Mřížky a geometrie čísel

Matěj Doležálek

Abstrakt. Teorie čísel a geometrie. Že spolu pramálo souvisí? Omyl! Prozkoumáme geometrické vlastnosti mřížových bodů a ukážeme, jak s jejich pomocí rozlousknout některé oříšky z teorie čísel. Cesta nás provede mlhavým trojmezím geometrie, teorie čísel a kombinatoriky s občasnou odbočkou do vysokoškolské algebry.

Na začátek pár poznatků, které se budou hodit v celé přednášce.

Definice. (kanonická mřížka) Bod (a, b) v rovině nazveme *mřížovým*, pokud jsou obě jeho souřadnice a, b celá čísla. Množinu všech mřížových bodů budeme nazývat *kanonickou mřížkou*.

Pozorování. (středový trik) *Pokud úsečka spojuje dva mřížové body, jejichž souřadnice mají stejné parity, pak je střed této úsečky opět mřížový bod.*

Cvičení. Mějme úsečku spojující mřížové body (a_1, b_1), (a_2, b_2). Pak na této úsečce kromě krajních bodů leží ještě dalších $\mathrm{NSD}(a_2 - a_1, b_2 - b_1) - 1$ mřížových bodů.

Pickův vzorec

Všichni jistě rádi počítáme obsahy. Nejsnáze se to dělá u jednoduchých tvarů, úplně nejlépe u těch pravidelných. Zde si však ukážeme, že výpočet je celkem snadný i u divokých komplikovaných mnohoúhelníků, dokud jsou jejich vrcholy mřížové body.

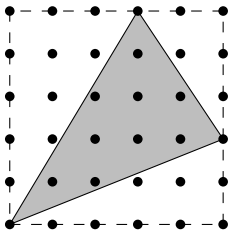
Úmluva. Není-li řečeno jinak, uvažujeme pouze mnohoúhelníky, které samy sebe neprotínají a nemají díry.

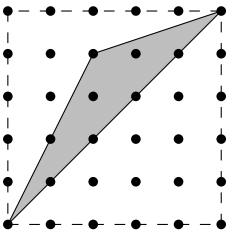
Definice. Mnohoúhelník zvěme *mřížovým*, je-li každý jeho vrchol mřížový bod.

Věta. (Pick) *Mřížový mnohoúhelník s i mřížovými body ve svém vnitřku a b mřížovými body na svém obvodu má obsah $i + \frac{b}{2} - 1$.*

Osnova důkazu. Rozmyslíme v několika krocích:

(1) Mnohoúhelníky, pro něž věta platí, můžeme „slepovat“ k sobě a věta bude stále platit. Stejně tak můžeme mnohoúhelníky, kde věta platí, „odřezávat“.
(2) Věta platí pro obdélníky a (hezky orientované) pravoúhlé trojúhelníky.
(3) Věta platí pro všechny trojúhelníky.
(4) Každý mnohoúhelník se dá rozřezat na trojúhelníky. □





Úloha 1. Uvažujme mřížový trojúhelník, jehož strany neobsahují kromě samotných vrcholů žádné mřížové body a který ve svém vnitřku obsahuje právě jeden mřížový bod. Nahlédněte, že tento vnitřní mřížový bod musí být těžištěm trojúhelníku.

Úloha 2. Kapitán pirátské lodi si chce pořídit zbrusu novou vlajku se zkříženými hnáty za 2022 dublonů. K dispozici má neomezenou zásobu mincí v hodnotách 1, 2 a 3 dublony. Kolika různými způsoby může zaplatit? (Způsoby zaplacení, které se liší jen pořadím mincí, nepovažujeme za různé.)

Úloha 3. (Eulerův vzorec) Uvažujme rovinné nakreslení grafu, ve kterém jsou všechny vrcholy mřížové body a všechny hrany jsou úsečky. Jsou-li v, e, s po řadě počty vrcholů, hran a stěn v tomto nakreslení, dokažte s pomocí Pickova vzorce rovnost $v - e + s = 2$.

Úloha 4. (Pick pro děravé mnohoúhelníky) Mějme v rovině mnohoúhelník P s h dírami. Formálně: nechť P vznikne odebráním navzájem disjunktních mřížových mnohoúhelníků $P_1, \ldots, P_h$ od mřížového mnohoúhelníku P_0, přičemž obvody jednotlivých P_i jsou disjunktní s obvodem P_0 i spolu navzájem. Dokažte, že pokud P obsahuje ve svém vnitřku a na svých obvodech po řadě i a b mřížových bodů, pak má obsah $i + \frac{b}{2} + h - 1$.

