mezinárodní
korespondenční
seminář

iksko.org

Čísla a čtverečky

Jakub Löwit

Abstrakt. Čísla a čtverečky jsou na první pohled celkem odlišné objekty. Přesto si nejsou úplně cizí, a co víc – existuje hned několik přístupů, jak je „ztotožnit“. Tím mnohdy dostáváme dobrou intuitivní představu o tom, co se vlastně děje. Jindy nám takový přístup umožní oddelegovat nějaký problém do úplně jiné části matematiky, kde se zčistajasna stává snadnějším (nebo alespoň méně těžkým).

Minkowského věta

Začneme tímto klasickým výsledkem, který je sám o sobě hezký. Sílu věty si demonstrujeme na pěkných (a dalších) příkladech.

Definice (Konvexní těleso). Množina bodů $M \in \mathbb{R}^n$ pro $n \in \mathbb{N}$ se nazývá *konvexní*, pokud s každými dvěma body obsahuje celou úsečku tyto body spojující, tj. x, $y \in M$ implikuje $\lambda x + (1-\lambda)y \in M$ pro každé $\lambda \in [0,1]$. Dále M je středově symetrická (kolem počátku), pokud $x \in M$ implikuje $-x \in M$, a je omezená, pokud leží v nějaké kouli.

Definice (Mřížka). Buď $n \in \mathbb{N}$. Mřížkou $\Lambda = \Lambda(B)$ v $\mathbb{R}^n$ s bází $B = v_1, \ldots, v_n$, kde v_i jsou lineárně nezávislé vektory, rozumíme množinu všech celočíselných lineárních kombinací vektorů z B, tedy $\Lambda = \{\sum_{i=1}^n a_i v_i \mid a_i \in \mathbb{Z}\}$. Základním rovnoběžnostěnem $T = T(\Lambda)$ mřížky Λ pak rozumíme množinu $T = \{\sum_{i=1}^n a_i v_i \mid a_i \in [0,1)\}$. Objem mřížky $\mathrm{Vol}(\Lambda)$ pak definujeme jako objem základního rovnoběžnostěnu $T(\Lambda)$.

Lemma 1. Objem $\mathrm{Vol}(\Lambda)$ mřížky Λ nezávisí na volbě báze.

Poslední lemma tedy ospravedlňuje zavedení objemu mřížky. Toto lemma ale vůbec není jen nějaký detail – samo o sobě často pomůže s řešením úlohy. Dále je dobré si uvědomit, že posunuté kopie T o celočíselné vektory tvoří rozklad celého $\mathbb{R}^n$.

Než se pustíme do práce, uvědomme si ještě jednu věc – obecná mřížka je silný nástroj, protože nám dovoluje vypustit silné věty na širší škálu problémů.

Příklad 2 (Minkovského věta o konvexním tělese). Ať Λ je mřížka v $\mathbb{R}^n$ a $M \in \mathbb{R}^n$ je konvexní, omezená a středově symetrická množina. Pokud navíc

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

potom M obsahuje mřížový bod různý od počátku.

Pojďme se podívat na použití této věty. Chceme-li ukázat, že existuje nějaký mřížový bod s požadovanými vlastnostmi, stačí nám říct, že tyto vlastnosti mají

všechny body v $\mathbb{R}^n$ v dostatečně velké konvexní, omezené a středově symetrické množině. Naši větu lze velmi často využít poměrně přímočaře – stačí pouze spočítat objem onoho vhodného tělesa v $\mathbb{R}^d$ a máme hotovo. Jindy je ale třeba myslet dopředu a zvolit si lišácky už i původní mřížku.

Příklad 3 (Německý lesík). Německý lesík obsahuje v každém mřížovém bodě kromě počátku strom se stejnou (nenulovou) tloušťkou kmene. V počátku stojí Němec a kochá se pravidelností lesa. Ukažte, že pokud je lesík dostatečně velký, Němec nevidí ven.

(starodávný folklór)

Příklad 4. Uvažte přirozená čísla a, b, c splňující rovnost $ac = b^2 + b + 1$. Ukažte, že rovnice $ax^2 - (2b+1)xy + cy^2 = 1$ má celočíselná řešení.

(Polsko)

Příklad 5. Ať n je přirozené číslo takové, že rovnice $x^2 + xy + y^2 = n$ má racionální řešení. Dokažte, že pak má už i celočíselná řešení.

