in \mathbf{C}^{\,\mathrm{calg}}$ a (21) implikuje nerovnost

$$\left|\beta - \frac{bp}{q}\right| < \frac{b}{q^{n/2+1+\varepsilon}} = \frac{b}{q^{\varepsilon/2}} \cdot \frac{1}{q^{n/2+1+\varepsilon/2}}\ .$$

Nekonečný počet řešení (21) by tedy znamenal i nekonečný počet řešení nerovnosti

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{q^{n/2+1+\varepsilon/2}} \ .$$

V dalším je proto α reálné celé algebraické číslo stupně ≥ 3.

Nejprve dokážeme pomocné tvrzení a čtyři lemmata.

Tvrzení 43 (Siegelovo lemma). *Buď dána soustava m homogeních lineárních rovnic s n neznámými, přičemž celočíselné koeficienty $a_{ij} \in \mathbf{Z}$ splňují nerovnost $|a_{ij}| \leq A$. Dále se předpokládá, že $n > m$. Potom má soustava celočíselné řešení $z_1, z_2, \ldots, z_n \in \mathbf{Z}$ takové, že některé z_i je nenulové a každé z_i splňuje nerovnost*

$$|z_i| \leq \lfloor (nA)^{m/(n-m)} \rfloor \ .$$

Důkaz. Pravou stranu poslední nerovnice označíme jako Z. Podle definice je $Z + 1 > (nA)^{m/(n-m)}$. Odtud plyne, že

$$(nAZ + 1)^m < (Z + 1)^n \ . \tag{22}$$

Lineární formy soustavy označíme jako L_j, $j = 1, \ldots, m$. A_j buď součet kladných koeficientů L_j a $-B_j$ součet záporných koeficientů. Pro $z_i \in \mathbf{Z}, i = 1 \ldots n$, splňující $0 \leq z_i \leq Z$ platí odhad

$$-B_j Z \leq L_j(z_1, \ldots, z_n) \leq A_j Z \ .$$

Dále $A_j + B_j \leq nA$. Číslo $L_j(z_1, \ldots, z_n) \in \mathbf{Z}$ padne do intervalu $[-B_j Z, A_j Z]$ délky nejvýše nAZ a může tedy nabývat nejvýše $nAZ + 1$ hodnot. Pro hodnoty m lineárních forem máme nejvýše

$$(nAZ + 1)^m$$

možností, což je podle (22) méně, než kolik je možných argumentů $z_1, \ldots, z_n$. Pro dva různé argumenty $v_1, \ldots, v_n$ a $w_1, \ldots, w_n$ proto (holubníkový princip) platí $L_j(v_1, \ldots, v_n) = L_j(w_1, \ldots, w_n)$ pro všechna $j = 1 \ldots m$. Pak $z_i = v_i - w_i$ představují hledané řešení. $\diamondsuit$

Následující výsledek plyne z tvrzení 12 v 1. kapitole.

Lemma 44. *Nechť polynom $P(x) \in \mathbf{Z}[x]$ má r-násobný racionální kořen p/q, $p \perp q$. Potom $P(x) = (qx - p)^r R(x)$, kde $R(x) \in \mathbf{Z}[x]$.*

Vahou $v(P)$ celočíselného polynomu $P \in \mathbf{Z}[x_1, \ldots, x_r]$ rozumíme největší absolutní hodnotu koeficientu. Připomínáme, že číslo $\alpha \in \mathbf{R}$ je celé algebraické stupně $n \geq 3$ a $\varepsilon > 0$ je pevné reálné číslo. Čísla $h \in \mathbf{N}$ a $\delta \in \mathbf{R}, 0 < \delta < 1$, jsou parametry, jejichž hodnotu vhodně zvolíme v závěru důkazu. Kladné konstanty $c_1, c_2, \ldots$, které postupně definujeme, závisejí jen na δ (a na čísle α, ale to se nemění). Položíme

$$m = \lfloor (n-2)(1+\delta)h/2 \rfloor \; . \tag{23}$$

Lemma 45. *Existují celočíselné polynomy* $P(x), Q(x) \in \mathbf{Z}[x]$, *oba nenulové, které mají následující tři vlastnosti. (i)* $\deg(P), \deg(Q) \leq m + h$, *(ii)* $v(P), v(Q) < c_2^h$ *a (iii) platí identita*

$$P(x) - \alpha Q(x) = (x-\alpha)^h (R_0(x) + \alpha R_1(x) + \cdots + \alpha^{n-1} R_{n-1}(x)) \; ,$$

kde $R_i(x) \in \mathbf{Z}[x]$ *a* $\deg(R_i) \leq m$.

Důkaz. Polynomy P a Q definujeme pomocí relace (iii). Polynomy R_i mají celkem $N = n(m+1)$ neznámých koeficientů. Redukcí mocnin α (nyní použijeme, že α je *celé* algebraické, podrobněji dále) vyjádříme pravou stranu rovnice v (iii) ve tvaru

$$S_0(x) + \alpha S_1(x) + \cdots + \alpha^{n-1} S_{n-1}(x) \; ,$$

kde koeficienty polynomů $S_i(x)$ jsou celočíselnými lineárními kombinacemi koeficientů polynomů $R_i(x)$. Zřejmě $\deg(S_i) \leq m + h$. Splnit (iii) a definovat tak $P = S_0$ a $Q = -S_1$ znamená zajistit, aby $S_2(x), \ldots, S_{n-1}(x)$ byly identicky nulové. Pro koeficienty polynomů R_i tak dostáváme $M = (n-2)(h+m+1)$ lineárních homogeních rovnic s celočíselnými koeficienty. Tvrzení 43 zaručující existenci nevelkého netriviálního (tj. všechny R_i nejsou identicky nulové) řešení lze použít, pokud

$$N = n(m+1) > M = (n-2)(h+m+1) \; .$$

To je ekvivalentní nerovnosti $m > \frac{1}{2}h(n-2) - 1$, kterou hodnota (23) splňuje pro každé $\delta > 0$.

