Pellova rovnice a kvadratické okruhy

Matěj Doležálek

Abstrakt. Příspěvek se zabývá slavnou Pellovou rovnicí a souvisejícími (reálnými) kvadratickými okruhy. Ukážeme si důkaz existence jejích netriviálních řešeních vycházející z tzv. diofantických aproximací, popíšeme grupovou strukturu jednotek v reálném kvadratickém okruhu a projdeme některé zajímavé úlohy a aplikace.

Pod přívlastkem „Pellova“ je známa diofantická rovnice[1]

$$x^2 - dy^2 = 1,$$

kde d je přirozené číslo, které není čtvercem celého čísla. V teorii čísel si vysloužila výjimečné postavení, neboť se za jejím jednoduchým zadáním skrývá velmi zajímavá struktura a spousta souvislostí s mnoha zajímavými oblastmi matematiky.

Okamžitě jsou vidět dvě řešení Pellovy rovnice: $(x, y) = (\pm 1, 0)$. Tato dvě řešení budeme nazývat triviálními a většinu času se o ně nebudeme moc zajímat. Dokážeme následující: Pellova rovnice má vždy nekonečně mnoho netriviálních řešení, z nichž všechna jsou generována[2] jediným z nich.

Kvadratické okruhy

Definice. *Kvadratickým okruhem* rozumíme množinu

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\},$$

kde $d \in \mathbb{Z}$ není čtvercem celého čísla, opatřenou operacemi sčítání a násobení obvyklým způsobem. Množina $\mathbb{Z}[\sqrt{d}]$ tedy obsahuje všechny výrazy tvaru $a + b\sqrt{d}$ pro a, b celá čísla.

Pokud $d > 0$, nazýváme $\mathbb{Z}[\sqrt{d}]$ *reálným* kvadratickým okruhem, pokud $d < 0$, nazýváme jej *komplexním* kvadratickým okruhem. Pokud v této definici všude napíšeme $\mathbb{Q}$ namísto $\mathbb{Z}$, dostaneme *kvadratické těleso* $\mathbb{Q}(\sqrt{d})$.

Obecně *komutativním okruhem* rozumíme množinu R, ve které umíme sčítat, odčítat a násobit podle všech obvyklých pravidel (a výsledky těchto operací jsou

[1] To značí, že hledáme pouze celočíselná řešení.

[2] Co přesně je tímto slovíčkem míněno, nalezneš dále v příspěvku.

opět prvky R). *Tělesem* pak rozumíme takový komutativní okruh, ve kterém navíc umíme dělit každým prvkem kromě nuly.

Cvičení. Rozmyslete si, že kvadratický okruh je komutativní okruh.

Cvičení. Co se stane, když $d = m^2$ pro nějaké $m \in \mathbb{Z}$?

Cvičení. Kdy platí $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$?

Cvičení. Rozmyslete si, že pokud pro $a_1, b_1, a_2, b_2 \in \mathbb{Q}$ platí $a_1 + b_1\sqrt{d} = a_2 + b_2\sqrt{d}$, pak už nutně $a_1 = a_2$ a zároveň $b_1 = b_2$.

V této přednášce se budeme zabývat hlavně reálnými kvadratickými okruhy, avšak intuice a motivace za uvedenou definicí je dost podobná zavedení komplexních čísel. Trápí nás kvadratická rovnice $x^2 - d = 0$, pro kterou nemáme v oboru celých (resp. racionálních) čísel řešení. No tak si ho prostě zavedeme pod jménem $\sqrt{d}$ a začneme s ním počítat. Jediné, co při tom požadujeme, je $(\sqrt{d})^2 = d$.

Definice. Pro každé číslo $\lambda = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ (resp. $\mathbb{Q}(\sqrt{d})$) definujeme jeho *sdružené číslo* jako

$$\overline{\lambda} = a - b\sqrt{d}$$

a jeho *normu* jako

$$N(\lambda) = \lambda \cdot \overline{\lambda} = a^2 - dy^2.$$

Cvičení. Rozmyslete si, že 0 je jediným prvkem $\mathbb{Q}(\sqrt{d})$ s normou 0.

Cvičení. Nechť $d \equiv 1 \pmod 4$. Rozmyslete si, že množina

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ a + b \cdot \frac{1+\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

tvoří komutativní okruh, jehož prvky mají celočíselné normy.

