Úvod do teorie čísel - příprava na zkoušku

Karel Velička

31. ledna 2025

Vyučující: *doc. RNDr. Martin Klazar, Dr.*

Obsah

1 Dirichletova věta na Diophantinovy aproximace a její aplikace.

Věta 1.1. ***(Dirichletova)*** *Pro každé $\alpha \in \mathbb{R}$ a každé $Q \in \mathbb{N}$, kde $Q \geq 2$, existují $p, q \in \mathbb{Z}$ takové, že $1 \leq q < Q$ a*

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

Důkaz. Předpokládejme, že existují Q čísla $\{n\alpha\}$ ($\in [0,1)$) pro $n = 0, 1, \ldots, Q-1$. Číslo $\{n\alpha\}$ je zbytek nějakého reálného čísla, tedy je ve tvaru $\{n\alpha\} = n\alpha - \lfloor n\alpha \rfloor$. Můžeme si je představit jako body ležící na kružnici s obvodem 1. Díky principu holubníku víme, že alespoň dva z nich jsou $\leq \frac{1}{Q}$. To znamená, že pro nějaké $m, n, r, s \in \mathbb{Z}$, kde $0 \leq n < m < Q$ platí:

$$|(m\alpha - r) - (n\alpha - s)| \leq \frac{1}{Q} \quad \iff \quad |\alpha(m-n) - (r-s)| \leq \frac{1}{Q}$$

Položíme $p := r - s$ a $q := m - n$. Dostaneme tak pro $1 \leq q < Q$ výsledné:

$$|\alpha q - p| \leq \frac{1}{Q} \quad \overset{\div q}{\iff} \quad \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq}.$$

■

Důsledek 1.1. *Pro každé $\alpha \in \mathbb{I}$ $(= \mathbb{R} \setminus \mathbb{Q})$ existuje nekonečně mnoho různých zlomků $\frac{p}{q}$, že*

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

Důkaz. Zkonstruujeme nekonečně mnoho zlomků $\frac{p_1}{q_1}, \ldots$ takových, že pro každý platí nerovnost

$$\left|\alpha - \frac{p_1}{q_1}\right| > \left|\alpha - \frac{p_2}{q_2}\right| > \cdots > 0.$$

Začneme s $p_1 := \lfloor \alpha \rfloor$ a $q_1 := 1$. Pokud $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ jsou už zkonstruované, vezmeme libovolné $Q \in \mathbb{N}$ takové, že $|\alpha - \frac{p_n}{q_n}| > \frac{1}{Q}$ (což je možné, protože α je iracionální) a použijeme *Dirichletovu větu.* Dostaneme tak zlomek $\frac{p}{q}$ takový, že $1 \leq q < Q$ a $|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} < \frac{1}{q^2}$.
Zároveň, jelikož $|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} \leq \frac{1}{Q} < |\alpha - \frac{p_n}{q_n}|$, tak můžeme položit $p_{n+1} := p_n$ a $q_{n+1} := q_n$. ■

Definice 1.1. ***(Fareyovy zlomky řádu** n**):*** Předpokládejme $\forall n \in \mathbb{N}$ uspořádaný seznam

$$F_n := \left(\frac{0}{1} = \frac{p_1}{q_1} < \frac{p_2}{q_2} < \ldots < \frac{p_m}{q_m} = \frac{1}{1}\right),$$

všech $m = m(n)$ zlomků $\frac{p}{q} \in [0,1]$ takových, že $0 < q \leq n$ a $(p,q) = 1$.

2 Hurwitzova věta.

Věta 2.1. ***(Farey–Cauchy)****: Pokud $\frac{a}{b} < \frac{c}{d}$ jsou dva po sobě jdoucí členy F_n, pak $bc - ad = 1$, což znamená, že $\frac{a}{b}$ a $\frac{c}{d}$ jsou jsou co nejblíže.*

Věta 2.2. ***(Hurwitz)****: Skládá se ze dvou částí:*

(1) Pro každé $\alpha \in \mathbb{I}$ existuje nekonečně mnoho různých $\frac{p}{q} \in \mathbb{Q}$, že:

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

(2) Pro každé reálné $A > \sqrt{5}$ platí, že nerovnice

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

má pouze konečně mnoho řešení $\frac{p}{q} \in \mathbb{Q}$.