Ze Siegelova lemmatu tedy dostaneme polynomy R_i. Získané polynomy P a Q nejsou současně nulové, protože na pravé straně (iii) je součin nenulových polynomů. Že jsou dokonce oba nenulové plyne z argumentu, který je použit obecněji v následujícím lemmatu. Splnili jsme (i) a (iii).

Zbývá dokázat odhad (ii). Víme, že α splňuje rovnici $\alpha^n = k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}$, kde $k_i \in \mathbf{Z}$. Nechť k je největší hodnota $|k_i|$. Pro $l \geq n$ máme rovnici $\alpha^l = \alpha^{l-n}\alpha^n = k_0\alpha^{l-n} + k_1\alpha^{l-n+1} + \cdots + k_{n-1}\alpha^{l-1}$. Indukcí podle l dostáváme, že $\alpha^l = k'_0 + k'_1\alpha + \cdots + k'_{n-1}\alpha^{n-1}$, kde $|k'_i| \leq (nk)^{l-n+1}$. S užitím těchto vyjádření upravíme pravou stranu (iii) na

$$\sum_{i=0}^{n-1} R_i(x) \sum_{j=0}^{h} (-1)^j \binom{h}{j} \alpha^{j+i} x^{h-j} = \sum_{i=0}^{n-1} R_i(x) T_i(\alpha, x) = \sum_{i=0}^{n-1} \alpha^i S_i(x) \ ,$$

kde polynom $T_i(\alpha, x) \in \mathbf{Z}[\alpha, x]$ má v α stupeň nejvýše $n-1$ a v x nejvýše h a jeho váha nepřesahuje

$$\binom{h}{\lfloor h/2 \rfloor} (nk)^{i+h-n+1} \ .$$

Podíváme se na koeficienty polynomů $S_i(x)$. Fixujeme celá čísla $a, 0 \leq a \leq h+m$ a $b, 0 \leq b \leq n-1$. Nechť $p_i(x) \in \mathbf{Z}[x]$, $\deg(p_i) \leq h$, je koeficient α^b v $T_i(\alpha, x)$. Koeficient x^a v $S_b(x)$ je roven koeficientu x^a v polynomu

$$\sum_{i=0}^{n-1} p_i(x) R_i(x) \ . \tag{24}$$

Homogení lineární soustava $S_2(x) \equiv 0, \ldots, S_{n-1}(x) \equiv 0$ pro neznámé koeficienty polynomů $R_i(x)$ má tedy celočíselné koeficienty, které v absolutní hodnotě nepřesahují

$$\binom{h}{\lfloor h/2 \rfloor} (nk)^h < c_1^h \ ,$$

kde c_1 je konstanta závislá jen na α.

Z (23) a definice M a N plyne, že

$$\frac{M}{N-M} = \frac{(n-2)(h+m+1)}{2(m+1)-(n-2)h} \leq \frac{(n-2)(h+m+1)}{(n-2)h\delta} \leq \frac{n}{\delta} \ .$$

Siegelovo lemma tedy poskytne $R_i(x) \in \mathbf{Z}[x]$ s vahou nepřesahující

$$\Big(n(m+1)c_1^h\Big)^{n/\delta} \ .$$

Polynomy $S_i(x) \in \mathbf{Z}[x]$ pak podle (24) mají váhu nejvýše

$$n \cdot (h+1) \cdot c_1^h \cdot \Big(n(m+1)c_1^h\Big)^{n/\delta} < c_2^h \ ,$$

kde konstanta c_2 závisí jen na α a δ. Protože $P = S_0$ a $Q = -S_1$, je odhad (ii) dokázán. $\diamondsuit$

Lemma 46. *Polynomy $P(x)$ a $Q(x)$ buďte jako výše. Potom polynom $W(x) = P(x)Q'(x) - P'(x)Q(x)$ není identicky nulový. Speciálně, $P(x)$ i $Q(x)$ jsou nenulové.*

DůKAZ. Jak víme, jeden z obou polynomů je nenulový, nechť to je třeba P. Kdyby W byl nulový, byla by nulová i racionální funkce $(Q/P)'$ a Q/P by byla konstanta $r \in \mathbf{Q}$. Levá strana (iii) předchozího lemmatu by se rovnala $P \cdot (1 - r\alpha)$. Číslo α by bylo alespoň h-násobným kořenem P. Pak by ale P musel být dělitelný h-tou mocninou minimálního polynomu α a měl by stupeň alespoň nh. To ale není možné, podle (i) má P stupeň nejvýše $h+m \leq h(n-1)$. $\diamondsuit$

Lemma 47. *Polynomy $P(x), Q(x)$ a $W(x)$ buďte jako výše. Jak víme, $W(x)$ je nenulový. Nechť $p/q \in \mathbf{Q}$ je libovolný zlomek. Číslo $k \in \mathbf{N}_0$ buď násobnost p/q jako kořene $W(x)$. Potom (i) $q^k < c_3^h$ a (ii) existují čísla $i, j \in \mathbf{N}_0$, $0 \leq i < j \leq k+1$, taková, že pro derivace $P(x)$ a $Q(x)$ platí*

$$P^{(i)}(p/q)Q^{(j)}(p/q) \neq P^{(j)}(p/q)Q^{(i)}(p/q) \ .$$

DůKAZ. Podle lemmatu 44 $(qx-p)^k$ dělí $W(x)$ v $\mathbf{Z}[x]$. Z (i) a (ii) lemmatu 45 a definice polynomu W vyplývá, že $v(W) < c_3^h$, kde c_3 závisí jen na α a δ. Tedy i $q^k < c_3^h$.