(Kömal)

Příklad 6. Předpokládejte, že a, b jsou taková racionální čísla, pro která má rovnice $ax^2 + by^2 = 1$ nějaké racionální řešení. Ukažte, že pak už jich má nekonečně mnoho.

(Kurschak Competition)

Příklad 7. Ukažte, že prvočíslo $p \geq 3$ lze zapsat jako součet dvou čtverců právě tehdy, když p dává zbytek 1 modulo 4.

Příklad 8. Existuje sféra v $\mathbb{R}^3$, na které leží právě jeden bod se všemi souřadnicemi racionálními?

(Tournament of the Towns)

Příklad 9. Mějme a, b, c přirozená čísla, jež splňují $ac = b^2 + 1$. Ukažte, že rovnice $ax^2 + 2bxy + by^2 = 1$ má celočíselné řešení.

(Kömal)

Příklad 10 (Lagrangeova věta o čtyřech čtvercích). Každé přirozené číslo lze zapsat jako součet čtyř čtverců celých čísel.

Příklad 11. Pro každé $n \in \mathbb{N}$, označme $f(n)$ počet způsobů, jak rozložit n na součet celočíselných mocnin dvojky (na jejich pořadí přitom nezáleží). Dokažte existenci konstant a, b takových, že pro všechna $n \in \mathbb{N}$ platí

$$2^{\frac{n^2}{2} - n\log_2(n) - an} < f(2^n) < 2^{\frac{n^2}{2} - n\log_2(n) - bn}.$$

(vylepšené IMO 1997)

Fareyovy zlomky

Definice (Fareyovy zlomky). Fareyovými zlomky řádu n rozumíme posloupnost $\mathcal{F}_n$ všech zlomků $0 \leq \frac{p}{q} \leq 1$ v základním tvaru, kde $1 \leq q \leq n$, seřazených podle velikosti.

Příklad 12 (Farey-Cauchyova věta). Nechť $\frac{a}{b} < \frac{c}{d}$ jsou dva vedlejší Fareyovy zlomky. Potom $\frac{a}{b} - \frac{c}{d} = \frac{1}{bd}$.

Předešlý příklad tedy vlastně říká, že rozdíl vedlejších Fareyových zlomků je v jistém smyslu nemenší možný.

Příklad 13. Ať $\frac{a}{b} < \frac{e}{f} < \frac{c}{d}$ jsou sousední Fareyovy zlomky. Pak

$$e = a + c,$$
$$f = b + d.$$

Příklad 14. Ať $n \in \mathbb{N}$. Označme M množinu všech mřížových bodů ležících v trojúhelníku (včetně hranice) určeném body $[1, n]$, $[n, n]$, $[n, 1]$, které navíc mají nesoudělné souřadnice. Spočtěte $\sum_{(x,y)\in M} \frac{1}{xy}$.

Definice (Fordova kružnice). Pro každé racionálnímu číslo $\frac{p}{q}$ nazveme kružnici s průměrem $\frac{1}{q^2}$, která leží nad první souřadnicovou osou a dotýká se jí v bodě $\frac{p}{q}$ jeho Fordovou kružnicí.

Příklad 15. Ukažte, že dvě Fordovy kružnice se dotýkají právě tehdy, když jim odpovídající zlomky sousedí v posloupnosti Fareyových zlomků nějakého řádu.

Definice (Medián). Mediánem dvou zlomků $\frac{a}{b}$, $\frac{c}{d}$ rozumíme zlomek $\frac{a+c}{b+d}$.

Definice (Stern-Brocotův strom). Stern-Brocotův strom je rekurzivně sestavený nekonečný binární strom s vrcholy ohodnocenými kladnými racionálními čísly. V nultém kroku obsahuje pouze vrchol $\frac{1}{1}$. V i-tém kroku obdržíme další řádek stromu o 2^i vrcholech tak, že pod každé číslo napíšeme jeho medián s největším menším číslem ve stromě a s nejmenším větším číslem ve stromě (pokud některé z nich neexistuje, použijeme vhodný ze zlomků $\frac{0}{1}$, $\frac{1}{0}$).

Příklad 16. Ukažte, že Stern-Brocotův strom obsahuje každé kladné racionální číslo právě jednou, a to ve zkráceném tvaru.