Úloha 5. *Půlbodem* nazveme libovolný bod tvaru $\left(\frac{a}{2}, \frac{b}{2}\right)$ pro celá čísla a, b. Nahlédněte, že libovolný půlbod ležící ostře uvnitř mřížového mnohoúhelníku lze vyjádřit jako střed úsečky spojující dva mřížové body ležící uvnitř nebo na obvodu tohoto mnohoúhelníku.

Pozorování. *Má-li mřížový mnohoúhelník obsah S, pak je $2S$ celé číslo.*

Úloha 6. Existuje rovnostranný trojúhelník s vrcholy v bodech kanonické mřížky?

Úloha 7. Dokažte, že pro liché $n \geq 5$ neexistuje pravidelný n-úhelník s vrcholy v bodech kanonické mřížky.

Úloha 8. Nahlédněte, že Pickovu větu nelze nijak přímočaře zobecnit do vyšších dimenzí. K tomu nalezněte v prostoru dva mnohostěny, které pokrývají svými vnitřky, stranami, hranami apod. vždy stejné počty mřížových bodů, ale přesto mají různé objemy.

Ve vyšších dimenzích tedy nemáme použitelnou obdobu Pickovy věty. Podobnou informaci však kóduje *Ehrhartova věta*, kterou uvedeme bez důkazu:

Věta. (Ehrhart) *Buď M (uzavřený) mřížový mnohostěn v d-rozměrném prostoru a nechť tM pro $t > 0$ označuje obraz M ve stejnolehlosti se středem v počátku a koeficientem t. Potom existuje polynom f_M takový, že pro každé $n \in \mathbb{N}$ pokrývá nM přesně $f_M(n)$ mřížových bodů.*

Úloha 9. Odvoďte pro mnohoúhelníky v rovině explicitní tvar Ehrhartova polynomu na základě Pickova vzorce.

Fareyovy zlomky

Vyzbrojeni Pickovým vzorcem zkusme prozkoumat třídu krásných tvrzení, která vzejdou, začneme-li zlomky nahlížet jako mřížové body v rovině.

Definice. Budiž dáno přirozené n. *Fareyovou posloupností řádu n* rozumíme posloupnost všech těch zlomků z intervalu $\langle 0, 1\rangle$, jejichž jmenovatel v základním tvaru nepřevyšuje n, seřazených vzestupně a značíme ji $\mathcal{F}_n$.

Lemma. *Rovnoběžník s vrcholy $(0,0)$, (a,b), (c,d) a $(a+c,b+d)$ má obsah $|ad-bc|$.*

Toto lemma je jen speciálním případem obecného faktu, že objem rovnoběžnostěnu je až na znaménko roven determinantu matice složené z vektorů jeho hran. Ale k tomu se ještě dostaneme.

Úloha 10. (Farey-Cauchy) Jsou-li $\frac{a}{b} < \frac{c}{d}$ sousední zlomky v $\mathcal{F}_n$, pak $\frac{c}{d} - \frac{a}{b} = \frac{1}{bd}$. Naopak pokud $0 \le \frac{a}{b} < \frac{c}{d} \le 1$ splňují $\frac{c}{d} - \frac{a}{b} = \frac{1}{bd}$, pak spolu sousedí v nějakém $\mathcal{F}_n$.

Úloha 11. (Dirichletova věta o diofantických aproximacích) Je dáno iracionální $\alpha \in (0,1)$. Dokažte, že existuje nekonečně mnoho zlomků $\frac{p}{q}$ v základním tvaru, které splňují $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

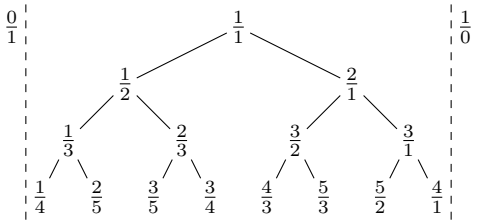
Definice. *Mediantem* zlomků $\frac{a}{b}$ a $\frac{c}{d}$ rozumíme zlomek $\frac{a+c}{b+d}$.

Úloha 12. Uvažujme tři po sobě jdoucí Fareyovy zlomky. Nahlédněte, že ten prostřední je mediantem zbylých dvou (uvažovaných v základním tvaru).