Důkaz. Dokážeme obě části zvlášť:

(1) Předpokládejme, že $\alpha \in (0,1)$. Ukážeme, že pokud $a/b < \alpha < c/d$ pro dvě po sobě jdoucí Fareyovy zlomky z množiny F_n, pak jeden ze tří zlomků

$$\frac{a}{b}, \quad \frac{c}{d}, \quad \frac{e}{f} = \frac{a+c}{b+d}$$

splňuje nerovnici. Postupným zařazováním α mezi dvě po sobě jdoucí členy F_n pro stále větší n (podobně jako u Dirichletovy nerovnosti) získáme nekonečně mnoho zlomků splňujících

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

Předpokládejme nyní sporem, že žádný z těchto tří zlomků nerovnici nesplňuje. Můžeme předpokládat, že $\alpha > e/f$, protože pro $\alpha < e/f$ bychom postupovali obdobně. Pak platí:

$$\alpha - \frac{a}{b} \geq \frac{1}{\sqrt{5}b^2}, \quad \alpha - \frac{e}{f} \geq \frac{1}{\sqrt{5}f^2}, \quad \frac{c}{d} - \alpha \geq \frac{1}{\sqrt{5}d^2}.$$

Sečtením první a třetí nerovnosti a také druhé a třetí nerovnosti dostáváme:

$$\frac{1}{bd} = \frac{c}{d} - \frac{a}{b} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{d^2}\right),$$

$$\frac{1}{df} = \frac{c}{d} - \frac{e}{f} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{f^2} + \frac{1}{d^2}\right).$$

Vynásobením první nerovnosti $\sqrt{5}b^2d^2$ a druhé $\sqrt{5}d^2f^2$ a jejich sečtením dostáváme:

$$d\sqrt{5}(b+f) = d\sqrt{5}(2b+d) \geq b^2 + 2d^2 + f^2 = 2b^2 + 3d^2 + 2bd,$$

což je ekvivalentní s

$$0 \geq \frac{1}{2}\left((\sqrt{5}-1)d - 2b\right)^2.$$

Z toho plyne, že $(\sqrt{5}-1)d - 2b = 0$, což vede na $\sqrt{5} = 1 + 2b/d \in \mathbb{Q}$, což je spor.

(2) Označme $\beta = (\sqrt{5}-1)/2$. Fixujme $A > \sqrt{5}$ a předpokládejme, že

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{Aq^2}$$

má nekonečně mnoho řešení $\frac{p}{q}$. Pak může být q libovolně velké. Jinými slovy:

$$\beta = \frac{p}{q} + \frac{\delta}{q^2},$$

kde $\delta \in \mathbb{R}, |\delta| < 1/A$. Přepíšeme to jako

$$\frac{\delta}{q} - q\frac{\sqrt{5}}{2} = q\beta - p - q\frac{\sqrt{5}}{2} = -q\frac{1}{2} - p.$$

Umocněním a odečtením $5q^2/4$ dostáváme identitu:

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = p^2 + pq - q^2.$$

Pro dostatečně velké q je absolutní hodnota levé strany menší než 1, protože $\delta^2/q^2 \to 0$ a $|\delta\sqrt{5}| < \sqrt{5}/A < 1$. To znamená, že rovnice $p^2 + pq - q^2 = 0$ má řešení $p, q \in \mathbb{Z}$, což je spor. Rovnice je totiž ekvivalentní s $(2p+q)^2 = 5q^2$, což opět vede na spor $\sqrt{5} = 1 + 2p/q \in \mathbb{Q}$.

■

3 Existence transcendentních čísel: Liouvilleova nerovnost.

Definice 3.1. ***(Algebraická čísla)****:* Říkáme, že $\alpha \in \mathbb{C}$ je *algebraické číslo*, pokud existuje nenulový polynom $p \in \mathbb{Q}[x]$ takový, že $p(\alpha) = 0$. Tedy $\sum_{i=0}^{n} \alpha_i x^i = 0$. *("je kořenem racionálního polynomu")*

Definice 3.2. ***(Transcendentní čísla)****:* Každé $\alpha \in \mathbb{C}$, které není algebraické, je *transcendentní.*