Příklad 17. Pro racionální číslo $\frac{p}{q}$ definujme jeho jednoduchost jako $f(\frac{p}{q}) = \frac{1}{pq}$. Spočtěte součet jednoduchostí n-tého řádku Stern-Brocotova stromu.

Pickova formule

Známá Pickova formule sice na první pohled může působit překvapivě, na druhý zase triviálně. Přestože se nejedná o komplikované tvrzení, existuje hned několik způsobů, jakými nás může překvapit. Často můžeme najít celkem překvapivé souvislosti s jinými tvrzeními.

Pracujeme pouze s jednoduchými mnohoúhelníky (tedy neprotínají samy sebe).

Příklad 18 (Pickova formule). Mějme libovolný mnohoúhelník M s vrcholy v mřížových bodech mřížky Λ v rovině. Označme V počet mřížových bodů, které leží ostře uvnitř M, dále nechť H je počet mřížových bodů na hranici M. Potom je obsah M roven $\mathrm{Vol}(\Lambda) \cdot (V + \frac{H}{2} - 1)$.

Příklad 19 (Děravá verze). Mějme libovolný mnohoúhelník M s vrcholy v mřížových bodech rovinné mřížky Λ. Označme V počet mřížových bodů, které leží ostře uvnitř M, dále nechť H je počet mřížových bodů na hranici M. Nakonec ať D je rovno počtu „děr“ v M. Potom je obsah M roven $\mathrm{Vol}(\Lambda) \cdot (V + \frac{H}{2} + D - 1)$.

Příklad 20. Existuje rovnostranný trojúhelník s vrcholy ve vrcholech běžné mřížky v $\mathbb{R}^2$?

Příklad 21. Ať M je mnohoúhelník s vrcholy v mřížových bodech. Pro každý mřížový bod p mnohoúhelníku M označme $f(p)$ velikost úhlu (v radiánech), pod kterým je vidět M z p. Dále $g(p) = \frac{f(p)}{2\pi}$. Dokažte, že obsah M je roven sumě $g(p)$ přes všechny body $p \in M$.

Příklad 22. *Půlbodem* nazývejme libovolný bod o souřadnicích $(k/2, l/2)$, kde k a l jsou celá čísla. Ukažte, že každý půlbod, který leží ostře uvnitř mřížového mnohoúhelíka, lze získat jako střed úsečky spojující dva mřížové body, které samy leží neostře v tomto mnohoúhelníku.

Příklad 23. Mějme mřížový trojúhelník ABC takový, že jedinými mřížovými body na jeho hranici jsou jeho vrcholy a uvnitř něj leží právě jeden mřížový bod. Dokažte, že tento bod je těžištěm trojúhelníku ABC.

Příklad 24 (Eulerova formule). Ať G je rovinný graf s v vrcholy, e hranami a s stěnami. Potom platí $v - e + s = 2$.

Dále si můžete rozmyslet, že z Pickovy formule plyne také Farey-Cauchyova věta. To nám tedy ukazuje souvislost Pickovy formule s rozkladem roviny na základní rovnoběžnostěny. Podívejme se nyní, co se dá říct o Pickově formuli a vyšších dimenzích.

Příklad 25. Rozhodněte, zda platí nějaká obdoba Pickovy formule ve vyšších dimenzích (tedy jestli objem r-dimenzionálního mnohostěnu lze pro pevné $r > 2$ obecně vyjádřit polynomiálním vztahem, který využívá pouze počet mřížových bodů ostře uvnitř mnohostěnu a na jeho hranici).

Definice (Konvexní V-mnohostěn). Pro $r, n \in \mathbb{N}_0$, $r \leq n$ rozumíme konvexním r-dimenzinálním mnohostěnem P v $\mathbb{R}^n$ konvexní obal konečného počtu bodů v $\mathbb{R}^n$. Přitom r je nejmenší číslo takové, že v $\mathbb{R}^r$ existuje konvexní mnohostěn shodný s P.

Příklad 26 (Ehrhart's theorem). Ukažte, že pro každý r-dimenzionální mnohostěn P v $\mathbb{R}^n$ lze najít polynom stupně r takový, že pro všechna $m \in \mathbb{N}$ platí $f(m) = |\mathbb{Z}^n \cap mP|$.

Racionální aproximace

Na chvíli se od celých čísel přesuneme k číslům racionálním a podíváme se na nějaké jejich vlastnoti, které souvisí s geometrií čísel a mřížkami.