Úloha 13. (Fordovy kružnice) Pro zlomek $0 \le \frac{p}{q} \le 1$ v základním tvaru nakreslíme kružnici s průměrem $\frac{1}{q^2}$, která se dotýká reálné osy v bodě $\frac{p}{q}$. Dokažte, že dvě takové kružnice se dotýkají právě tehdy, když spolu odpovídající zlomky sousedí v některém $\mathcal{F}_n$.

Definice. (Sternův-Brocotův strom) Sestrojme nekonečný binární strom následovně. Na počátku mějme v kořeni zlomek $\frac{1}{1}$, od něhož se v dáli po řadě nalevo a napravo vznáší „zlomky“ $\frac{0}{1}$ a $\frac{1}{0}$. Tyto „zlomky“ v dáli nebudou mít žádné potomky, zatímco počínaje kořenem $\frac{1}{1}$ bude mít každý jiný zlomek dva potomky: levého, který bude mediantem tohoto zlomku s nejbližším nižším zlomkem na této

nebo vyšší úrovni, a pravého, který bude mediantem tohoto zlomku s nejbližším vyšším zlomkem na této nebo vyšší úrovni.



Úloha 14. Nahlédněte, že Sternův-Brocotův strom obsahuje všechna kladná racionální čísla, a to dokonce v základním tvaru.

Úloha 15. Definujme *jednoduchost* zlomku $\frac{p}{q}$ jako $j\left(\frac{p}{q}\right) = \frac{1}{pq}$. Určete součet jednoduchostí všech 2^n zlomků v n-tém řádku Sternova-Brocotova stromu.

Úloha 16. Uvažujme pro $n \geq 5$ navzájem různé mřížové body $(a_1, b_1), \ldots, (a_n, b_n)$ v rovině, které splňují $|a_i b_{i+1} - a_{i+1} b_i| = 1$ pro každé $1 \leq i \leq n$, přičemž uvažujeme $(a_{n+1}, b_{n+1}) = (a_1, b_1)$. Dokažte, že $|a_i b_j - a_j b_i| = 1$ je splněno i pro nějakou dvojici nesousedních indexů i, j. (Korean TST)

Nutná dávka analyticko-geometrických (ne)definic

Další na jídelníčku je Minkowského věta. K jejímu náležitému strávení si však nejdřív potřebujeme osvojit nějaké ošklivější technické koncepty v čele s (obecnou) mřížkou. Nebude to samo o sobě moc zábava, ale je to potřeba ...

S objemem budeme pracovat pouze v intuitivním pojetí. Abychom ctěného čtenáře ušetřili od pojmů jako *měřitelná množina*, budeme ty množiny bodů, u kterých dává smysl hovořit o objemu, nazývat *útvary*. Intuitivně si račte představovat libovolnou slušně vychovanou hroudu.

Nedefinice. *Objem* útvaru U je nějaké nezáporné číslo, jež značíme $\operatorname{Vol} U$. Pro jeho počítání platí:

(i) Má-li d-rozměrný „hranol“ $(d-1)$-rozměrnou podstavu s objemem S a na ní kolmou výšku h, pak je objem hranolu roven $h \cdot S$.
(ii) Má-li d-rozměrný „kužel“ $(d-1)$-rozměrnou podstavu s objemem S a na ní kolmou výšku h, pak je objem kužele roven $\frac{1}{d} \cdot h \cdot S$.
(iii) Pro disjunktní útvary U_1, U_2 platí $\operatorname{Vol}(U_1 \cup U_2) = \operatorname{Vol} U_1 + \operatorname{Vol} U_2$.
(iv) Je-li U' obrazem U v posunutí (či obecněji nějakém shodném zobrazení), pak $\operatorname{Vol} U' = \operatorname{Vol} U$.
(v) d-rozměrná koule s poloměrem R má objem $C_d R^d$, kde C_d je nějaká konstanta. Pro C_d existuje (komplikovaný) explicitní předpis, nám však postačí prvních pár hodnot:

$$C_1 = 2, \qquad C_2 = \pi, \qquad C_3 = \frac{4\pi}{3}, \qquad C_4 = \frac{\pi^2}{2}.$$

Dále se nám bude hodit umět počítat objemy rovnoběžnostěnů. K tomu, bohužel, musíme zaběhnout k *maticím*. Co že to matice je? Račte si vybrat: obdélníček plný čísel, sloupcové vektory zapsané vedle sebe, řádkové vektory zapsané pod sebou, pro fajnšmekry jenom reprezentace nějakého lineárního zobrazení.

Matice a objemy propojuje koncept *determinantu*. Opět si k němu dovolíme zamlčet „tu korektní“ definici a místo toho pragmaticky popsat, jak s tím pracovat.

