Geometrie čísel

Vít „Vejtek“ Musil

Abstrakt. Jakkoliv se to může zdát pozoruhodné, geometrie je vskutku užitečným nástrojem v teorii čísel. I velmi obtížnou úlohu jde někdy vyřešit extrémně jednoduchým geometrickým argumentem. Jedním z nich je tzv. Minkowského věta, kterou si dokážeme a aplikujeme na některá tvrzení, jako je slavná Lagrangeova věta o čtyřech čtvercích. Na závěr dojde i na diofantické rovnice a úlohy z matematické olympiády.

Body, mřížky, rovnoběžnostěny

Pojďme rovnou k tomu hlavnímu. Minkowského věta zhruba řečeno říká, že dostatečně velký symetrický útvar rozumného tvaru nemůže míjet mřížové body. Tolik nejasností si přímo koleduje o definici.

Začněme těmi mřížovými body. Často se jeden spokojí s definicí mřížky v $\mathbb{R}^2$, totiž že to jsou ty body roviny, jejichž souřadnice jsou celočíselné. Přímočarým zobecněním získáme definici v $\mathbb{R}^n$ pro libovolné přirozené n. My však budeme ještě náročnější.

Definice. Buď $n \in \mathbb{N}$. *Mřížkou* $\Lambda = \Lambda(B)$ v $\mathbb{R}^n$ s *bází* $B = \{v_1, \dots, v_n\}$, kde v_i jsou lineárně nezávislé vektory v $\mathbb{R}^n$, nazveme množinu všech celočíselných lineárních kombinací vektorů z báze B, přesněji

$$\Lambda = \Big\{ \sum_{i=1}^{n} a_i v_i;\ a_i \in \mathbb{Z} \Big\}.$$

Základním rovnoběžnostěnem $T = T(B)$ mřížky $\Lambda(B)$ nazveme množinu

$$T = \Big\{ \sum_{i=1}^{n} a_i v_i;\ a_i \in \langle 0, 1) \Big\}.$$

Objem mřížky definujme jako objem základního rovnoběžnostěnu a označme $\mathrm{Vol}(\Lambda)$.

Naše definice je konzervativní v tom smyslu, že zvolíme-li si bázi $\mathbb{R}^2$ z vektorů $v_1 = (0, 1)$ a $v_2 = (1, 0)$, pak mřížka Λ odpovídá našemu původnímu chápaní mřížky v rovině. Základní rovnoběžník je pak „čtverec“ $\langle 0, 1) \times \langle 0, 1)$. Objem Λ je zjevně roven jedné.

Povšimněme si, že množiny $\{x+T;\, x\in\Lambda\}$ tvoří rozklad celého prostoru, tj. pro každý bod $y\in\mathbb{R}^n$ existuje právě jeden bod mřížky $x\in\Lambda$ takový, že $y\in x+T=\{x+z;\, z\in T\}$.

V uvedené definici jsme zůstali ještě něco málo dlužni – objem mřížky totiž závisí na T. Potíž je v tom, že více bází může definovat tutéž mřížku, ačkoli T vypadá různě. Příkladem budiž třeba báze $\{(2,3),(3,4)\}$. Snadno si rozmyslíme, že generuje onu „základní“ mřížku v $\mathbb{R}^2$ stejně jako báze, kterou jsme volili výše. Pomocí základů lineární algebry však lze triviálně odvodit fakt, že pokud dvě báze generují tutéž mřížku, odpovídající základní rovnoběžnostěny mají stejný objem.

Připomeňme si zbývající potřebné pojmy.

Definice. Množina $M\subseteq\mathbb{R}^n$ se zove *konvexní*, pokud s každými dvěma body obsahuje úsečku tyto body spojující, tj. $x,y\in M$ implikuje $\lambda x+(1-\lambda)y\in M$ pro každé $\lambda\in\langle 0,1\rangle$. M je *středově symetrická*, pokud $x\in M$ implikuje $-x\in M$, a je *omezená*, pokud leží v nějaké kouli.

Minkowského věta

Nyní již můžeme poctivě vyslovit Minkowského větu.

Věta. (Minkowski, 1891) *Buďte $M\subseteq\mathbb{R}^n$ konvexní, omezená a středově symetrická množina a $\Lambda\subseteq\mathbb{R}^n$ mřížka splňující*

$$2^n\,\mathrm{Vol}(\Lambda)<\mathrm{Vol}(M),$$

kde $\mathrm{Vol}(M)$ *je objem M. Potom B obsahuje mřížový bod různý od počátku.*

Uvědomme si, co věta speciálně říká pro rovinu a onu „základní mřížku“. Její objem je zřejmě roven jedné. Pokud tedy má M předepsané vlastnosti a objem větší než 4, pak obsahuje mřížový bod různý od počátku. Ze symetrie navíc plyne, že obsahuje mřížové body alespoň tři (včetně počátku).

