Pellova rovnice

Franta Konopecký

Úvod

Co se skrývá pod tímto pojmem? Patří to vůbec do pohádky?

Jako Pellova rovnice je známa rovnice

$$x^2 - Dy^2 = 1, \tag{$\heartsuit$}$$

kde $D > 0$ je přirozené číslo, které není druhou mocninou. Řešení hledáme v celých číslech. Tato rovnice je jednou z nejdůležitějších rovnic v teorii čísel.

Zobecněním Pellovy rovnice jsou tzv. Pellovské rovnice tvaru $ax^2 \pm by^2 = c$. K řešení konkrétní Pellovské rovnice je potřeba různých metod, které zvládá např. program Mathematica verze 5.0 zadáním příkazu:

`Reduce[`$f[x,y]$` && Element[x|y, Integers]]`

kde $f[x,y]$ je levá strana zadané rovnice. Tento příspěvek se však zabývá výhradně řešením Pellovy rovnice.

Triviálními řešeními Pellovy rovnice jsou dvojice $(x,y) \in \{(1,0),(-1,0)\}$. Těmi se již dále zabývat nebudeme a automaticky s nimi nebudeme počítat.

Jak vypadají řešení

Pro pochopení, jak Pellova rovnice funguje, je podstatná následující věta. Neříká nic jiného, než, že když už jsme našli nějaké řešení (x,y) Pellovy rovnice, tak umíme pomocí něj najít dalších nekonečně mnoho různých řešení.

Věta 1. *Předpokládejme, že rovnici $x^2 - Dy^2 = 1$ vyhovuje řešení $(x,y) = (p,q)$, pro nějaká $p,q \in \mathbb{N}$. Pak jsou řešeními i všechny dvojice celých (!) čísel (x,y) tvaru*

$$x = \frac{(p+q\sqrt{D})^n + (p-q\sqrt{D})^n}{2} \tag{1}$$

$$y = \frac{(p+q\sqrt{D})^n - (p-q\sqrt{D})^n}{2\sqrt{D}}. \tag{2}$$

Vzorečky na první pohled spadlé z nebe mají jednoduchý důkaz (prostým dosazením (neroznásobovat na n-tou!)) i jednoduché odvození. Odvození (a vlastně i o maličko delší důkaz) je následující:

Důkaz: Za předpokladu, že (p,q) řeší zadanou rovnici, je $1 = p^2 - Dq^2 = (p+q\sqrt{D})(p-q\sqrt{D})$, z čehož následně plyne $1 = 1^n = ((p+q\sqrt{D})(p-q\sqrt{D}))^n = (p+q\sqrt{D})^n(p-q\sqrt{D})^n$. Dále je zřejmé, že existují pevně daná $x, y \in \mathbb{N}$, že

$$x + y\sqrt{D} = (p+q\sqrt{D})^n \tag{3}$$

$$x - y\sqrt{D} = (p-q\sqrt{D})^n \tag{4}$$

Pokud totiž roznásobíme výraz $(p + q\sqrt{D})^n$, určitě dostaneme nějaké přirozené číslo (v našem značení je to číslo x) plus y-násobek odmocniny $\sqrt{D}$. Čísla x, y pak získáme prostým vyřešením soustavy rovnic (3),(4). To, že nám vyjdou i z výše napsaných nechutných výrazů celá čísla, je dáno „požráním“ odmocnin $\sqrt{D}$ v čitateli zlomků.

Další věta říká, že množina řešení Pellovy rovnice je maximálně[3] množina dvojic $\left\{\left(\frac{(p+q\sqrt{D})^n+(p-q\sqrt{D})^n}{2}, \frac{(p+q\sqrt{D})^n-(p-q\sqrt{D})^n}{2\sqrt{D}}\right)\right\}$ pro pevně daná celá čísla (p, q) a $n = \{1, 2, 3, \dots\}$ (pokud existují řešení, tak jsou v tomto tvaru a jiná řešení už daná rovnice nemá).

Věta 2. *Mějme dvě různá celočíselná řešení (x,y) a (x',y') zadané rovnice (1). Pak existují celá čísla p, q a přirozená čísla k, l taková, že $x + y\sqrt{D} = (p + q\sqrt{D})^k$ a $x' + y'\sqrt{D} = (p + q\sqrt{D})^l$.*

Důsledek. Pro každá dvě různá řešení existuje „společný dělitel“ těchto řešení. Z existence minimálního řešení (nejmenšího dělitele všech ostatních řešení) rovnice (1) (tuto existenci si každý hravě zvládne rozmyslet) pak plyne množina řešení $\{(x + y\sqrt{D})\}$ ve tvaru $\{(p + q\sqrt{D})^n\}$.

Věta 3. *Pokud $D = d^2$ pro nějaké $d \in \mathbb{N}$, pak nemá Pellova rovnice $x^2 - y^2d^2 = 1$ celočíselné řešení.*

Věta 3 nám bude jasná, když si Pellovu rovnici upravíme do tvaru $x^2 - (yd)^2 = 1$ a otážeme se, kdy může být rozdíl dvou čtverců[4] roven jedné.