Pro důkaz části (ii) zderivujme k krát $W(x)$. Podle Leibnizovy formule pro derivaci součinu dostaneme

$$W^{(k)}(x) = \sum_{0 \leq i < j \leq k+1} P^{(i)}(x)Q^{(j)}(x) - P^{(j)}(x)Q^{(i)}(x) \ .$$

Protože $W^{(k)}(p/q) \neq 0$, je některý ze sčítanců v p/q nenulový a část (ii) je dokázána. $\diamondsuit$

DůKAZ VĚTY 42. Nechť $p/q \in \mathbf{Q}$ a $r/s \in \mathbf{Q}$ jsou dvě řešení nerovnosti (21), přičemž $q < s$. Uvidíme, že pro dostatečně velké pevné q a $s \to \infty$ (což lze zaručit, je-li řešení nekonečně mnoho) dostaneme spor. Díky záměně α číslem $\|\alpha\|$ můžeme předpokládat, že $|\alpha| < 1/2$ a $|p/q|, |r/s| \leq 1$.

Polynomy $P(x), Q(x)$ a $W(x)$ buďte jako výše. Nechť $k \in \mathbf{N}_0$ je násobnost p/q jako kořene $W(x)$. Uvažme čísla i a j z (ii) posledního lemmatu. Alespoň pro jedno z nich, označme ho j, platí

$$sP^{(j)}(p/q) - rQ^{(j)}(p/q) \neq 0 \; . \tag{25}$$

Víme, že $0 \leq j \leq k+1 \leq 2(m+h) < 2nh$. (Protože j nepřesahuje stupně P a Q, platí dokonce $j \leq m+h$.) Položíme

$$u = \frac{P^{(j)}(p/q) \cdot q^{m+h-j}}{j!} \quad \text{a} \quad v = \frac{Q^{(j)}(p/q) \cdot q^{m+h-j}}{j!} \; .$$

Patrně $u, v \in \mathbf{Z}$. Rovnost (iii) lemmatu 45 nám říká,že

$$P(x) - \alpha Q(x) = (x-\alpha)^h R(\alpha, x) \; ,$$

kde $R(\alpha, x) \in \mathbf{Z}[\alpha, x]$ má váhu nejvýše c_2^h. Po j-násobném derivování podle x a vydělení $j!$ dostaneme

$$\frac{P^{(j)}(x)}{j!} - \frac{\alpha Q^{(j)}(x)}{j!} = (x-\alpha)^{h-j} R^*(\alpha, x) \; ,$$

kde $R^*(\alpha, x) \in \mathbf{Z}[\alpha, x]$. Po provedení úpravy vidíme, že

$$v(R^*) < j^2 \cdot \binom{2hn}{hn}^3 \cdot v(R) < c_4^h \; .$$

Dosadíme $x = p/q$ a vynásobíme q^{m+h-j}. Protože ($|\alpha|, |p/q| \leq 1$)

$$|R^*(\alpha, p/q)| < v(R^*) \cdot (m+1)n < c_5^h \; ,$$

dostaneme odhad

$$|u - \alpha v| < c_5^h q^{m+h-j} \left| \alpha - \frac{p}{q} \right|^{h-j} \; . \tag{26}$$

Z definice v plyne, že

$$\begin{aligned} |v| &< q^{m+h-j} \cdot v(Q) \cdot (m+h+1) \cdot \binom{h+m}{j} \\ &< q^{m+h-j} c_6^h \; . \end{aligned} \tag{27}$$

Z (25) plyne, že $us - vr \neq 0$. Avšak $us - vr \in \mathbf{Z}$. Po rozepsání $us - vr = us - v\alpha s + v\alpha s - vr$ nám nerovnosti (21) (zlomky p/q a r/s splňují Thueho nerovnost), (26) a (27), označíme-li exponent $n/2 + 1 + \varepsilon$ v (21) jako λ, dají

$$\begin{aligned} 1 &\leq |us - vr| \leq s \cdot |u - \alpha v| + |v| \cdot s \cdot |\alpha - r/s| \\ &< c_7^h\left(sq^{m+h-j-\lambda(h-j)} + q^{m+h-j}s^{1-\lambda}\right) . \end{aligned}$$

Vzhledem k $q^{-j} \leq 1$ a $q^{j(\lambda-1)} \leq q^{k(\lambda-1)}q^{\lambda-1} < c_8^h q^{\lambda-1}$ (používáme odhad (i) posledního lemmatu) máme

$$\begin{aligned} 1 &< c_9^h\left(sq^{m+h-\lambda h+\lambda-1} + q^{m+h}s^{1-\lambda}\right) \\ &= c_9^h\left(sq^{m-(\lambda-1)(h-1)} + q^{m+h}s^{1-\lambda}\right) . \end{aligned} \tag{28}$$

Nyní zvolíme parametry h a δ v závislosti na $n, \varepsilon, p/q$ a r/s:

$$h = \lfloor \log s / \log q \rfloor + 2 \quad \text{a} \quad \delta = \frac{\varepsilon}{n-2} .$$

Takže c_9 závisí jen na α a ε a

$$c_9^h \leq c_9^2 \cdot s^{\log c_9 / \log q} . \tag{29}$$

Podíváme se na exponenty v nerovnosti (28). Číslo $m - (\lambda - 1)(h - 1)$ je nejvýše

$$\begin{aligned} &\left(\frac{n}{2} - 1\right)(1+\delta)\left(2 + \frac{\log s}{\log q}\right) - \left(\frac{n}{2} + \varepsilon\right)\frac{\log s}{\log q} \\ = &\left(\delta\left(\frac{n}{2} - 1\right) - \varepsilon - 1\right)\frac{\log s}{\log q} + (n-2)(1+\delta) . \end{aligned}$$