Ilustrujme nyní použití Minkowského věty na jednoduchém příkladě.

Příklad. Umístěme do každého mřížového bodu prostoru vyjma počátku kouli o poloměru $r>0$ (společný pro všechny koule). Dokažte, že neexistuje přímka procházející počátkem, která neprotíná žádnou z těchto koulí.

Předpokládejme pro spor, že existuje přímka procházející počátkem, která míjí všechny koule se středem v mřížových bodech. Podél této přímky lze tedy zkonstruovat „pás“ o libovolné délce a průměru r tak, aby neprotínal žádný mřížový bod. Nyní stačí vzít pás dostatečně dlouhý na to, aby jeho objem byl větší než 2^n, kde n je dimense prostoru. Pak podle Minkowského věty tento obsahuje mřížový bod, což není možné.

Dva a čtyři čtverce

Minkowského věta se ukáže býti užitečným nástrojem k důkazu následujících dvou tvrzení. První říká, že každé prvočíslo tvaru $4k+1$ lze zapsat jako součet dvou čtverců. Lagrangeova věta pak zaručí, že vůbec každé číslo lze zapsat jako součet čtverců čtyř.

Ke každému z důkazů budeme potřebovat po jednom snadném lemmatu, které dokážeme čistě algebraickými prostředky.

Lemma. *Buď p prvočíslo tvaru $4k+1$ pro nějaké přirozené k. Potom existuje celé číslo a splňující*

$$a^2 \equiv -1 \pmod{p}.$$

Tvrzení. *Buď p prvočíslo tvaru $4k+1$ pro nějaké přirozené k. Potom rovnice*

$$p = x^2 + y^2$$

má řešení $x, y \in \mathbb{Z}$.

Lemma. *Buď p prvočíslo. Potom rovnice*

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

má řešení $x, y \in \mathbb{Z}$.

Použitím Čínské zbytkové věty a předchozího lemmatu dostáváme téměř bezprostředně důsledek. Připomeňme, že číslo se zove bezčtvercovým, pokud se v jeho prvočíselném rozkladu vyskytne každé prvočíslo v nejvýše první mocnině.

Korolár. *Rovnice $x^2 + y^2 + 1 \equiv 0 \pmod{m}$ má v celých číslech řešení pro každé bezčtvercové číslo $m \in \mathbb{N}$.*

Věta. (Lagrange, 1770) *Buď n nezáporné celé číslo. Pak rovnice*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

má řešení $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.

Pro úplnost ještě dodejme, že oba tyto výsledky mají i své čistě algebraické důkazy. Zvídavý čtenář nechť nahlédne do poznámek [1].

Diofantické rovnice

Dokázat, že nějaká diofantická rovnice nemá řešení, je poměrně klasický problém. Co když ale máme dokázat, že řešení má? Také zde nám může být pan Minkowski k ruce.

Následující úloha poskytuje návod, jak lze nalézt odpověď dokonce na celou třídu podobných problémů.

Úloha. Buďte a, b, c kladná celá čísla splňující $ac = b^2 + b + 1$. Pak rovnice

$$ax^2 - (2b+1)xy + cy^2 = 1$$

má řešení $x, y \in \mathbb{Z}$. (Polská MO)

Uvažujme ty body roviny (x, y), pro které platí $ax^2 - (2b+1)xy + cy^2 < 2$. Jednoduchými výpočty ověříme, že se jedná o vnitřek elipsy s obsahem $4\pi/\sqrt{3} > 4$. Zřejmě je tato elipsa konvexní, středově symetrická i omezená. Podle Minkowského věty tak obsahuje mřížový bod (x, y) různý od počátku. Protože $ac = b^2 + b + 1$, je jistě $ax^2 - (2b+1)xy + cy^2 > 0$ a z celočíselnosti všech konstant nutně dostáváme $ax^2 - (2b+1)xy + cy^2 = 1$. Čísla x, y jsou tedy hledaným řešením.

Je vidět, že stejný postup bude fungovat pro rovnice, které ve smyslu předchozího návodu definují konvexní omezené množiny, jež jsou symetrické kolem nějakého mřížového bodu a mají dostatečně velký objem.

Tento argument jistě zazní i v následující úloze, leč sám stačit nebude. Podstatným krokem je ještě zvolit si lišácky mřížku.

Úloha. Buď n přirozené číslo takové, že rovnice

$$x^2 + xy + y^2 = n$$

má řešení $x, y \in \mathbb{Q}$. Pak tato rovnice má také řešení $x, y \in \mathbb{Z}$. (KöMaL)

Tímto náš výklad končí. Další úlohy a zajímavé aplikace lze nalézt například v knize Problems From the Book [2], kde je problematice věnována celá kapitola *Geometry and Numbers*.

Literatura

[1] Martin Klazar, *Introduction to Number Theory*, Lecture notes
[2] Titu Andreescu, Gabriel Dospinescu, *Problems From the Book*, XYZ Press, 2008