Sdružené číslo nám dává způsob, jak z $\lambda = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ vytáhnout jeho racionální a iracionální část – platí

$$a = \frac{\lambda + \overline{\lambda}}{2}, \qquad b = \frac{\lambda - \overline{\lambda}}{2\sqrt{d}}.$$

Stejně tak nám norma pomůže rozepsat

$$\frac{1}{\lambda} = \frac{\overline{\lambda}}{N(\lambda)} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}.$$

Cvičení. Rozmyslete si, že kvadratické těleso je těleso.

Nyní už je vidět, proč jsme si zavedli kvadratické okruhy. Pokud pojmenujeme $\omega = x + y\sqrt{d}$, můžeme Pellovu rovnici jednoduše přepsat jako[3] $N(\omega) = 1$. Kvadratické okruhy nám dávají zajímavou algebraickou strukturu „pod“ Pellovou rovnicí.

[3] Triviální řešení pak odpovídají $\omega = \pm 1$

Cvičení. Rozmyslete si, že $\overline{(\alpha \cdot \beta)} = \overline{\alpha} \cdot \overline{\beta}$.

Důsledek. *Norma je úplně multiplikativní, neboli* $N(\alpha\beta) = N(\alpha)N(\beta)$.

V kvadratickém okruhu můžeme dělat většinu věcí, které můžeme dělat v celých číslech. Teď se zaměřme na dělitelnost a modulení. Pro $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ řekneme, že α *dělí* β (píšeme $\alpha \mid \beta$), pokud existuje $\gamma \in \mathbb{Z}[\sqrt{d}]$ splňující $\beta = \alpha \cdot \gamma$. Pro nenulové α je to ekvivalentní tomu, že $\frac{\beta}{\alpha} \in \mathbb{Z}[\sqrt{d}]$. Dále

$$\alpha \equiv \beta \pmod{\lambda}$$

značí, že $\lambda \mid (\alpha - \beta)$.

Cvičení. Dokažte, že v $\mathbb{Z}[\sqrt{d}]$ existuje přesně $|N(\lambda)|$ zbytkových tříd mod λ.

Lemma. *Pokud* $N(\alpha) = N(\beta) = k \neq 0$ *a zároveň* $\alpha \equiv \beta \pmod{k}$, *pak už* $\alpha \mid \beta$.

Poznámka. (stěžejní trik) Reálné kvadratické okruhy mají následující super vlastnost: jejich prvky jsou reálná čísla. Takže ač většinu času s čísly $a + b\sqrt{d}$ zacházíme jako s dvojicemi (a, b), můžeme je kdykoliv začít porovnávat či řadit jako reálná čísla. Na rozdíl od komplexních kvadratických okruhů se také $N(\lambda)$ nijak přímočaře neodvíjí od $|\lambda|$. Máme tedy dvě různé „velikosti“ čísla $\lambda \in \mathbb{Z}[\sqrt{d}]$: jednak jeho absolutní hodnotu $|\lambda|$ jakožto reálného čísla, ale taky jeho normu $N(\lambda)$, a tyto dvě „velikosti“ dávají dvě zcela odlišné informace.

To hlavní

Postupně ukážeme, že dokud $d \in \mathbb{N}$ není čtverec celého čísla, tak Pellova rovnice má netriviální řešení. Po cestě se bude hodit Dirichletův princip.

Věta. (Dirichletova o diofantických aproximacích) *Nechť je* α *reálné číslo a* t *přirozené číslo. Potom existují* $p \in \mathbb{Z}$, $q \in \{1, \ldots, t\}$ *taková, že* $|q\alpha - p| < \frac{1}{t}$.

Cvičení. Rozmyslete si, že pro nečtvercové $d \in \mathbb{N}$ je množina $\mathbb{Z}[\sqrt{d}]$ hustá v $\mathbb{R}$, tedy že mezi každými dvěma různými reálnými čísly leží nějaký prvek $\mathbb{Z}[\sqrt{d}]$.