Nedefinice. *Determinant* čtvercové $d \times d$ matice

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix} = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_d)$$

je nějaké číslo, jež značíme $\det A$. Pro jeho počítání platí:

(i) Rozvoj podle sloupce: kdykoliv zvolíme $1 \leq j \leq d$, pak platí

$$\det A = \sum_{i=1}^{d} (-1)^{i+j} a_{ij} \det A_{ij},$$

kde A_{xy} značí matici $(d-1) \times (d-1)$, která vznikne z A vyškrtnutím x-tého řádku a y-tého sloupce.

(ii) Přičítání sloupců k jiným nemění determinant: Je-li $\mathbf{u}$ vektor, který leží v nadrovině určené sloupcovými vektory $\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_d$, pak

$$\det(\mathbf{a}_1|\cdots|(\mathbf{a}_j + \mathbf{u})|\cdots|\mathbf{a}_d) = \det A.$$

(iii) Determinant diagonální matice: Pokud je A *diagonální*, tzn. všechny její prvky vyjma $a_{11}, a_{22}, \ldots, a_{dd}$ jsou nulové, pak $\det A = a_{11} \cdot a_{22} \cdots a_{dd}$.

Pravidla (i) a (ii) platí i tehdy, když zaměníme sloupce a řádky.

Hned si také rozmysleme cvičení, které dává intuitivní představu za determinantem a osvětluje některé jeho vlastnosti. Zdůrazněme, že tohle je celý důvod, proč se o determinanty vůbec staráme – chceme počítat *nějaké* objemy.

Cvičení. Rozmyslete si, že objem d-rozměrného rovnoběžnostěnu, jehož hrany odpovídají vektorům $\mathbf{v}_1, \ldots, \mathbf{v}_d$, je roven $|\det(\mathbf{v}_1|\cdots|\mathbf{v}_d)|$. K tomu pomohou následující pozorování:

(1) Je-li matice v diagonálním tvaru, objem i determinant jsou si rovny.
(2) Sloupcové úpravy, které zachovávají determinant, zachovávají i objem.

Definice. *Mřížkou* v $\mathbb{R}^d$ rozumíme množinu $\Lambda \subset \mathbb{R}^d$, pokud není podmnožinou žádné nadroviny[1] a lze ji pro nějakou d-tici vektorů $\mathbf{b}_1, \ldots, \mathbf{b}_d$ vyjádřit přesně jako množinu všech součtů $t_1\mathbf{b}_1 + \cdots + t_d\mathbf{b}_d$ pro celá čísla $t_1, \ldots, t_d$. Takovou d-tici $\mathbf{b}_1, \ldots, \mathbf{b}_d$ nazýváme *bází* mřížky Λ.

Definice. Je-li $\mathbf{b}_1, \ldots, \mathbf{b}_d$ báze mřížky Λ, pak *determinantem* Λ (značíme $\det \Lambda$) označujeme absolutní hodnotu determinantu matice $(\mathbf{b}_1 \mid \cdots \mid \mathbf{b}_d)$.

Bystří mohou namítat, že bází mřížky by mohlo být mnoho – co když každá z nich dává jiný determinant? Bez obav:

Tvrzení. $\det \Lambda$ *nezávisí na volbě konkrétní báze.*

Vzpomíná si ještě ctěný čtenář na objemovou interpretaci determinantu? Pak jej jistě nepřekvapí následující:

Pozorování. *Je-li $\mathbf{b}_1, \ldots, \mathbf{b}_d$ nějaká báze mřížky $\Lambda \subset \mathbb{R}^d$, pak je $\det \Lambda$ objem tzv. fundamentálního rovnoběžnostěnu $\{t_1\mathbf{b}_1 + \cdots + t_d\mathbf{b}_d \mid t_1, \ldots, t_d \in \langle 0, 1)\}$.*

Cvičení. Rozmyslete si, že Pickova věta platí i pro obecnou mřížku v $\mathbb{R}^2$, pokud výsledný obsah vynásobíme $\det \Lambda$.

Úloha 17. Reálná čísla a, b, c splňují $a, c > 0$ a zároveň $D = 4ac - b^2 > 0$. Dokažte, že nerovnost $ax^2 + bxy + cy^2 < R^2$ určuje v rovině elipsu s obsahem $\frac{2\pi}{\sqrt{D}}R^2$.

Pro počítání objemů se nám také občas bude hodit poznat kolmé vektory, oprášíme proto základní vlastnosti skalárního součinu. Pro ty z vás, kdo vidíte skalární součin poprvé, vězte, že není třeba se s tím příliš trápit :-).