Věta 3.1. ***(Lagrangeova o střední hodnotě):*** *Pokud $f : [0,1] \to \mathbb{R}$ je spojitá, pak*

$$\exists c \in (a,b) : f'(c) = \tfrac{f(b)-f(a)}{b-a} =: z.$$

Věta 3.2. ***(J. Liouvilleova)****: Pro každé algebraické číslo $\alpha \in \mathbb{I}$ existuje $n \in \mathbb{N}$ a konstanta $c > 0$ taková, že pro každé $\frac{p}{q} \in \mathbb{Q}$ platí:*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}.$$

Důkaz. Předpokládejme, že $0 \neq f \in \mathbb{Z}[x]$ má minimální stupeň $n = \deg f(x)$, kde $f(\alpha) = 0$. Zjevně, $n \geq 2$. Označme $I = [\alpha - 1, \alpha + 1]$ a vezměme libovolný zlomek $\frac{p}{q}$; můžeme předpokládat, že $q \in \mathbb{N}$. Mohou nastat dva případy:

(a) $\frac{p}{q} \notin I$: Triviálně $\left|\alpha - \frac{p}{q}\right| \geq 1 \geq \frac{1}{q^n}$.

(b) $\frac{p}{q} \in I$: Podle *Lagrangeovy věty o průměru* existuje $\zeta \in \mathbb{R}$, které leží mezi α a $\frac{p}{q}$ a splňuje rovnost

$$f(\alpha) - f\left(\frac{p}{q}\right) = f'(\zeta) \cdot \left(\alpha - \frac{p}{q}\right).$$

Označme $d = \max(\{|f'(x)| : x \in I\})(> 0)$, připomeňme, že $f(\alpha) = 0$, a získáme hranici

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{f(\frac{p}{q})}{d}.$$

Tvrdíme, že $f(\frac{p}{q}) \neq 0$. Kdyby $f(\frac{p}{q}) = 0$, pak by pro vhodné číslo $N \in \mathbb{N}$ byl součin $g(x) = N \cdot \frac{f(x)}{x - p/q} \in \mathbb{Z}[x]$ celočíselný polynom s $g(\alpha) = 0$ a $\deg g(x) = \deg f(x) - 1 = n - 1$, což je ovšem ve sporu s definicí $f(x)$.

Proto pro $f(x) = \sum_{i=0}^{n} a_i x^i$, kde $a_i \in \mathbb{Z}$, máme hranici:

$$\left|f\left(\frac{p}{q}\right)\right| = \frac{1}{q^n} \cdot \left|\sum_{i=0}^{n} a_i p^i q^{n-i}\right| \geq \frac{1}{q^n} \quad \text{a} \quad \left|\alpha - \frac{p}{q}\right| \geq \frac{1/d}{q^n}.$$

Spojením hranic z (a) a (b) dostaneme požadovanou hranici, takovou, že pro každý zlomek $\frac{p}{q}$ platí:

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{\min(\{1, \frac{1}{d}\})}{q^n}.$$

■

Důsledek 3.1. *Pro každé $k \in \mathbb{N}, k \geq 2$, je číslo $\lambda(k) = \sum_{n=0}^{\infty} k^{-n!}$ transcendentní.*

4 Důkaz transcendence Eulerova čísla

Definice 4.1. ***(Algebraická čísla)):*** Říkáme, že $\alpha \in \mathbb{C}$ je *algebraické číslo*, pokud existuje nenulový polynom $p \in \mathbb{Q}[x]$ takový, že $p(\alpha) = 0$. Tedy $\sum_{i=0}^{n} \alpha_i x^i = 0$.

Definice 4.2. ***(Transcendentní čísla)):*** Každé $\alpha \in \mathbb{C}$, které není algebraické, je *transcendentní.*

Věta 4.1. *Eulerovo číslo $e = 2.71\ldots$ je transcendentní.*

Důkaz. Předpokládejme sporem, že Eulerovo číslo e je algebraické, tedy že pro $n \in \mathbb{N}$ a nějaké koeficienty $a_i \in \mathbb{Z}$:

$$a_n e^n + \ldots + a_1 e + a_0 = \sum_{i=0}^{n} a_i e^i = 0$$

Vynásobením vhodnou mocninou e můžeme předpokládat, že $a_0 \neq 0$. Násobením této rovnice číslem

$$\int_0^\infty x^r((x-1)(x-2)\cdots(x-n))^{r+1}e^{-x}\,dx,$$

které závisí na parametru $r \in \mathbb{N}$ (zvolíme později), dostaneme:

$$a_n e^n \int_0^\infty + a_{n-1}e^{n-1}\int_0^\infty + \ldots + a_1 e \int_0^\infty + a_0 \int_0^\infty = 0.$$