Lemma. *Nechť je* $\alpha \in \mathbb{R}$ *iracionální. Pak existuje nekonečně mnoho zlomků* $\frac{p}{q}$ *v základním tvaru takových, že* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Lemma. *Nechť* $\alpha = \sqrt{d}$ *a nechť je* $\frac{p}{q}$ *zlomek popsaný v předchozím lemmatu. Potom* $|N(p + q\sqrt{d})| < 2\sqrt{d} + 1$.

Věta. *Pellova rovnice má netriviální řešení.*

Důkaz. Předchozí dvě lemmata nám dohromady vytváří nekonečně mnoho čísel $\lambda \in \mathbb{Z}[\sqrt{d}]$, z nichž každé má celočíselnou normu splňující $|N(\lambda)| < 2\sqrt{d} + 1$. Množina celých čísel v absolutní normě menších než $2\sqrt{d} + 1$ je ale konečná, takže musí existovat celé k takové, že existuje nekonečně mnoho $\lambda \in \mathbb{Z}[\sqrt{d}]$ splňujících $N(\lambda) = k$; toto k musí být nenulové, neboť jen 0 má normu 0. Stejně tak zbytkových tříd mod

k je v $\mathbb{Z}[\sqrt{d}]$ jen konečně mnoho (konkrétně k^2), takže alespoň jedna z nich obsahuje nekonečně mnoho prvků s normou k. Máme tak nekonečnou podmnožinu $\mathbb{Z}[\sqrt{d}]$, jejíž prvky mají všechny stejnou normu a jsou kongruentní modulo tato norma. Pro libovolná dvě taková λ_1, λ_2 pak tedy $\lambda_2 \mid \lambda_1$, neboli $\omega = \frac{\lambda_1}{\lambda_2} \in \mathbb{Z}[\sqrt{d}]$. Z multiplikativity normy ale nutně $N(\omega) = 1$. Když vezmeme čtyři různá $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, pak jsou $\frac{\lambda_2}{\lambda_1}$, $\frac{\lambda_3}{\lambda_1}$ a $\frac{\lambda_4}{\lambda_1}$ po dvou různá, takže alespoň jedno z nich není ± 1 a představuje tak netriviální řešení Pellovy rovnice. □

S pomocí stěžejního triku svedeme dokonce dokázat, že z jediného netriviálního řešení Pellovy rovnice už umíme vygenerovat všechna řešení.

Věta. (grupová struktura) *Existuje $\omega_0 \in \mathbb{Z}[\sqrt{d}]$ takové, že $\omega \in \mathbb{Z}[\sqrt{d}]$ splňuje $N(\omega) = 1$ právě tehdy, pokud $\omega = \pm\omega_0^k$ pro nějaké $k \in \mathbb{Z}$. Takové ω_0 nazýváme* fundamentálním řešením *příslušné Pellovy rovnice.*

Cvičení. Rozmyslete si, že předchozí věta platí i tehdy, pokud namísto $N(\omega)$ píšeme $|N(\omega)|$.[4]

Cvičení. Nechť $d \equiv 1 \pmod 4$. Rozmyslete si, že předchozí věta i předchozí cvičení platí i tehdy, pokud namísto $\mathbb{Z}[\sqrt{d}]$ píšeme $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Základní úlohy

Úmluva. Číslo a nazvěme *čtvercem* v množině S, pokud existuje $b \in S$ splňující $a = b^2$. Není-li řečeno jinak, mluvme o čtvercích v $\mathbb{Z}$.

Příklad 1. Řešte v celých číslech $x^2 + y^2 - 1 = 4xy$.

Definice. *Trojúhelníková čísla* definujme jako $T_n = \frac{n(n+1)}{2}$.

Příklad 2. Najděte všechna n, pro která je T_n čtverec.

Příklad 3. Najděte všechny dvojice $m, n \in \mathbb{N}$ splňující $T_n - T_m = mn$.

Příklad 4. Dokažte, že pokud $3n + 1$ a $4n + 1$ jsou čtverce, pak $56 \mid n$.

Příklad 5. Definujme posloupnost *Fibonacciho čísel* vztahy $F_0 = 0$, $F_1 = 1$ a $F_{n+2} = F_{n+1} + F_n$ pro $n \geq 0$. Dokažte, že pro $x \in \mathbb{N}$ je alespoň jedno z čísel $5x^2 \pm 4$ čtverec, právě pokud je x Fibonacciho číslo.