Příklad 27 (Dirichletova věta o racionálních aproximacích). Pro dané $\alpha \in \mathbb{R}$, $Q \in \mathbb{Q}$ existují čísla $p \in \mathbb{Z}$, $q \in \mathbb{N}$ taková, že

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

Příklad 28. Pro dané $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ existuje nekonečně mnoho racionálnch čísel $\frac{p}{q}$ splňujících

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

Iracionální čísla tedy jdou docela dobře aproximovat racionálními čísly s „malými“ jmenovateli. Všimněme si, že pokud budeme uvažovat čísla $\frac{p}{q}$ pouze ve zkráceném tvaru, pro racionální α má tato nerovnost pouze konečně mnoho řešení.

Příklad 29 (Hurwitz's theorem). Pro všechna $a \in \mathbb{R} \setminus \mathbb{Q}$ má nerovnost

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

nekonečně mnoho racionálních řešení $\frac{p}{q}$. Přitom $\sqrt{5}$ je největší taková konstanta (pro libovolnou větší konstantu už existují iracionání čísla, pro která má přísušná nerovnost pouze konečně mnoho řešení).

Předchozí věty nám dobře popisují obecné vlastnosti aproximování reálných čísel čísly racionálními. O konkrétních číslech nám toho ale říkají velmi málo. Z tohoto důvodu nyní bude chtít pro libovolné reálné α induktivně zadefinovat posloupnost racionálních čísel, která jej dobře aproximují. K tomu využijeme analogii ke známému Euklidovu algoritmu.

Definice (Řetězové zlomky). Pro α libovolné reálné induktivně zadefinujeme posloupnosti a_i, b_i tak, že $a_0 = \lfloor \alpha \rfloor$, $b_0 = \alpha - a_0$. Dále pro $i + 1 \geq 1$ mohou nastat dva případy. Pokud $b_i = 0$, algoritmus skončí. V opačném případě definujeme $a_{i+1} = \left\lfloor \frac{1}{b_i} \right\rfloor$, $b_{i+1} = \frac{1}{b_i} - a_{i+1}$.

Nyní konečně n-tou konvergentu $[a_0, a_1, a_2, \ldots, a_n]$ definujeme jako

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}.$$

Řetězovým zlomkem čísla α myslíme výraz

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}.$$

tedy limitu konvergent pro $n \to \infty$.

Všimněme si, že a_0 je celé, a_i pro $i \geq 1$ jsou přirozené, b_i leží v intervalu $[0, 1)$. Všechny konvergenty jsou tedy racionální čísla. Intuitivně vidíme, že se konvergenty postupně blíží k α. Jak ale něco takového může souviset s geometrií čísel? Odpovědí je Euklidův algoritmus, který má pěkné geometrické znázornění. A můžou nám nějaké obrázky pomoci s řešením takto jemných algebraických problémů? Společně s tím, co už známe – můžou!

Při obrázkové reprezentaci Euklidova algoritmu pro aproximaci nějakého reálného α se vyplatí použít mřížku s bázovými vektory $(\alpha, 1)$, $(-1, 0)$.

Příklad 30. Pro racionální číslo $\frac{p}{q}$ splývá hledání odpovídajícího řetězového zlomku s Euklidovým algoritmem pro hledání $\gcd(p, q)$. Speciálně α má konečný řetězový zlomek právě tehdy, když je racionální.

Z obrázkové reprezentace algoritmu je zřejmé, že konvergenty aproximují číslo α lépe a lépe, a to střídavě z obou stran. Nyní si vychutnejme praktičnost mřížky na příkladu, který nám ukáže, jak moc je aproximace řetězovým zlomkem dobrá.

Příklad 31. Ukažte, že pro $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\epsilon \in \mathbb{R}$ pevná má nerovnost $\left|\alpha - \frac{p}{q}\right| < \frac{\epsilon}{q^2}$ nekonečně mnoho racionálních řešení $\frac{p}{q}$ právě tehdy, když ji splňuje nekonečně mnoho různých konvergent $\frac{p_n}{q_n}$ čísla α.

Obdélníky a reciprocita

Učiňme nyní krok stranou a vychutnejme si úplně jiný aspekt korelace čísel a čtverečků – druhým mocninám se přece neříká čtverce jen tak. Dokonce už staří řekové interpretovali součiny jako obdélníky, a i v olympiádní matematice nám takový přístup může přijít k duhu. Prvočísla typicky postrádají pravidelnost a vhodná obdélníčková reformulace problému nám ji mnohdy poskytne.