Rozdělením intervalu integrace $[0,\infty)$ na $[0,i]$ a $[i,\infty)$ přepíšeme tuto rovnici jako

$$P_1(r) + P_2(r) = \left(\sum_{i=0}^{n} a_i e^i \int_0^i\right) + \left(\sum_{i=0}^{n} a_i e^i \int_i^\infty\right) = 0.$$

Cílem je ukázat, že

(a) $|P_1(r)| < c^r$ pro všechna $r \in \mathbb{N}$ s konstantou $c > 1$ nezávislou na r,

(b) $|P_2(r)| \geq r!$ pro nekonečně mnoho $r \in \mathbb{N}$.

Pak rovnost nutně $\forall r \in \mathbb{N} : P_1(r) + P_2(r) \neq 0$, protože $\frac{|P_1(r)|}{r!} \to 0$ pro $r \to \infty$, ale $\frac{|P_2(r)|}{r!} \geq 1$ pro nekonečně mnoho r, což je spor.

Odhad $P_1(r)$ Na intervalu $[0,n]$ platí

$$|x^r((x-1)(x-2)\cdots(x-n))^{r+1}| \leq n^r(n^n)^{r+1} \quad \text{a} \quad |e^{-x}| \leq 1.$$

Proto pro $i = 0, 1, \ldots, n$:

$$\left|\int_0^i x^r((x-1)(x-2)\cdots(x-n))^{r+1}e^{-x}\,dx\right| \leq in^r(n^n)^{r+1} \leq (n^{n+1})^{r+1}.$$

Odtud:

$$\begin{aligned}|P_1(r)| = \left|\sum_{i=0}^{n} a_i e^i \int_0^i\right| &\leq |a_0| + |a_1|e\left|\int_0^1\right| + \ldots + |a_n|e^n\left|\int_0^n\right| \leq \\ &\leq (|a_0| + |a_1|e + \ldots + |a_n|e^n)(n^{n+1})^{r+1}.\end{aligned}$$

Což odpovídá tvaru c^r, tedy $|P_1(r)| < c^r$.

Odhad $P_2(r)$ Nejprve vyhodnotíme integrál $\int_0^\infty x^k e^{-x}\,dx$ pro $k \in \mathbb{N}_0$. Integrací per partes dostáváme:

$$\int_0^\infty \frac{x^k}{e^x}\,dx = \left[\frac{x^k}{e^x}\right]_0^\infty + k\int_0^\infty \frac{x^{k-1}}{e^x}\,dx = k\int_0^\infty \frac{x^{k-1}}{e^x}\,dx = \ldots = k!.$$

Obecně, pokud je $p(x) = b_n x^n + \cdots + b_1 x + b_0$ polynom, pak:

$$\int_0^\infty \frac{p(x)}{e^x}\,dx = \sum_{k=0}^{n} b_k k!.$$

Pro $P_2(r)$ substitucí $y = x - i$ získáme:

$$\begin{aligned} e^i \int_i^\infty &= \int_0^\infty x^r((x-1)(x-2)\cdots(x-n))^{r+1}e^{-(x-i)}\,dx = \\ &= \int_0^\infty (y+i)^r((y+i-1)(y+i-2)\cdots(y+i-n))^{r+1}e^{-y}\,dy. \end{aligned}$$

Pro $i = 0$ je polynom v integrandu tvaru $(-1)^{n(r+1)}(n!)^{r+1}y^r + ay^{r+1} + \cdots$. Pro $i \geq 1$ je nejmenší mocnina y s nenulovým koeficientem y^{r+1}. Z výše uvedeného a kongruencí plyne, že $P_2(r)$ je celočíselným násobkem $r!$ a pro nekonečně mnoho r platí $|P_2(r)| \geq r!$, což je spor. ■