Definice. *Skalární součin* vektorů $\mathbf{u} = (u_1, \ldots, u_d)$ a $\mathbf{v} = (v_1, \ldots, v_d)$ definujeme jako $\mathbf{u} \cdot \mathbf{v} = u_1v_1 + \cdots + u_dv_d$.

Ne zcela očividná geometrická interpretace skalárního součinu je, že promítneme $\mathbf{u}$ na přímku určenou $\mathbf{v}$ a (orientovanou) délku této projekce znásobíme s délkou $\mathbf{v}$. S tímto pohledem pak nepřekvapí:

Cvičení. Vektory $\mathbf{u}, \mathbf{v} \in \mathbb{R}^d$ jsou kolmé, právě když $\mathbf{u} \cdot \mathbf{v} = 0$.

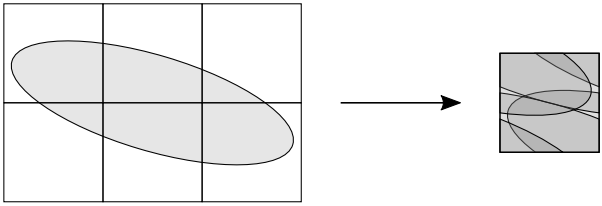
Minkowského věta

Jako předskokana pana Minkowského nejprve představme pana Blichfeldta:

Věta. (Blichfeldt) *Mějme v d-rozměrném prostoru útvar s objemem V. Potom lze tento útvar posunout tak, aby obsahoval alespoň $\lceil V \rceil$ bodů kanonické mřížky.*

Důkaz. Rozřežme daný útvar podél jednotkových krychliček kanonické mřížky a tyto rozřezané dílky přeložme přes sebe. Pokud se v některém bodě jednotkové krychličky překryje alespoň $\lceil V \rceil$ různých dílků, vyhráli jsme. Pokud ne, pak je objem roven nanejvýš $\lceil V \rceil - 1 < V$, což je spor. □

[1] Jinými slovy: Λ je „roztažená po celém $\mathbb{R}^d$“. Pouze zakazujeme to, aby Λ degenerovaně ležela jen v nějakém menším podprostoru.



Cvičení. Pro obecnou mřížku Λ se věta zobecní zohledněním determinantu – náš útvar bude v nějakém posunutí obsahovat alespoň $\left\lceil \frac{V}{\det \Lambda} \right\rceil$ bodů z Λ.

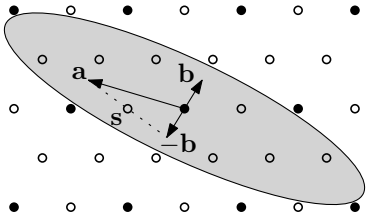
K samotné Minkowského větě zbývá ještě jedna stěžejní definice:

Definice. Množinu M bodů v d-rozměrném prostoru nazveme *konvexní*, pokud pro libovolné body $A, B \in M$ je i celá úsečka AB obsažena v M.

Sami se přesvědčte (ale nedokazujte formálně), že např. koule, kvádry, válce či rovnoběžnostěny jsou konvexní. Mnohoúhelníky jsou obecně konvexní právě tehdy, mají-li všechny vnitřní úhly menší než $180°$.

Věta. (Minkowski) *Buďte v d-rozměrném prostoru dány mřížka Λ a útvar C, který je konvexní a středově souměrný podle počátku. Pokud* $\operatorname{Vol} C > 2^d \det \Lambda$, *pak v C leží nějaký nenulový bod z Λ.*

Důkaz. Uvažme dvojnásobně nafouknutou mřížku 2Λ, ta má determinant $2^d \det \Lambda$, což je méně než $\operatorname{Vol} C$. Podle předchozího cvičení pak jde C posunout tak, aby obsahovala alespoň dva různé body z 2Λ. To znamená, že nějaké dva různé body $\mathbf{a}, \mathbf{b} \in C$ splňují $\mathbf{a} - \mathbf{b} \in 2\Lambda$. Ze středové souměrnosti ale C obsahuje i bod $-\mathbf{b}$ a z konvexnosti také střed $\mathbf{s}$ úsečky spojující $\mathbf{a}$ s $-\mathbf{b}$. Máme tak $0 \neq \mathbf{s} \in C$, ale díky $\mathbf{a} - \mathbf{b} \in 2\Lambda$ taky $\mathbf{s} = \frac{\mathbf{a}+(-\mathbf{b})}{2} \in \Lambda$, jak jsme chtěli. □



Úloha 18. (německý lesík) V poloměru $R > 0$ od počátku se rozkládá džungle. V každém mřížovém bodě uvnitř tohoto kruhu vyjma počátku roste strom s jistým pevně daným poloměrem $r > 0$. V počátku stojí pirát. Nahlédněte, že pokud je R dostatečně velké, pirát nevidí z džungle ven.