Příklad 32. Nalezněte bijekci $\mathbb{N} \to \mathbb{N}^2$ danou nějakým polynomem.

(folklor)

Příklad 33. Pro reálná $a_{i,j}$ dokažte nerovnost

$$\sum_{i=1}^{n-1} \sqrt{\sum_{j=1}^{m} (a_{i,j} - a_{i+1,j})^2} \geq \sqrt{\sum_{j=1}^{m} (a_{1,j} - a_{n,j})^2}$$

a určete, kdy nastává rovnost.

(folklor)

Příklad 34. Ivan má dvě nesoudělná čísla a, b. Před sebou má Turecké vojsko. Postupně se dívá na čísla 1, 2, …, ab. Za každé číslo zaútočí na jednoho Turka. Ivan Turka zabije právě tehdy, kdy je mezi přečtenými čísly sudý počet násobků čísel a, b. Kolik Turků Ivan celkem pobil?

(ruský folklor)

Příklad 35. Uvažme mřížku $p \times p$, která je nakreslena na toru. Určete maximální počet mřížových bodů takový, že žádné tři z nich neleží na přímce.

Příklad 36. David a Honza jedou autem. Neshodli se, kdo bude řídit, a tak si zvolili nesoudělná čísla d a h. David po každých d kilometrech zahne o 90 stupňů doprava a Honza každých h kilometrů zahne o 90 stupňů doleva. Pokud by měli oba zahnout najednou, tak budou pokračovat rovně. Na začátku míří ke svému cíli. Dokažte, že se k němu dostanou nezávisle na jeho vzdálenosti od startu, právě když $d \equiv h \pmod 4$.

(MKS 36-5-8)

Příklad 37 (Frobenius Coin Problem). Máte dány mince dvou nesoudělných hodnot a, b. Najděte největší číslo, které nejde pomocí takových mincí zaplatit.

Příklad 38 (Sylvester's theorem). Právě polovina čísel $1, 2, \ldots, (a-1)\cdot(b-1)$ jde zaplatit pomocí mincí s nesoudělnými hodnotami a, b.

Definice (Kvadratický zbytek). Číslo $1 \leq a \leq p-1$ nazýváme kvadratickým zbytkem modulo p, jestliže existuje nějaké celé x splňující $x^2 \equiv a \pmod p$.

Kvadratických zbytků modulo p je přitom vždy právě $\frac{p-1}{2}$. K tomuto zjištění si stačí rozdělit nenulové zbytky modulo p na dvě poloviny (což je obecně dobrý způsb, jak se ke zbytkům chovat).

Definice (Legendreův symbol). Ať p je prvočíslo, a celé číslo. Potom definujeme Legendreův symbol jako

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{pokud } p \mid a, \\ 1, & \text{pokud } a \text{ je kvadratický zbytek modulo } p, \\ -1, & \text{pokud } a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Lemma 39 (Eulerovo kritérium). Pro prvočíslo $p \geq 3$ a a celé platí $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Eulerovo kritérium je přitom důsledkem Malé Fermatovy věty a faktu, že každý polynom stupně n má nejvýše n kořenů modulo p. Taková myšlenka rozhodně není triviální, a později se určitě ještě bude hodit. Dále si všimněme, že

Lemma 40 (Gaussovo lemma). Mějme prvčíslo $p \geq 3$ a a libovolné celé. Označme m počet čísel $a, 2a, \ldots, \frac{p-1}{2}$, jejichž zbytek modulo p je ostře větší než $\frac{p-1}{2}$. Potom $\left(\frac{a}{p}\right) = a^m$.

Gaussovo lemma plyne z faktu, že násobení zbytků modulo p nenulovým zbytkem a tyto zbytky pouze permutuje.

Lemma 41 (Zolotarevovo lemma). Pro prvočíslo $p \geq 3$ a a nesoudělné s p platí $\left(\frac{a}{p}\right) = \epsilon\,(\pi_a)$, kde π_a značí permutaci indukovanou na zbytcích modulo p násobením číslem a, ϵ značí její znaménko.