Takže

$$sq^{m-(\lambda-1)(h-1)} < s^{\delta(n/2-1)-\varepsilon}q^{(n-2)(1+\delta)} < s^{-\varepsilon/2}q^{2n} . \tag{30}$$

Číslo $m + h$ je nejvýše

$$\begin{aligned} \tfrac{1}{2}(n-2)(1+\delta)h + h &= \left(\left(\frac{n}{2} - 1\right) + \left(\frac{n}{2} - 1\right)\delta + 1\right)h \\ &\leq \left(\delta\left(\frac{n}{2} - 1\right) + \frac{n}{2}\right)\left(\frac{\log s}{\log q} + 2\right) . \end{aligned}$$

Protože $1-\lambda = -\frac{n}{2} - \varepsilon$, máme

$$q^{m+h} s^{1-\lambda} < s^{\delta(n/2-1)-\varepsilon} q^{\delta(n-2)+n} < s^{-\varepsilon/2} q^{2n} . \tag{31}$$

Z (28), (29), (30) a (31) dostáváme odhad

$$1 < 2c_9^2 \cdot s^{\log c_9/\log q - \varepsilon/2} \cdot q^{2n} . \tag{32}$$

Předpokládejme, že řešení Thueho nerovnosti (21) je nekonečně mnoho. Nejprve z nich vybereme řešení p/q takové, že $q > c_9^{4/\varepsilon}$, čímž s získá v (32) záporný exponent $< -\varepsilon/4$. Pak vybereme druhé řešení r/s takové, že $s > (2c_9^2 \cdot q^{2n})^{4/\varepsilon}$. Tím se pravá strana nerovnosti (32) stala menší než 1 a získali jsme kýžený spor. Proto má nerovnost (21) pouze konečně mnoho řešení.

Závěrečný argument důkazu Thueho věty — volba s závisí na volbě q — odkrývá jeho principiální neefektivnost. Pro dané α a ε je dokázána pouze konečnost počtu řešení nerovnosti (21). Ani v principu nelze z důkazu získat konkrétní horní odhad pro velikost jmenovatelů řešení.

2.8 Poznámky

2.1 Dirichletova věta a Fareyovy zlomky. Literatura: Hardy a Wright [16] a Schmidt [34]. Holubníkový princip použitý v důkazu Dirichletovy věty se často nazývá Dirichletův. Důkaz věty 20 pochází od Hermita. Tato věta byla známa již před Eulerem, například Fermatovi, ale poprvé ji dokázal Euler. S jeho původním důkazem se lze seznámit v Edwardsově knize [11]. Článek [8] se zabývá historií Fareyových zlomků. Podrobné informace o zpřesněních Hurwitzovy věty (úlohy 5 a 6) přinášejí Schmidt [34] a Cassels [9].

2.2 Řetězové zlomky. Literatura: Hardy a Wright [16] a Schmidt [34]. Prvních 50 členů řetězového rozvoje algebraické iracionality $\sqrt[3]{2}$ je

$$\begin{aligned}\sqrt[3]{2} \;&=\; //1,3,1,5,1,1,4,1,1,8,1,14,1,10,2,1,4,12,2,3,2,1,3,4,1,1,2,14,\\ &\quad 3,12,1,15,3,1,4,534,1,1,5,1,1,121,1,2,2,4,10,3,2,2,\ldots// .\end{aligned}$$

Delší výlet do řetězového rozvoje čísla $\sqrt[3]{2}$ za pomoci programu MAPLE prozrazuje, že z prvních 1000 členů je jich větších než 100 celkem dvanáct:

$$a_{35} = 534, a_{41} = 121, a_{91} = 186, a_{114} = 372, a_{375} = 186, a_{420} = 220,$$

$$a_{510} = 255, a_{571} = 7451, a_{586} = 113, a_{617} = 151, a_{619} = 4941, a_{936} = 108.$$

Jsou členy rozvoje omezené nebo neomezené? Na co si vsadíte?

Řetězovými zlomky se zabývá Perronova monografie [30]. Dají se do nich rozvíjet nejen čísla, ale i funkce, jak jsme viděli v 2.3, a mají řadu zajímavých kombinatorických aspektů: viz článek [13] a kniha Gouldena a Jacksona [15]. Jako ukázku těchto kombinatorických souvislostí uvádíme úlohu 7. Řetězovými zlomky se dá dokázat i Hurwitzova věta, viz [34].

2.3 Řetězový rozvoj čísla e. Literatura: Lang [19]. Narozdíl od e se řetězový rozvoj čísla π neřídí žádným známým jednoduchým pravidlem. Uvádíme prvních 50 členů:

$$\begin{aligned}\pi \;=\; & //3,7,15,1,292,1,1,1,2,1,3,1,14,2,1,1,2,2,2,2,1,84,2,1,1,15,\\ & \quad 3,13,1,4,2,6,6,99,1,2,2,6,3,5,1,1,6,8,1,7,1,2,3,7,\ldots// \,.\end{aligned}$$

Jsou však známa hezká vyjádření pomocí zobecněných řetězových zlomků s obecnými čitateli, například

$$\frac{4}{\pi}=1+\cfrac{1^2}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{\vdots}}}}\quad\text{a}\quad\frac{\pi}{4}=\cfrac{1}{1+\cfrac{1^2}{3+\cfrac{2^2}{5+\cfrac{3^2}{\vdots}}}}\,.$$

Oba výsledky jsou klasické, první byl známý již v 17. století. Následující Langeho vyjádření [20] je prý nové:

$$\pi=3+\cfrac{1^2}{6+\cfrac{3^2}{6+\cfrac{5^2}{6+\cfrac{7^2}{\vdots}}}}\,.$$

Funkce $F(c,x)$, která sehrála klíčovou roli v odvození řetězového rozvoje e, je zadána tzv. *hypergeometrickou řadou*. Řada $\sum_n a_n$ je hypergeometrická, pokud podíl a_{n+1}/a_n je racionální funkce v n (podíl dvou polynomů v n). Obvykle se hypergeometrické řady značí takto:

$${}_mF_n\left[\begin{array}{cccc|c} a_1 & a_2 & \ldots & a_m & \\ b_1 & b_2 & \ldots & b_n & \end{array} x\right]=\sum_{k\ge 0}\frac{(a_1)_k(a_2)_k\cdots(a_m)_k}{(b_1)_k(b_2)_k\cdots(b_n)_k}\cdot\frac{x^k}{k!}\,,$$

kde $(a)_k = a(a+1)\cdots(a+k-1)$ pro $k \in \mathbf{N}$ a $(a)_0 = 1$. Naše $F(c,x)$ je tedy ${}_0F_1$ s jediným parametrem c.