Cvičení. Nechť je v předchozí úloze naopak pevně dáno $R > 1$. Vyrobte co nejlepší dolní odhad pro hodnotu r, při které ještě pirát v některém směru vidí z džungle ven.

Lemma. *Mějme prvočíslo $p \equiv 1 \pmod 4$. Pak existuje c takové, že $c^2 + 1 \equiv 0 \pmod p$.*

Úloha 19. (Fermatova věta o dvou čtvercích) Prvočíslo $p \equiv 1 \pmod 4$ lze vyjádřit jako $p = x^2 + y^2$ pro celá čísla x, y.

Lemma. *Je-li p prvočíslo, pak lze zvolit celá čísla x, y tak, že $x^2 + y^2 + 1 \equiv 0 \pmod p$.*

Úloha 20. (Lagrangeova věta o čtyřech čtvercích) Každé prvočíslo p lze vyjádřit jako $p = x^2 + y^2 + z^2 + w^2$ pro celá čísla x, y, z, w.

Úloha 21. Jsou dána přirozená čísla a, b, c splňující $ac = b^2 + b + 1$. Dokažte, že rovnice $ax^2 - (2b+1)xy + cy^2 = 1$ má celočíselné řešení. (Polská MO)

Úloha 22. (Pick z Minkowského) Dokažte pomocí Minkowského věty, že trojúhelník, který má vrcholy v bodech kanonické mřížky a kromě nich neobsahuje žádné další mřížové body, musí mít obsah $\frac{1}{2}$.

Úloha 23. (opět Dirichletova věta o diofantických aproximacích) Budiž dáno reálné číslo α a přirozené N. Dokažte, že existuje nějaký zlomek $\frac{p}{q}$ s $1 \le q \le N$ splňující $\left|\alpha - \frac{p}{q}\right| \le \frac{1}{qN}$.

Úloha 24. (simultánní aproximace) Buďte dána přirozená čísla k, N a reálná $\alpha_1, \ldots, \alpha_k$. Dokažte, že lze zvolit celá čísla $p_1, \ldots, p_k$ a přirozené $1 \le q \le N$ tak, aby bylo pro každé $i \in \{1, \ldots, k\}$ splněno $\left|\alpha_i - \frac{p_i}{q}\right| \le \frac{1}{q\sqrt[k]{N}}$.

Úloha 25. Nahlédněte, že mřížka $\Lambda \subset \mathbb{R}^d$ musí obsahovat nějaký nenulový vektor $\mathbf{v}$ velikosti $|\mathbf{v}| \le \sqrt{d} \cdot \sqrt[d]{\det \Lambda}$.

Další úlohy

Úloha 26. Dvě nekonečné posloupnosti celých čísel $a_1, a_2, \ldots$ a $b_1, b_2, \ldots$ splňují

$$(a_n - a_{n-1})(a_n - a_{n-2}) + (b_n - b_{n-1})(b_n - b_{n-2}) = 0$$

pro všechna $n > 2$. Dokažte, že pro nějaký index k je splněno $a_k = a_{k+2016}$.
(*i*KS 5–A5)

Úloha 27. (jednoznačnost dvou čtverců) Už víme, že $p = x^2 + y^2$ má pro prvočíslo $p \equiv 1 \pmod 4$ řešení. Dokažte, že toto řešení je dokonce jednoznačné až na změnu znamének a pořadí.

Úloha 28. V rovině je dán konvexní mřížový pětiúhelník. Dokažte, že (uzavřený) pětiúhelník, který vytínají úhlopříčky původního pětiúhelníku, obsahuje mřížový bod.