Co tedy víme? Kvadratické zbytky souvisí s rozdělením zbytků „na dvě poloviny“ a algebraicky si dobře rozumí s jejich permutováním. Co je ale pro nás důležitější – pokud uvážíme vhodnou tabulku, mají často zajímavé geometrické vlastnosti.

Příklad 42 (Kvadratická reciprocita). Pro prvočísla p, $q \geq 3$ platí vztah

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Další Minkowského věty

Udělejme si nyní krátký výlet trochu hlouběji do Minkowského teorie o geometrie čísel. Na to bude potřeba trochu vysokoškolské matiky, a od olympiádního uplatnění se tím trochu vzdálíme. Na druhou stranu si tím lépe osaháme Minkowského větu a získáme mírný nadhled. Začneme přitom tvrzeními, na které moc hluboké teorie potřeba není.

Příklad 43 (Věta o lineárních formách). Ať $A = (a_{ij})$ je $n \times n$ invertovatelná matice nad reálnými čísly. Jsou dána kladná reálná čísla c_1, c_2, …, c_n, pro která platí $\prod_{i=1}^{n} c_i > |\det(A)|$. Dokažte existenci celých čísel x_1, x_2, …, x_n, z nichž je alespoň jedno číslo nenulové a pro všechna $i \in \{1, \ldots, n\}$ platí nerovnost $\left|\sum_{j=1}^{n} a_{ij} x_j\right| < c_i$.

Příklad 44 (Součin homogenních lineárních forem). Mějme $n \times n$ invertovatelnou matici $A = (a_{ij})$ nad reálnými čísly. Potom existují celá čísla x_1, x_2, …, x_n, ne všechna nulová, splňující $\prod_{i=1}^{n} \left|\sum_{j=1}^{n} a_{ij} x_j\right| \leq \frac{n!}{n^n} \cdot |\det(A)|$.

Příklad 45. Ať $A = (a_{ij})$ je $n \times n$ symetrická matice nad racionálními čísly. Navíc pokud $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ je bod s alespoň jednou souřadnicí nenulovou, pak $\sum_{1 \leq i,j \leq n} a_{ij} x_i x_j > 0$. Dokažte existenci bodu $x = (x_1, x_2, \ldots, x_n)$, který má alespoň jednu souřadnici nenulovou a platí pro něj

$$\sum_{1 \leq i,j \leq n} a_{ij} x_i x_j < n \cdot (\det(A))^{\frac{1}{n}}.$$

Příklad 46. Pro $n \leq 4$ uvažme symetrickou matici A $n \times n$ nad celými čísly s $\det(A) = 1$. Potom existuje matice B nad celými čísly taková, že $A = B^T B$, kde B^T značí matici získanou z B osovou symetrií podle hlavní diagonály.

Zajímavostí je, že předchozí tvrzení obecně platí dokonce pro $n \leq 7$. Využít jej v olympiádním příkladu je sice trikové, ale není to nemožné, jak si hned můžete vyzkoušet.

Příklad 47. Buďte x, y, $z \in \mathbb{N}$ taková, že $xy = z^2 + 1$. Dokažte, že potom je $x = a^2 + b^2$, $y = c^2 + d^2$, $z = ac + bd$ pronějaká celá čísla a, b, c, d.

(Irán 2001)

S vysokoškolskou matematikou se (částečně) rozloučíme uvedením supersilné verze Minkowského věty, jejíž důkaz už je těžký. Obyčejná Minkowského věta totiž mluví prostě o „velkých“ věcech. Vůbec ale neklade důraz na to, „kterým směrem“ jsou velké. To následující věta bohatě vynahrazuje.

Definice (Postupná minima). Mějme konvexní, omezenou a středově symetrickou množinu M v $\mathbb{R}^d$. Jako i-té postupné minimum množiny M, které označíme μ_i, myslíme nejmenší hodnotu λ takovou, že λM obsahuje i lineárně nezávislých bodů.

Nejdříve tedy vezmeme λ tak malé, aby λM neobsahovalo žádné mřížové body kromě počátku. Nyní budeme λ postupně zvětšovat až λM bude obsahovat alespoň jeden mřížový bod na své hranici. Toto λ označíme jako μ_1 a pojmenujeme ho prvním postupným minimem. Dále pokračujeme podobně – zvětšujeme λ, dokud nenarazíme na mřížový bod lineárně nezávislý na všech předchozích, načež si zaznamenáme další minimum (někdy si můžeme zaznamenávat i několik minim současně). Proces skončí, když obsadíme všech d dimenzí (a díky podmínkám kladeným na M se tak nutně stane).