Hypergeometrické řady splňují zajímavé identity. Třeba Gaussovu ${}_2F_1$ identitu

$${}_2F_1\left[\begin{array}{cc|c} a & b & \\ c & & \end{array} 1\right] = \frac{(c-a-b-1)!(c-1)!}{(c-a-1)!(c-b-1)!}\,.$$

Zde $a,b,c \in \mathbf{C}$ a musí platit, že $b \le 0$ je celé číslo nebo $\mathrm{Re}(c-a-b) > 0$. Pro $x \in \mathbf{C}$ chápeme $x!$ jako $\Gamma(x+1)$, kde $\Gamma(x)$ je Eulerova gamma funkce.

Nebo Dixonovu ${}_3F_2$ identitu

$${}_3F_2\left[\begin{array}{ccc|c} a & b & c & \\ d & e & & \end{array} 1\right] = \frac{(a/2)!(a-b)!(a-c)!(a/2-b-c)!}{a!(a/2-b)!(a/2-c)!(a-b-c)!}\,,$$

kde $d = a-b+1$, $e = c-b+1$ a $\mathrm{Re}(1+a/2-b-c) > 0$. Její úpravou se dostane Dixonova binomická identita

$$\sum_k (-1)^k \binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!b!c!}\,.$$

Tyto a mnohé jiné identity se dnes umějí dokázat čistě mechanickým postupem, který lze naprogramovat. Nová metoda počítačových důkazů binomických a jiných identit, kterou předložili Wilf a Zeilberger v článku [38], vrhla na tuto nepřehlednou oblast kombinatoriky jasné světlo a učinila rázem práci starých mistrů identit v mnoha ohledech zastaralou. Poučení lze nalézt ve Wilfově textu [37] a knize Petkovšeka, Wilfa a Zeilbergera [31].

2.4 Iracionalita čísla $\zeta(3)$. Literatura: Hlawka, Schoißengaier a Taschner [18]. Apéry publikoval svůj důkaz v [1]. Viz též [32] nebo [23]. Námi uvedený důkaz náleží Beukersovi [6].

Euler kromě $\zeta(2)$ nalezl i další hodnoty $\zeta(s)$ v sudých číslech:

$$\zeta(4) = \tfrac{\pi^4}{90},\ \zeta(6) = \tfrac{\pi^6}{945},\ \zeta(8) = \tfrac{\pi^8}{9450},\ \zeta(10) = \tfrac{\pi^{10}}{93555},\ \zeta(12) = \tfrac{691\pi^{12}}{638512875},\ldots$$

Nalezl i obecný vzorec pro $\zeta(2k)$ (úloha 12). Apéryho věta je jediný známý výsledek o aritmetickém statutu čísel $\zeta(2k+1)$, která jsou jinak obestřena tajemstvím. O Eulerových pracích o funkci $\zeta(s)$ a jeho marném úsilí najít formuli pro $\zeta(2k+1)$ píše Ayoub [2].

2.5 Transcendence čísel e a π. Literatura: Hilbert [17] a LeVeque [21]. Iracionalita e plyne hned z nekonečnosti řetězového rozvoje. Známý jednoduchý důkaz založený na vyjádření $\mathrm{e} = 1/0! + 1/1! + 1/2! + \cdots$ uveřejnil

r. 1815 Fourier. Iracionalitu π dokázal Lambert v r. 1766, mezeru v jeho postupu zaplnil později Lagrange.

V sedmém z třiadvaceti problémů předložených Hilbertem v r. 1900 na kongresu matematiků v Paříži se vyžadovalo dokázat, že pokud $\alpha, \beta \in \mathbf{C}$ jsou dvě algebraická čísla, přičemž $\alpha \neq 0, 1$ a β není racionální, je číslo $\alpha^\beta = \exp(\beta \log \alpha)$ transcendentní. To opravdu dokázali a sedmý Hilbertův problém tak v roce 1934 nezávisle na sobě vyřešili Gelfond a Schneider. Tudíž je číslo e^π transcendentní (úloha 16). Zda je π^e transcendentní nebo alespoň iracionální není známo. Monografie o transcendentních číslech a diofantických aproximacích jsou Baker [3], Šidlovskij [33] a Feldman a Něstěrenko [12].

O historii čísla π se píše populárně v Beckmannovi [4]. V českém překladu chybí pár slov o autorovi této úspěšné, často vydávané, citované a překládané knihy. Petr Beckmann (1924–1993) se narodil v Praze. Do r. 1963 pracoval v Československé akademii věd. Pak byl pozván jako hostující profesor na coloradskou univerzitu v USA, kde zůstal natrvalo. Publikoval přes 50 článků o teorii pravděpodobnosti a šíření elektromagnetických vln. Od 70-tých let až do smrti publikoval protechnologicky orientovaný bulletin propagující mimo jiné výrobu energie v atomových elektrárnách. (Pokračuje stále na internetu jako „Fort Freedom“ [14].)

Řadu klasických i nejnovějších výsledků o čísle π a mnoho odkazů na literaturu přináší, a to v češtině, článek [29]. Viz též knihu Berggrena a bratří Borweinů [5].