5 Popište teorii Pellových (diofantovských) rovnic.

Definice 5.1. ***(Pellova rovnice).*** je to diofantická rovnice tvaru

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

kde $x, y \in \mathbb{Z}$ jsou neznámé a $d \in \mathbb{N}$ je pevný parametr, který není čtvercem.
Pokud se rovnice $x^2 - dy^2 = m$, pro parametr $m \in \mathbb{Z}$, pak mluvíme o ***zobecněné Pellově rovnici.***

Rovnice má vždy triviální řešení $(x, y) = (\pm 1, 0)$. Pokud $d = e^2 \in \mathbb{N}$ je čtverec, pak faktorizace $x^2 - dy^2 = (x - ey)(x + ey)$ ukazuje, že existuje pouze triviální řešení. Totéž platí, pokud $d \in \mathbb{Z}$ a $d < 0$. Pro $d = 0$ jsou všechna řešení $(\pm 1, z)$, kde $z \in \mathbb{Z}$.
Pro malá d lze netriviální řešení najít metodou pokus-omyl: třeba $(2, 1)$ pro $x^2 - 3y^2 = 1$, nebo $(3, 2)$ pro $x^2 - 2y^2 = 1$.

Generování řešení Pokud existuje netriviální řešení, pak existuje nekonečně mnoho řešení. Pro libovolná dvě řešení $(a, b), (e, f) \in \mathbb{Z}^2$ Pellovy rovnice je dvojice $(g, h) \in \mathbb{Z}^2$ definovaná jako

$$g + h\sqrt{d} = (a + b\sqrt{d})(e + f\sqrt{d})$$

také řešením. To plyne z faktu, že

$$g^2 - dh^2 = (a^2 - db^2)(e^2 - df^2) = 1 \cdot 1 = 1.$$

Pokud máme netriviální řešení $(a, b) \in \mathbb{N}^2$, pak pro $k = 1, 2, \ldots$ platí

$$a_k + b_k\sqrt{d} = (a + b\sqrt{d})^k,$$

což generuje nekonečně mnoho řešení $(a_k, b_k) \in \mathbb{N}^2$. Například řešení $(a, b) = (3, 2)$ pro $x^2 - 2y^2 = 1$ generuje řešení $(a_2, b_2) = (17, 12)$, $(a_3, b_3) = (99, 70)$ atd.

Věta 5.1. ***(Lagrange, 1770).*** *Každá Pellova rovnice $x^2 - dy^2 = 1$ má netriviální řešení (a tedy nekonečně mnoho řešení).*

Důkaz. Protože d není čtverec, $\sqrt{d}$ je iracionální. Podle druhé části Dirichletovy věty (kapitola 1) existuje nekonečně mnoho zlomků p/q takových, že

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

Tyto zlomky splňují

$$|p^2 - dq^2| = q|\sqrt{d} - p/q| \cdot |p + q\sqrt{d}| < \frac{|p + q\sqrt{d}|}{q} \leq \frac{p}{q} + \sqrt{d} \leq 2\sqrt{d} + 1.$$

Podle principu holubníku (pro nekonečně mnoho holubů a konečně mnoho děr) existuje $c \in \mathbb{Z}$ takové, že $p^2 - dq^2 = c$ pro nekonečně mnoho $p/q \in \mathbb{Q}$. Iracionalita $\sqrt{d}$ znamená, že $c \neq 0$. Existuje pouze konečně mnoho možností pro zbytky p, q modulo $|c|$, takže můžeme vybrat dva různé zlomky $p_1/q_1, p_2/q_2$ takové, že $p_1^2 - dq_1^2 = p_2^2 - dq_2^2 = c$ a $p_1 \equiv p_2$, $q_1 \equiv q_2$ modulo $|c|$. Uvažujme čísla a, b definovaná jako

$$a + b\sqrt{d} = \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} = \frac{(p_1 + q_1\sqrt{d})(p_2 - q_2\sqrt{d})}{c}.$$

Pak (a, b) je netriviální řešení Pellovy rovnice. ■

Struktura řešení Množina všech řešení Pellovy rovnice

$$R = \{a + b\sqrt{d} : a, b \in \mathbb{Z}, a^2 - db^2 = 1\}$$

tvoří multiplikativní abelovskou grupu s neutrálním prvkem $1 = 1 + 0\sqrt{d}$. Podgrupa kladných řešení

$$U = \{\alpha \in R : \alpha > 0\}$$

je generována nejmenším přirozeným řešením $\varepsilon = \varepsilon(d)$, tj. $U = \{\varepsilon^k : k \in \mathbb{Z}\}$. Grupa všech řešení $(R, \cdot)$ je izomorfní $(\mathbb{Z}, +) \times (\mathbb{Z}_2, +)$.