Jiná konstanta

Občas se nám může stát, že dostaneme rovnici

$$x^2 - dy^2 = c$$

pro jiné c než 1. Těmto rovnicím se obecně říká rovnice Pellova typu a i v jejich řešení nám pomůžou reálné kvadratické okruhy. Případ $c = -1$ (často se mu říká *záporná*

[4] Samozřejmě pak můžeme dostat odlišné ω_0.

Pellova rovnice) jsme už vlastně potkali – víme, že řešení rovnice $|N(\omega)| = 1$ mají grupovou strukturu, takže pokud záporná Pellova rovnice má nějaké nejmenší řešení ω_0, můžeme všechna další vygenerovat jako $\pm\omega_0^\ell$, kde ℓ je liché celé číslo.

Příklad 6. Najděte všechna $n \in \mathbb{N}$, pro která existuje přirozené $k < n$ splňující

$$\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}.$$

Cvičení. Rozmyslete si, že pokud je ω_0 nejmenší řešení záporné Pellovy rovnice, pak už je ω_0^2 fundamentální řešení obyčejné Pellovy rovnice.

Příklad 7. Dokažte, že pokud je $\frac{x^2+1}{y^2} + 4$ čtverec, pak už je to nutně 9.

Příklad 8. Nechť je p liché prvočíslo. Ukažte, že rovnice $x^2 - py^2 = -1$ má řešení, právě pokud $p \equiv 1 \pmod 4$.

Obecně pro všechna c můžeme z jednoho řešení dostat nekonečně mnoho dalších: pokud $N(\lambda) = c$, pak i $N(\omega^n\lambda) = c$ pro libovolné n, kde ω je fundamentální řešení Pellovy rovnice. Pozor si ale musíme dát na to, že to nemusí být všechna řešení – může existovat více takovýchto „rodinek“.

Definice. Budiž ω_0 fundamentální řešení Pellovy rovnice a pojmenujme množinu[5] $U = \{\pm\omega_0^n \mid n \in \mathbb{Z}\}$. *Orbitou* nazvěme každou množinu L, která je tvaru

$$L = U\lambda = \{\omega\lambda \mid \omega \in U\}.$$

Orbitě vždy přiřkneme (společnou) normu všech jejích prvků.

Cvičení. Rozmyslete si, že různých orbit dané normy k je jen konečně mnoho (např. určitě méně než k^2).

Příklad 9. Najděte všechna řešení rovnice $x^2 - 3y^2 = 13$.

Příklad 10. Nechť je $p \equiv 3 \pmod 4$ prvočíslo. Dokažte, že právě jedna z rovnic $x^2 - py^2 = \pm 2$ má řešení.

Cvičení. (dvojky jsou fajn) Rozmyslete si, že vždy existuje nanejvýš jedna orbita normy 2 (resp. -2). Z toho pokud je ω fundamentální řešení Pellovy rovnice, pak nejmenší řešení rovnice $N(\lambda) = 2$ (resp. $N(\lambda) = -2$) splňuje $\lambda = \omega\overline{\lambda}$ (resp. $\lambda = -\omega\overline{\lambda}$), neboli $\lambda^2 = 2\omega$ (v obou případech).

Čtverce v $\mathbb{Z}[\sqrt{d}]$

Cvičení. Pokud q je racionální číslo a zároveň čtverec v $\mathbb{Q}(\sqrt{d})$, pak je v $\mathbb{Q}$ buďto čtverec, nebo d-násobek čtverce, a to podle toho, zdali je základ tohoto čtverce ryze racionální, nebo ryze iracionální.

[5] Pro fajnšmekry grupu.

Příklad 11. Dokažte, že pokud je $m = 2+2\sqrt{28n^2+1}$ celé číslo pro nějaké $n \in \mathbb{N}$, pak už je m čtvercem celého čísla.

Příklad 12. Dokažte, že pokud je n^2 rozdílem třetích mocnin dvou po sobě jdoucích přirozených čísel, pak už je $2n-1$ čtverec v $\mathbb{Z}$.

Příklad 13. Seřaďme v rostoucí posloupnost $a_0, a_1, \ldots$ všechna nezáporná čísla a_n, pro která jsou $a_n + 1$ i $3a_n + 1$ čtverce. Dokažte, že pro libovolné přirozené n je $1 + a_{n-1}a_n$ čtverec.