Své knihy mají už i čísla e a $i = \sqrt{-1}$: Maor [24] a Nahin [28]. Knihy věnované zlatému řezu ϕ jsou Beutelspacher a Petri [7] a Walser [36].

2.6 Liouvilleova nerovnost. Literatura: Schmidt [34]. Jak víme, π je transcendentní číslo. Není ale Liouvilleovo. V r. 1953 Mahler (Kurt, nikoli Gustav a už vůbec ne Zdeněk) totiž dokázal [22], že $|\pi - p/q| > q^{-42}$ pro každý zlomek $p/q \in \mathbf{Q}$, kde $q \geq 2$.

Dobře známý je klasický Cantorův důkaz existence transcendentních čísel. Protože $|\mathbf{R}| > \aleph_0$ (diagonální metoda), ale $|\mathbf{C}^{\,\mathrm{alg}}| = \aleph_0$ (snadno se sestrojí bijekce mezi množinami $\mathbf{C}^{\,\mathrm{alg}}$ a $\mathbf{N}$), dostáváme, že $|\mathbf{R} \backslash \mathbf{C}^{\,\mathrm{alg}}| > \aleph_0$. (Viz úlohy 17 a 18).

2.7 Thueho věta. Literatura: Sprindžuk [35]. Prvním zesílením Liouvilleovy nerovnosti byl Thueho průlom v r. 1909. Siegel (Carl-Ludwig, nikoli Horst) v r. 1921 snížil exponent dále z $n/2+1+\varepsilon$ na (zhruba) $2\sqrt{n}+\varepsilon$. Dyson a Gelfond nezávisle na sobě v r. 1947 dosáhli dalšího zlepšení $\sqrt{2n}+\varepsilon$. V r.

1955 Roth snížil exponent až na $2+\varepsilon$: Nerovnost

$$|\alpha - p/q| < q^{-2-\varepsilon}$$

má pro každé iracionální algebraické číslo $\alpha \in \mathbf{R}$ a $\varepsilon > 0$ jen konečně mnoho řešení $p/q \in \mathbf{Q}$.

> And, only recently, the proof of a conjecture on approximations to algebraic numbers, long sought for by many of the world's most eminent mathematicians, was found by one whose Cambridge examination record was not so briliant that such an outstanding performance could have been expected from him.

napsal o tom Mordell [27]. V r. 1958 byla Rothovi za tento hluboký výsledek udělena „Nobelova cena za matematiku", Fieldsova medaile. Důkaz Rothovy věty lze nalézt ve Schmidtově knize [34] nebo v Casselsovi [9].

Fieldsovy medaile se udělují každé čtyři roky na Mezinárodním kongresu matematiků počínajíc rokem 1936. O historii ceny a jejích laureátech do r. 1994 pojednává Monastyrskij [26].

Jiný Rothův úspěch, který přispěl k jeho vyznamenání, byl tento významný výsledek z aditivní teorie čísel: Pro jakkoli malé $\varepsilon > 0$ se vždy najde $n_0 = n_0(\varepsilon) \in \mathbf{N}$ takové, že každá podmnožina množiny $\{1, 2, \ldots, n\}$, kde $n > n_0$, s alespoň εn prvky obsahuje aritmetickou posloupnost délky 3. Za zobecnění Rothovy analytické metody na aritmetické posloupnosti obecné pevné délky (a za další výsledky) byl vyznamenán Fieldsovou medilí v r. 1998 Gowers.

Zajímavou postavou historie Thueho a Rothovy věty je Freeman Dyson (1918). Kromě ryze matematických prací (vedle zmíněného zlepšení Thueho věty publikoval například řadu prací o číselných rozkladech) se proslavil hlavně výsledky v teoretické fyzice. V r. 1949 dokázal vzájemnou ekvivalenci tří různých teorií kvantové elektrodynamiky (QED): Feynmanovy, Schwingerovy a Tomonagovy (tři nositelé Nobelovy ceny za fyziku za rok 1965). Podrobnosti a odkazy lze najít například v Mehrově knize [25]. Viz též Dysonovy spisy [10].

2.9 Úlohy

1. (**2**) *Harmonické číslo* je zlomek

$$H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\ .$$

Dokažte, že pro žádné $n > 1$ není H_n přirozené číslo.

2. (**0**) Ukažte, že část 2 věty 19 pro racionální α neplatí.

3. (**2**) Dokažte, že pro každé iracionální číslo $\alpha \in \mathbf{R}$ je posloupnost zlomkových částí $(\{n\alpha\} : \ n = 1, 2, \ldots)$ hustá v intervalu $[0, 1]$. (Pro každé $x \in [0, 1]$ a $\varepsilon > 0$ existuje $n \in \mathbf{N}$ tak, že $|x - \{n\alpha\}| < \varepsilon$.)

4. (**1**) Nechť $\alpha \in \mathbf{R}$ je iracionální. Ukažte, že alespoň jeden ze sousedních Fareyových zlomků $a/b < c/d$ řádu n, přičemž $a/b < \alpha < c/d$, splňuje nerovnost
$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2} \ .$$

5. (**1**) Dvě iracionální čísla $\alpha, \beta \in \mathbf{R}$ se nazývají *ekvivalentní*, existují-li čísla $a, b, c, d \in \mathbf{Z}$ taková, že $ad - bc = \pm 1$ a
$$\beta = \frac{a\alpha + b}{c\alpha + d} \ .$$
Dokažte, že jde opravdu o relaci ekvivalence. Dokažte dále, že α a β jsou ekvivalentní, právě když jsou jejich řetězové rozvoje až na konečně mnoho členů shodné.