Věta 5.2. *Pokud zobecněná Pellova rovnice $x^2 - dy^2 = m$ má celočíselné řešení, pak má nekonečně mnoho celočíselných řešení.*

Důkaz. Pokud (a, b) je řešení $x^2 - dy^2 = m$ a (e, f) je řešení $x^2 - dy^2 = 1$, pak

$$g + h\sqrt{d} = (a + b\sqrt{d})(e + f\sqrt{d})$$

je také řešení $x^2 - dy^2 = m$. Násobením jednoho řešení $x^2 - dy^2 = m$ nekonečně mnoha řešeními $x^2 - dy^2 = 1$ získáme nekonečně mnoho řešení $x^2 - dy^2 = m$. ■

6 Fermatova věta: $x^4 + y^4 = z^2$ nemá netriviální řešení.

Věta 6.1. ***(Fermat, 17. století).*** *Diofantovská rovnice $x^4 + y^4 = z^2$ nemá řešení v $x, y, z \in \mathbb{N}$.*

Důkaz. Předpokládejme, že $(x, y, z) \in \mathbb{N}^3$ je řešení. Můžeme předpokládat, že x, y, z jsou nesoudělná. (Společný dělitel lze vydělit, čímž získáme řešení s nesoudělnými složkami.) Opět platí, že x, y mají různou paritu, a předpokládáme, že x je liché a y je sudé. Rovnici přepíšeme jako

$$y^4 = (z - x^2)(z + x^2).$$

Protože z, x jsou lichá, $(z, x) = 1$, a součet a rozdíl faktorů je $2z$ a $2x^2$, vidíme, že $(z - x^2, z + x^2) = 2$. To znamená, že

$$z - x^2 = 2a^4 \quad \text{a} \quad z + x^2 = 8b^4,$$

nebo jsou pravé strany prohozeny, a a, b jsou nesoudělná a a je liché. Odečtením rovnic dostaneme $x^2 = 4b^4 - a^4$, což je modulo 4 nemožné. Pravé strany tedy musí být prohozeny:

$$z - x^2 = 8b^4 \quad \text{a} \quad z + x^2 = 2a^4$$

a $x^2 = a^4 - 4b^4$, $z = a^4 + 4b^4$. Předchozí rovnici přepíšeme jako

$$4b^4 = (a^2 - x)(a^2 + x).$$

Opět platí, že $(a^2 - x, a^2 + x) = 2$. Nyní máme pouze jednu možnost, že každý faktor je dvojnásobkem bikvadrátu: $a^2 - x = 2c^4$, $a^2 + x = 2d^4$ s $c, d \in \mathbb{N}$. Sečtením obou rovnic dostaneme $a^2 = c^4 + d^4$. Počínaje řešením $(x, y, z) \in \mathbb{N}^3$ jsme sestrojili další řešení $(c, d, a) \in \mathbb{N}^3$ stejné rovnice. Ale $a < z$ (protože $z = a^4 + 4b^4$). Opakováním argumentu bychom mohli získat nekonečně mnoho přirozených řešení, jejichž třetí složky by tvořily nekonečnou ostře klesající posloupnost. To je v množině $\mathbb{N}$ nemožné, a dostáváme se do sporu. Tedy neexistuje řešení v přirozených číslech. ■

7 Lagrangeova věta o čtyřech čtvercích, geometrický důkaz.

Definice 7.1. (Mřížka). *Mřížka* $\Lambda = \Lambda(B) \in \mathbb{R}^n$ s bazí $B = \{v_1, \ldots, v_n\}$, kde $v_i \in \mathbb{R}^n$ jsou lineárně nezávislé vektory, je množina celočíselných lineárních kombinací vektorů z báze:

$$\Lambda = \left\{ \sum_{i=1}^{n} a_i v_i \;\middle|\; a_i \in \mathbb{Z} \right\}.$$

Objem značíme Vol *a je určen determinantem matice.*

Věta 7.1. ***(Minkowski).*** *Pokud $B \subseteq \mathbb{R}^n$ je konvexní těleso, které je ohraničené, středově symetrické a $\Lambda \subseteq \mathbb{R}^n$ je mřížka splňující podmínku $2^n \mathrm{Vol}(\Lambda) < \mathrm{Vol}(B)$, pak*

$$B \cap \Lambda \neq \{(0, 0, \ldots, 0)\},$$

tedy B obsahuje bod mřížky různý od původní.