Prvočísla a valuace

Věta. (binomická) *V libovolném komutativním okruhu platí*

$$(x+y)^n = x^n + nx^{n-1}y + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + y^n.$$

Cvičení. Nechť $n \in \mathbb{N}$ a prvočíslo p dělí d. Potom pokud $a + b\sqrt{d} = (x + y\sqrt{d})^n$ a zároveň $p \nmid x$, pak[6] $v_p(b) = v_p(y) + v_p(n)$.

Příklad 14. Najděte všechna n taková, že $3^n - 2$ je čtverec.

Cvičení. Budiž p prvočíslo. Dokažte, že pouze pro konečně mnoho n je $p^n - 2$ čtverec.

Lemma. *Nechť je ω fundamentální řešení Pellovy rovnice. Potom má pro $|n| > 1$ iracionální složka ω^n prvočíselného dělitele, který nedělí d.*

Příklad 15. Najděte všechny dvojice nezáporných celých čísel (x, n), pro něž je splněna rovnice $3 \cdot 2^x + 4 = n^2$.

Příklad 16. Najděte všechna celočíselná řešení rovnice $5^a - 3^b = 2$.

Věta. (Størmerova) *Budiž P konečná množina prvočísel. Přirozené číslo nazvěme* hladkým, *pokud jsou všichni jeho prvočíselní dělitelé z P. Pak existuje pouze konečně mnoho párů po sobě jdoucích hladkých čísel.*

Cvičení. Dokažte, že existuje jen konečně mnoho párů hladkých čísel lišících se o 2.

[6] $v_p(n)$ zde značí *p-valuaci* přirozeného n, tedy největší nezáporné celé číslo splňující $p^{v_p(n)} \mid n$.

Návody

1. Substituce $z = x - 2y$, potom grupová struktura.

3. Důsledně uprav na čtverce. Obdržíš Pellovu rovnici s $d = 8$.

4. Vzorečky pro racionální a iracionální část dají $7 \mid n$. Z kvadratických zbytků mod 8 vymlať $8 \mid n$.

5. Nechť $\varphi = \frac{1+\sqrt{5}}{2}$. Indukcí dokaž vzoreček $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (\overline{\varphi})^n)$ a následně využij grupové struktury jednotek v $\mathbb{Z}[\varphi]$.

7. Ekvivalentně: záporná Pellova rovnice $x^2-(m^2-4)y^2 = -1$ má řešení pouze pro $m = 3$. Rozliš dva případy podle parity, vždy odhadni z malých případů explicitní konstrukci pro nějaké řešení příslušné kladné Pellovy rovnice a zkoumej, kdy může toto řešení být čtvercem v $\mathbb{Z}[\sqrt{m^2-4}]$.

8. Vezmi fundamentální řešení kladné Pellovy rovnice a použij jeho minimalitu.

9. Ujisti se, že máš všechny orbity. Pomůže stěžejní trik.

10. Vezmi fundamentální řešení Pellovy rovnice a použij jeho minimalitu.

11. Vyjádři z grupové struktury a použij předchozí cvičení.

13. Vyjádři z Pellovy rovnice pro $d = 3$. Zatni zuby a poupravuj získaný humus na $\left(\frac{\omega^{2n}+\omega^{-2n}-8}{6}\right)^2$, kde ω je fundamentální řešení.

14. Uprav v $\mathbb{Z}[\sqrt{3}]$, porovnej 3-valuace iracionálních částí a hoď na to stěžejní trik.

16. Substitucí $x = 3^b + 1$, $y = 3^{\frac{b-1}{2}}5^{\frac{a-1}{2}}$ obdržíš Pellovu rovnici s $d = 15$. Najdi spor pomocí nežádoucího prvočísla v iracionální části.

Literatura a zdroje

[1] Anh Dung „Tonda“ Le: *Pellova rovnice*, Lipová-lázně, 2016.

[2] Edward J. Barbeau: *Pell's Equation*, Springer, 2003.

[3] Dušan Djukić: *Pell's equation*, *https://pdfs.semanticscholar.org/6079/b973581e07fff9fe3c9de3003051267dd837.pdf*