Věta 48 (Minkowského věta o postupných minimech). Ať Λ je mřížka v $\mathbb{R}^d$, M konvexní, omezená a středově symetrická množina. Dále nechť pro i od 1 do d jsou μ_i její postupná minima. Potom platí nerovnost

$$\frac{1}{n!}\prod_{i=1}^{d}\frac{2}{\mu_i} \leq \frac{\mathrm{Vol}(M)}{\det(\Lambda)} \leq \prod_{i=1}^{d}\frac{2}{\mu_i}.$$

Speciálně si rozmyslete, jak z této věty plyne původní Minkowského věta. Někdy jsou proto tyto věty označovány jako první a druhé Minkowského věta o postupných minimech.

Pro libovolnou dimenzi najděte konvexní množiny, pro které v předchozí větě nastává první, popřípadě druhá rovnost.

Náhodné lumpárny

Zbývá vypsat hromadu příkladů na volné chvíle. Jejich řazení mírně souvisí s obtížností, z velké části je ale také náhodné. Některé z uvedených příkladů jsou celkem těžké, obzvláště ty, co mají název. Část příkladů souvisí s Minkowského větou, která je pak cenným pomocníkem.

Příklad 49. Je dán konvexní pětúhelník v rovině s vrcholy v mřížových bodech. Ukažte, že vnitřní pětiúhelník pěticípé hvězdy, kterou tyto body určují, obsahuje alespoň jeden mřížový bod.

(Rusko)

Příklad 50. Dvě posloupnosti celých čísel $a_1, a_2, \ldots$ a $b_1, b_2, \ldots$ splňují pro všechna přirozená $n > 2$ vztah $(a_n - a_{n-1})(a_n - a_{n-2}) + (b_n - b_{n-1})(b_n - b_{n-2}) = 0$. Dokažte, že existuje kladné číslo k takové, že $a_k = a_{k+2016}$. (iKS 5-A5)

Příklad 51. V rovině je mnohoúhelník s obsahem alespoň n. Dokažte, že obsahuje $n+1$ mřížových bodů takových $A(x_i, y_i)$ takových, že $x_i - x_j$, $y_i - y_j$ jsou celá čísla pro libovolná $i, j \in 1, 2, ...n+1$.

(Čína TST 1998)

Příklad 52. Uvažte polynom $P(x)$ stupně n s celočíselnými koeficienty, který má n reálných kořenů x_1, x_2, …, x_n a navíc je ireducibilní nad racioálními čísly. Dokažte, že

$$\prod_{1 \le i < j \le n} |x_i - x_j| \ge \frac{n^n}{n!}.$$

Příklad 53. Rozhodněte, zda čtverec $n \times n$ může pokrýt $(n+1)^n$ celočíselných mřížových bodů.

(AMM)

Příklad 54. Nechť a, b, c, d jsou přirozená čísla taková, že existuje 2004 dvojic (x, y), $0 \le x, y \le 1$, pro které jsou čísla $ax + by$, $cx + dy$ celá. Najděte $\gcd(b, d)$, víte li, že $\gcd(a, c) = 6$.

(Bulharsko 2005)

Příklad 55 (Scott's theorem). Ostře uvnitř mnohoúhelníku M s alespoň čtyřmi vrcholy leží přesně $k > 0$ celočíselných mřížových bodů. Ukažte, že P pokrývá nejvýše $3k + 6$ mřížových bodů.

Příklad 56. Pro $n \in \mathbb{N}$ označme $g(n)$ počet způsobů, jak zaplatit $n!$ pomocí mincí v hodnotách $k!$ pro $1 \le k \le n$ (na pořadí mincí nezáleží). Dokažte, že existuje konstanta c taková, že

$$n^{\frac{n^2}{2} - cn} \cdot e^{\frac{-n^2}{4}} \le f(n) \le n^{\frac{n^2}{2} + cn} \cdot e^{\frac{-n^2}{4}}.$$

(Putnam 2007)

Příklad 57. Uvažte graf G, jehož vrcholy odpovídají bodům s racionálními souřadicemi v $\mathbb{R}^n$ pro n přirozené, přičemž dva vrcholy jsou spojeny hranou právě tehdy, když je vzdálenost odpovídajích bodů rovna 1. Najděte nejmenší n takové, že G je souvislý.