6. (**3**) Nechť $\alpha \in \mathbf{R}$ je iracionální a není ekvivalentní zlatému řezu ϕ. Potom má nerovnost $q\|q\alpha\| < 1/\sqrt{8}$ nekonečně mnoho řešení $q \in \mathbf{N}$.

7. (**3**) Nechť b_n je n-té *Bellovo číslo*, které udává počet všech rozkladů množiny $\{1, 2, \ldots, n\}$ na neprázdné a disjunktní podmnožiny ($b_1 = 1, b_2 = 2, b_3 = 5, \ldots$). Dokažte identitu
$$\sum_{n=0}^{\infty} b_n x^n = \cfrac{1}{1 - x - \cfrac{x^2}{1 - 2x - \cfrac{2x^2}{1 - 3x - \cfrac{3x^2}{\vdots}}}} \ .$$

8. (**3**) Podejte rigorózní důkaz, že $\zeta(2) = \pi^2/6$.

9. (**2**) *Násobnou zeta funkci* $\zeta(a_1, a_2, \ldots, a_l)$ definujeme jako

$$\zeta(a_1, a_2, \ldots, a_l) = \sum_{n_1 < n_2 < \cdots < n_l} \frac{1}{n_1^{a_1} n_2^{a_2} \ldots n_l^{a_l}} .$$

Dokažte identitu

$$\zeta(1,2) = \zeta(3) .$$

10. (**4**) Předchozí výsledek je zvláštním případem obecné identity, kterou nyní popíšeme. K vektoru $a = (a_1, a_2, \ldots, a_n) \in \mathbf{N}^n$, kde $a_n > 1$, definujeme *duální vektor* $b = (b_1, b_2, \ldots, b_m) \in \mathbf{N}^m$ následovně. Místo a napíšeme posloupnost nul a jedniček $10^{a_1-1}10^{a_2-1}\ldots 10^{a_n-1}$, kde 0^k znamená k nul. Všimněme si, že posloupnost má délku $a_1 + a_2 + \cdots + a_n$ a končí nulou. Otočíme ji a nuly nahradíme jedničkami a naopak. Dostaneme posloupnost tvaru $10^{b_1-1}10^{b_2-1}\ldots 10^{b_m-1}$ (patrně $b_m > 1$), která určuje duální vektor b. Vektor duální k b je zjevně a. Dokažte, že pro duální vektory a a b platí identita

$$\zeta(a_1, a_2, \ldots, a_n) = \zeta(b_1, b_2, \ldots, b_m) .$$

Například, $\zeta(1,2) = \zeta(3)$ nebo $\zeta(2,3,4) = \zeta(1,1,2,1,2,2)$.

11. (**4**) Nechť $K_n = (V, E)$ je úplný graf na vrcholech $V = \{1, 2, \ldots, n\}$ (E je množina všech dvouprvkových podmnožin V) a $w : E \to \mathbf{R}$ je ohodnocení jeho hran. Kostrou K_n rozumíme každou maximální množinu $T, T \subset E$, která neobsahuje cyklus (je to strom s $n-1$ hranami). Její váha $w(T)$ se definuje jako $\sum_{e \in T} w(e)$. Minimální kostra $T_{\min}$ je kostra s nejmenší vahou.

Nechť je ohodnocení w dáno nezávislými náhodnými veličinami $X_e, e \in E$, které mají rovnoměrné rozdělení v intervalu $[0,1]$. Dokažte, že pro takové w očekávaná váha minimální kostry splňuje

$$\lim_{n \to \infty} \mathrm{E}(w(T_{\min})) = \zeta(3) .$$

12. (**4**) Dokažte, že

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{2^{2k-1}\pi^{2k}(-1)^{k-1}B_{2k}}{(2k)!} ,$$

kde $B_{2k} \in \mathbf{Q}$ jsou Bernoulliova čísla (viz úloha 22 v kapitole 1).

13. (**3**) Spočítejte, že číslo π má reprezentaci ve tvaru součtu 4 skorogeometrických řad

$$\pi = \sum_{n=0}^{\infty} \frac{1}{16^n} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right).$$

Ukažte, jak tento vzorec umožňuje spočítat k-tou číslici hexadecimálního (šestnáctkového) rozvoje π bez počítání číslic jí předcházejících.

14. (**2**) Dokažte jednoduše, že číslo e není kvadratickou iracionalitou.

15. (**1**) Ukažte, že existují kladná iracionální čísla $\alpha, \beta \in \mathbf{R}$ taková, že $\alpha^\beta \in \mathbf{Q}$.

16. (**1**) Jak plyne z Gelfond–Schneiderovy věty, že e^π je transcendentní?

17. (**1**) Připomeňte si podrobnosti Cantorova důkazu existence transcendentních čísel.

18. (**2**) Cantorův důkaz se někdy nesprávně označuje jako nekonstruktivní. Ukažte, že tomu tak není — na jeho podkladě načrtněte algoritmus (tj. počítačový program), který generuje cifry desetinného rozvoje transcendentního čísla.

19. (**2**) Nechť $\alpha \in \mathbf{R}$ je algebraické číslo stupně $n \geq 2$, $b \in \mathbf{N}$ je vůdčí koeficient polynomu $p(x) \in \mathbf{Z}[x]$ stupně n s kořenem α, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ jsou kořeny $p(x)$ a $p/q \in \mathbf{Q}$. Z horních a dolních odhadů veličiny

$$|b^n \prod_{i=1}^{n} (q\alpha_i - p)|$$

odvoďte Liouvilleovu nerovnost.

20. (**1**) Dokažte pomocí tvrzení 41, že číslo $\beta = 10^{-1!} + 10^{-2!} + 10^{-3!} + \cdots$ je transcendentní.

21. (**3**) Dokažte, že každé reálné číslo je součtem dvou Liouvilleových čísel.

Literatura

[1] R. Apéry, Interpolation de fractions continues et irracionalite de certaines constantes, *Mathematiques, Bull. Sect. Sci.,* **3** (1981), 37–53.