Úloha 29. Pro přirozené n nechť $f(n)$ značí počet způsobů, jak zaplatit částku n pomocí mincí v hodnotách všech mocnin dvojky. Všech druhů mincí přitom máme neomezené množství a způsoby zaplacení, které se liší jen pořadím mincí, nepovažujeme za různé. Dokažte, že pro $n \geq 3$ platí $2^{n^2/4} < f(2^n) < 2^{n^2/2}$. (IMO 1997)

Úloha 30. Buď dána konečná množina $S = \{p_1, \ldots, p_n\}$ prvočísel. Pro $x \in \mathbb{R}$ nechť $f(S, x)$ počet těch přirozených čísel nepřevyšujících x, která mají všechny své prvočíselné dělitele v S. Nahlédněte, že $f(S, x) \approx \frac{(\log x)^n}{n! \log p_1 \cdots \log p_n}$, resp. formálně $\lim_{x\to\infty} \frac{f(S,x)}{(\log x)^n} = \frac{1}{n! \log p_1 \cdots \log p_n}$.

Úloha 31. Budiž dáno přirozené číslo $m \geq 2$, potom nazvěme mřížový bod v rovině *m-mřížovým*, pokud jsou obě jeho souřadnice násobky m. Dokažte, že existuje konstanta $c > 0$ s vlastností: kdykoliv mřížový trojúhelník v rovině obsahuje právě jeden m-mřížový bod, pak má obsah nanejvýš cm^3. (China TST 2021)

Úloha 32. Buďte dána C, d a r. Vektor $\mathbf{w} \in \mathbb{R}^d$ délky 1 nazveme *(C, r)-žůžovým*, pokud pro každý nenulový mřížový vektor $\mathbf{z}$ splňuje vztah $|\mathbf{w} \cdot \mathbf{z}| \geq \frac{C}{|\mathbf{z}|^r}$, kde $\cdot$ je skalární součin a $|\mathbf{z}|$ značí délku vektoru $\mathbf{z}$. Dokažte, že:

(a) Pro $r < d - 1$ nikdy neexistuje žádný (C, r)-žůžový vektor.
(b)** Pro $r > d - 1$ lze zvolit C tak, aby existoval nějaký (C, r)-žůžový vektor.

Na úplný závěr zabitá úloha s hlubokými souvislostmi v algebraické teorii čísel – jedná se o jistou podobu tzv. *Minkowského meze*:

Úloha 33. Buď $f(x)$ monický polynom stupně n s celočíselnými koeficienty, který je ireducibilní nad $\mathbb{Q}$ a má n reálných kořenů $r_1, \ldots, r_n$. Potom platí

$$\prod_{1\leq i<j\leq n} |r_i - r_j| \geq \frac{n^n}{n!}.$$

Návody

1. Těžiště se pozná tak, že dělí trojúhelník na tři menší s navzájem rovnými obsahy.

2. Jedničky lze vždy jednoznačně doplnit. Interpretuj validní způsoby zaplacení jako mřížové body překryté jistým trojúhelníkem.

3. Spočítej obsah „celého grafu“, tzn. doplňku vnější stěny, dvěma způsoby: jednou přímo a podruhé posčítáním všech vnitřních stěn.

4. Jednoduše odečti Pickovské obsahy děr.

5. Středově zobraz mnohoúhelník podle půlbodu a počítej obsahy. Pozor, mohou vzniknout díry!

6. Čtverec vzdálenosti dvou mřížových bodů je celé číslo ...

7. Trik: nafoukni dvakrát a vezmi středy nejdelších úhlopříček. Jako mnohem techničtější alternativa jde taky zkoumat racionalitu jistých hodnot goniometrických funkcí.

8. Možností je mnoho. Jednou z těch přímočařejších jsou tzv. *Reeveovy čtyřstěny*: zafixuj půlčtverečkovou podstavu a poté hýbej výškou čtyřstěnu.

9. Ve stejnolehlosti se snadno předvídatelně chovají obsah mnohoúhelníku a počet mřížových bodů na hranici. Body uvnitř dopočítej z Pickova vzorce.

10. Interpretuj zlomky jako mřížové body a rozmysli, co dovedeš říct o trojúhelníčcích, které určují. V opačném směru stačí vzít $n = \max\{b, d\}$.

11. Pro libovolné n spadne α mezi nějaké dva Fareyovy zlomky.

12. Zapiš si vztah z Fareyovy-Cauchyovy věty pro obě sousedící dvojice.

13. Prostě to spočítej a použij Fareyovu-Cauchyovu větu.

14. Půlky Sternova-Brocotova stromu jsou hezky souměrné a levou tvoří Fareyovy zlomky. Potomci mají vždy větší jmenovatele, takže každý mediant tvoří nový Fareyův zlomek, který už bude v základním tvaru.

15. $j\left(\frac{p+q}{q}\right) + j\left(\frac{p}{p+q}\right) = j\left(\frac{p}{q}\right)$. Tyto zlomky se vždy najdou na následujícím řádku, protože operace $\frac{p}{q} \mapsto \frac{p+q}{q}$ a $\frac{p}{q} \mapsto \frac{p}{p+q}$ se k Sternovu-Brocotovu stromu chovají hezky.