(Irán 1998)

Příklad 58. V rovině je dán kruh se středem v počátku a poloměrem R. V každém mřížovém bodě kruhu kromě počátku stojí nekonečně vysoká válcovitá žirafa s poloměrem r (mimo kruh žirafy nejsou). Přitom r je zvoleno tak, aby bylo co největší a zároveň aby při pohledu z počátku bylo vidět i něco jiného než žirafy. Dokažte nerovnost

$$\frac{1}{\sqrt{R^2 + 1}} \le r < \frac{1}{R}.$$

(AMM)

Příklad 59. Pro přirozené $n \geq 2$ uvažme čtverec $[0, n] \times [0, n]$. Uvnitř tohoto čtverce leží mnohoúhelník P s obsahem alespoň n. Dokažte, že P pokrývá alespoň jeden mřížový bod.

Příklad 60. Je dána mřížka 2004×2004. Najděte největší přirozené n takové, že lze nakreslit konvexní n-úhelník s vrcholy v mřížových bodech zadané mřížky.

(USA TST 2004)

Příklad 61. V rovině leží mnohoúhelník $A_1A_2 \ldots A_k$, jehož vrcholy leží v mřížových bodech a na jedné kružnici. Ať existuje liché přirozené číslo n, které dělí druhé mocniny délek všech stran mnohoúhelníku. Ukažte, že pak už n dělí dvojnásobek obsahu mnohoúhelníku.

(IMO 2016)

Příklad 62. Najděte všechny šestice a, b, c, x, y, z celých čísel splňující $ax^2 + by^2 + cz^2 = abc + 2xyz - 1$, $ab + bc + ca \geq x^2 + y^2 + z^2$, a, b, $c > 0$.

Příklad 63 (Davenport-Cassels). Ukažte, že každé přirozené číslo, které je součtem tří čtverců racionálních čísel, je také součet tří čtverců celý čísel.

Příklad 64 (Straus theorem). Dokažte, že v $\mathbb{R}^n$ pro n přirozené lze najít $n + 2$ bodů, jejichž vzdálenosti jsou lichá čísla, právě tehdy, když $16 \mid n + 2$.

Příklad 65 (Hensley's theorem). Dokažte, že pro všechna k, $n \in \mathbb{N}$ existuje konstanta $B(n, k)$ taková, že pro každý n-dimenzionální mnohostěn s vrcholy v mřížových bodech, který obsahuje ostře uvnitř právě k mřížových bodů, platí $\mathrm{Vol}(P) \leq B(n, k)$.

Příklad 66 (Lagarias-Ziegler's theorem). Dokažte, že pro $n, k \in \mathbb{N}$ pevná existuje pouze konečně mnoho různých n-dimenzionálních mnohostěnů s vrcholy v celočíselných mřížových bodech, které obsahují právě k mřížových bodů ostře uvnitř.

Příklad 67 (Schinzel circles). Ukažte, že pro každé přirozené n existuje kružnice v rovině, na které leží právě n mřížových bodů.

Příklad 68 (Kulikowski sphere). Ukažte, že pro každé přirozené n existuje sféra v prostoru, na které leží právě n mřížových bodů.

Příklad 69 (Browkin's theorem). Pro každý rovinný obrazec a každé přirozené číslo n existuje jemu podobný obrazec, který obsahuje právě n mřížových bodů.

Příklad 70 (Blichfeld's theorem). Nechť A je omezená oblast v rovině s obsahem $S > n$ po $n \in \mathbb{N}$. Pak existuje obrazec v rovině shodný s A, který obsahuje alespoň $n + 1$ mřížových bodů. Tvrzení platí obdobně v $\mathbb{R}^d$ pro libovolné $d \in \mathbb{N}$.

Literatura a Zdroje

[1] Gabriel Dospinescu, Titu Andreescu: Problems from the Book
[2] PraSečí přednášky od Vejtka Musila, Jardy Hančla a dalších
[3] Skripta Martina Klazara k předmětu Úvod do teorie čísel
[4] Apostol: Modular Functions and Dirichlet Series in Number Theory
[5] Goldman: Queen of Mathematics
[6] Fuchs, Tabachnikov: Mathematical Omnibus
[7] Wolfram Math World
[8] Mathlinks
[9] Cut the Knot