[2] R. Ayoub, Euler and the zeta function, *Amer. Math. Monthly,* **81** (1974), 1067–1086.

[3] A. Baker, *Transcendental Number Theory,* Cambridge University Press, Cambridge, UK 1975.

[4] P. Beckmann, *A History of π (pi),* St. Martin's Press, New York 1971. [Páté vydání v r. 1982. České vydání: P. Beckmann, Historie Čísla π, Akademia, Praha 1998.]

[5] L. Berggren, J. M. Borwein and P. B. Borwein, *π: A Source Book,* Springer, New York 1997.

[6] F. Beukers, A note on the irrationality of $\zeta(2)$ and $\zeta(3)$, *Bull. London Math. Soc.,* **11** (1979), 268–272.

[7] A. Beutelspacher und B. Petri, *Der goldene Schnitt,* Spektrum, Heidelberg 1996.

[8] M. Bruckheimer and A. Arcavi, Farey series and Pick's area theorem, *Math. Intell.,* **17** (1995), 64–67.

[9] J. W. S. Cassels, *An Introduction to Diophantine Approximation,* Cambridge University Press, Cambridge, UK 1957.

[10] F. J. Dyson, *Selected Papers of Freeman Dyson with Commentary,* AMS, Providence, RI 1996.

[11] G. Edvards, *Posledňaja Těorema Ferma,* Mir, Moskva 1980. [Původně: H. M. Edwards, Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory, Springer, New York 1977.]

[12] N. I. Feldman and Yu. V. Nesterenko, *Transcendental Numbers,* Springer, Berlin 1998. [Jde o 44. svazek řady Encyklopaedia of Mathematical Sciences, překlad z ruštiny.]

[13] P. Flajolet, Combinatorial aspects of continued fractions, *Discrete Math.,* **32** (1980), 165–181.

[14] Fort Freedom, `http://www.fortfreedom.org`

[15] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration,* John Wiley & Sons, New York 1983.

[16] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, Oxford 1945. [Tato klasická učebnice se dočkala od r. 1938 celkem 5 vydání, posledního v roce 1979.]

[17] D. Hilbert, Über die Transzendenz der Zahlen e und π, *Math. Ann.,* **43** (1893), 216–219. [Viz též: *Gesammelte Abhandlungen. Erster Band, Zahlentheorie,* Springer, Berlin 1932.]

[18] E. Hlawka, J. Schoissengaier and R. Taschner, *Geometric and Analytic Number Theory,* Springer, Berlin 1991.

[19] S. Lang, *Introduction to Diophantine Approximations,* Addison-Wesley, Reading, MA 1966.

[20] L. J. Lange, An elegant continued fraction for π, *Amer. Math. Monthly,* **106** (1999), 456–458.

[21] W. J. LeVeque, *Fundamentals of Number Theory,* Addison-Wesley, Reading, MA 1977.

[22] K. Mahler, On the approximation of π, *Nederl. Akad. Wet., Proc., Ser. A,* **56** (1953), 30–42.

[23] Yu. I. Manin and A. A. Panchiskin, *Encyclopeadia of Mathematical Sciences, Volume 49, Number Theory I,* Springer, Berlin 1995.

[24] E. Maor, *e: the Story of a Number,* Princeton University Press, Princeton, NJ 1994.

[25] J. Mehra, *The Beat of a Different Drum. The Life and Science of Richard Feynman,* Clarendon Press, Oxford 1994.

[26] M. Monastyrsky, *Modern Mathematics in the Light of the Fields Medals,* A K Peters, Wellesley, MA 1998.

[27] L. J. Mordell, *Reflections of a Mathematician,* Cambridge University Press, Cambridge, UK 1959.

[28] P. I. Nahin, *An Imaginary Tale: the Story of* $\sqrt{-1}$, Princeton University Press, Princeton, NJ 1998.

[29] I. Netuka a J. Veselý, Nedávné poznatky o čísle π, *Pokroky matematiky fyziky a astronomie,* **43** (1998), 217–236.

[30] O. Perron, *Die Lehre von den Kettenbrüchen, Band I und II,* B. G. Teubner Verlagsgesellschaft, Stuttgart 1954 (Band I) und 1957 (Band II). [Třetí vydání. Reprint v Chelsea, New York 1950.]

[31] M. Petkovšek, H. S. Wilf and D. Zeilberger, $A = B$, A K Peters, Wellesley, MA 1996.

[32] A. van der Poorten, A proof that Euler missed. Apèry's proof of the irrationality od $\zeta(3)$. An informal report., *Math. Intell.,* **1** (1979), 195–203.

[33] A. B. Shidlovskii, *Transcendental Numbers,* de Gruyter, Berlin 1989.

[34] V. Šmidt, *Diofantovy Približenija,* Mir, Moskva 1983. [Původně: W. M. Schmidt, Diophantine Approximation. Lecture Notes in Mathematics 785, Springer, Berlin 1980.]

[35] V. G. Sprindžuk, *Klassičeskije Diofantovy Uravněnija ot Dvuch Něizvěstnych,* Nauka, Moskva 1981. [Anglické vydání: V. G. Sprindzhuk, Classical Diophantine Equations. Lecture Notes in Mathematics 1559, Springer, Berlin 1993.]

[36] H. Walser, *Der goldene Schnitt,* B. G. Teubner, Stuttgart 1996.

[37] H. S. Wilf, *Identities and Their Computer Proofs*, zápisy z přednášek 1993. [Dostupné pomocí „anonymous ftp“ jako soubor `pub/wilf/lecnotes.ps` na adrese `ftp.cis.upenn.edu`.]

[38] H. S. Wilf and D. Zeilberger, Rational functions certify combinatorial identities, *Journal Amer. Math. Soc.,* **1** (1990), 147–158.