16. Podívej se na (ve vhodném smyslu) „největší“ vektor.

17. Přenásobením vhodnou maticí získáš kružnici $x^2 + y^2 < R^2$, obsah se mění s determinantem.

18. Pouprav si pohled: místo stromů s poloměrem a paprsků světla bez šířky uvažuj bodové stromy a paprsek světla s šířkou.

19. Jako množinu ber (otevřenou) kouli s poloměrem $\sqrt{2p}$. Mřížku vyrob z vektorů $(1, c)$ a $(0, p)$.

20. Použij podobnou strategii jako u dvou čtverců: volbou mřížky zajisti, aby všechny její body měly čtverec vzdálenosti od počátku $0 \pmod p$, volbou množiny pak zajisti, že to nemůže být $2p$ či víc.

21. Díky zadané podmínce má výraz nalevo malý diskriminant – to odpovídá velkému obsahu elipsy.

22. Vyrob z několika kopií trojúhelníku větší rovnoběžník se středem v mřížovém bodě.

23. Interpretuj $\frac{p}{q}$ jako mřížový bod (p, q). Trošičku uprav kýžené podmínky, aby dávaly symetrickou konvexní množinu a spočítej objem.

24. Přímočaře rozšiř konstrukci z předchozí úlohy. Věci, co potřebuješ počítat, vypadají fakt hezky – podstavy jsou obdélníky/kvádry.

25. Koule by možná dala lepší konstantu, nicméně postačí krychle.

26. Kolmé vektory.

27. Je-li k kružnice $x^2 + y^2 = p$ a Λ mřížka vyrobená z vektorů $(1, c)$, $(0, p)$, chceš dokázat $|k \cap \Lambda| = 4$. Pick pomůže.

28. Tady žádná věta nepomůže! Použij středový trik, připrav se na rozebrání případů a neboj se opřít o indukci!

29. Počet mřížových bodů $\approx$ objem. V dokazovaném odhadu je spousta místa, stačí rozumně odhadnout chybu.

30. Souřadnice v $\mathbb{R}^n$ interpretuj jako exponenty v prvočíselném rozkladu. Rozdíl objemu a počtu pokrytých mřížových bodů je nanejvýš úměrný povrchu, takže celkem malý.

31. Zkombinuj dvě možnosti, jak zkonstruovat další m-mřížový bod: buďto $(m+1)$-násobně stejnolehli z některého vrcholu, anebo najdi dost velký rovnoběžník zacentrovaný v onom jednom m-mřížovém bodě, jehož (alespoň) půlka leží uvnitř trojúhelníku.

32. (a) Je-li dáno $\mathbf{w}$, najdi $\mathbf{z}$, které ho rozbije, pomocí Minkowského věty. Množina daná touto vlastností není konvexní, ale dovedeš v ní najít válec libovolně velkého objemu. (b) Je-li dáno $\mathbf{z}$, spočti, jak velkou část jednotkové sféry, kterou toto $\mathbf{z}$ zakazuje, a nahlédni, že součet konverguje, takže pro dost malé C nebude zakázaná celá sféra. Možná narazíš na to, že s povrchy se blbě pracuje – vypořádej se s tím nějak.

33. Račte se posadit a připoutat, bude to jízda:

(1) Levá strana je determinant mřížky s bázovými vektory $(1, r_i, r_i^2, \ldots, r_i^{n-1})$.
(2) Do Minkowského věty chceš použít množinu $\{|x_1| + \cdots + |x_n| < n\}$. Proč?
(3) Protože AGčko!
(4) Pro body z mřížky ale z Viètových vztahů musí být $x_1 \cdots x_n$ celé číslo.
(5) Profit.

Literatura a zdroje

[1] Jakub Löwit: *Čísla a čtverečky*, sborník *i*KS, 2017.
[2] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book*, XYZ Press, 2008.
[3] Jiří Matoušek: *Introduction to Discrete Geometry*, KAM MFF UK, *kam.mff.cuni.cz/~matousek/kvg1-tb.pdf*.
[4] Martin Klazar: *Úvod do teorie čísel*, KAM MFF UK, *kam.mff.cuni.cz/~klazar/ln_utc.pdf*.
[5] Keith Conrad: *Sums of two squares and lattices*, *kconrad.math.uconn.edu/blurbs/ugradnumthy/Picksumofsq.pdf*.