Věta 4. *Pro každé $D > 0$, $D \neq d^2$, má rovnice (1) alespoň jedno celočíselné řešení.*

Důsledek. (Vět 2 a 4) Každá Pellova rovnice[5] má množinu řešení (x, y) přesně ve tvaru $\left\{\left(\frac{(p+q\sqrt{D})^n+(p-q\sqrt{D})^n}{2}, \frac{(p+q\sqrt{D})^n-(p-q\sqrt{D})^n}{2\sqrt{D}}\right)\right\}$ pro pevně daná čísla p, q, a $n \in \mathbb{N}$.

Zbývá ještě dát návod, jak to první, nebo alespoň jedno řešení, najít … To bude i náznak důkazu, že toto řešení existuje, a tedy i věty 4. Pro tyto účely si ujednotíme označení.

Značení 1. Řetězové zlomky (z Víťovy přednášky) budeme značit způsobem

$$[a_0, a_1, a_2, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\cdots}{\cdots + \cfrac{1}{a_n}}}} \quad \text{a} \quad [a_0, a_1, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}},$$

[3]prozatím „maximálně“, později „právě“

[4]druhých mocnin

[5]s $D \neq d^2$

kde $a_1, a_2, \dots \in \mathbb{N}$.

Značení 2. p_n, q_n jsou čísla taková, že $\mathrm{nsn}(p_n, q_n) = 1$ a $\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$.

Nyní si pomůžeme několika nedokázanými větami. Začíná špetka humusu.

Věta 5. *Každé reálné číslo r lze jednoznačně vyjádřit právě jedním způsobem ve tvaru $r = [a_0, a_1, a_2, \dots, a_n]$ nebo $r = [a_0, a_1, a_2, \dots]$. První způsob je pro čísla racionální, druhý pro iracionální.*

Věta 6. (Jediná, se kterou se obracejte na Víťu) *Každou iracionální odmocninu $\sqrt{D}$ lze zapsat ve tvaru $\sqrt{D} = [a_0, \overline{a_1, a_2, \dots, a_{k-1}, 2a_0}] = [a_0, a_1, a_2, \dots, a_{k-1}, 2a_0, a_1, a_2, \dots, a_{k-1}, 2a_0, a_1, \dots]$.*

Věta 7. *Koeficienty $a_0, a_1, \dots$ a čísla $p_0, p_1, \dots; q_0, q_1, \dots$ hledáme pomocí těchto rekurentních vztahů (P_n, Q_n jsou další pomocné posloupnosti):*

$$\begin{array}{cc}
P_0 = 0,\ P_1 = a_0, & P_n = a_{n-1}Q_{n-1} + P_{n-1} \\
Q_0 = 1,\ Q_1 = D - a_0^2, & Q_n = \frac{D-P_n^2}{Q_{n-1}} \\
a_0 = \lfloor D \rfloor, & a_n = \lfloor \frac{a_0+P_n}{Q_n} \rfloor \\
p_0 = a_0,\ p_1 = a_0a_1 + 1, & p_n = a_np_{n-1} + p_{n-2} \\
q_0 = 1,\ q_1 = a_1, & q_n = a_nq_{n-1} + q_{n-2}
\end{array}$$

A na co nám to všechno je? Odpověď není jednoduchá `;)`. Ale pomůže nám v ní jediná věta, další věta ...

Věta 8. *Pro čísla zadaná rekurencí v předchozí větě platí vztahy:*

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n+1}$$
$$p_n^2 - Dq_n^2 = (-1)^{n+1}Q_{n+1} \quad (\clubsuit)$$

Teď s nápovědou, že právě pro $n = k$ (připomínáme, že k je délka periody posloupnosti a_n u řetězových zlomků) je $Q_k = 1$, a detailním shlédnutím identity ($\clubsuit$) nám vyvstane, že jakmile najdeme periodu k, tak čísla q_{k-1}, p_{k-1} (popřípadě q_{2k-1}, p_{2k-1}) jsou nejmenším řešením zadané rovnice. Jak tato řešení používat a jestli jsou skutečně řešeními se dozvíte na přednášce (ať zbude aspoň střípek tajemna nad tímto krásným problémem).

A poslední věta je na zamyšlení, jak nám vyřešení základní Pellovy rovnice může pomoct i s dalšími obecnějšími rovnicemi.

Věta 9. *Nechť existuje nějaké celočíselné řešení rovnice $x^2 - Dy^2 = \pm c$, pak existuje těchto řešení nekonečně mnoho.*

Literatura

Kdo by se chtěl dozvědět víc, tak tady je stránka, ze které jsem převážně čerpal: `http://mathworld.wolfram.com/PellEquation.html`. Ať vám slouží.