Lemma 7.1. *Pro každé prvočíslo p má kongruence $a^2 + b^2 + 1 \equiv 0 \pmod{p}$ řešení $a, b \in \mathbb{Z}$.*

Důsledek 7.1. *Pro každé bezčtvercové číslo $n = p_1 p_2 \ldots p_r$ má kongruence $a^2 + b^2 + 1 \equiv 0 \pmod{n}$ řešení $a, b \in \mathbb{Z}$.*

Důkaz. (Náznak): Z Čínské věty o zbytcích. Dokážeme $a^2 + b^2 + 1 \equiv 0 \pmod{p_i}$ a tedy

$$a^2 + b^2 + 1 \equiv 0 \pmod{p_1 p_2 \ldots p_n = n}.$$

■

Věta 7.2. ***(Lagrange).*** *Pro $\forall n \in \mathbb{N}_0$ má rovnice $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ řešení $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.*

Důkaz. **(Geometrický).**
Stačí dokázat větu pouze pro bezčtvercová čísla n. Každé $n \in \mathbb{N}$ lze totiž zapsat ve tvaru $n = s^2 m$, kde m je bez čtverce, a pokud $m = \sum_{i=1}^{4} x_i^2$, pak $n = \sum_{i=1}^{4} (s x_i)^2$.
Nechť n je číslo bez čtverce. Pomocí *Důsledku 7.1.* vezmeme $a, b \in \mathbb{N}$ taková, že $a^2 + b^2 + 1$ je násobkem n. Budeme pracovat v $\mathbb{R}^4$ s mřížkou

$$\Lambda = \Lambda(\{u_1, u_2, u_3, u_4\}),$$

kde

$$u_1 = (n, 0, 0, 0), \quad u_2 = (0, n, 0, 0), \quad u_3 = (a, b, 1, 0), \quad u_4 = (b, -a, 0, 1).$$

Vektory u_i jsou z definice lineárně nezávislé a jelikož je báze dolní trojúhelníková matice, tak

$$\mathrm{Vol}(\Lambda) = \det(M(\Lambda)) = n^2.$$

Dále potřebujeme konvexní těleso B. Položíme $B = K(r)$, čtyřrozměrnou kouli se středem v počátku a poloměrem $r > 0$. Protože

$$\mathrm{Vol}(K(1)) = \frac{\pi^2}{2},$$

platí $\mathrm{Vol}(K(r)) = \frac{\pi^2 r^4}{2}$. Z podmínky $2^n\mathrm{Vol}(\Lambda) < \mathrm{Vol}(B)$ Minkowského věty máme:

$$\frac{\pi^2 r^4}{2} > 2^4 n^2 \iff r^2 > \frac{4\sqrt{2}}{\pi} n \approx (1.80063\ldots)n.$$

Zvolíme $r^2 = 1.9n$. Tím je splněna podmínka na objemy B (ostatní podmínky na B – konvexita a středová symetrie – jsou také splněny). Podle Minkowského věty existuje bod $z \in K(r)$:

$$z = \sum_{i=1}^{4} a_i u_i \in \Lambda,$$

kde ne všechny $a_i \in \mathbb{Z}$ jsou nulové. Vyjádřeno v souřadnicích,

$$0 < |z|^2 = (a_1 n + a_3 a + a_4 b)^2 + (a_2 n + a_3 b - a_4 a)^2 + a_3^2 + a_4^2 \leq r^2 < 2n.$$

Celé číslo $|z|^2$ je tedy součtem čtyř čtverců a leží v intervalu $[1, 2n-1]$. Navíc,

$$|z|^2 = a_3^2(a^2+b^2+1) + a_4^2(a^2+b^2+1) + 2a_3a_4ab - 2a_3a_4ab + n(\cdots)$$

ukazuje, že $|z|^2$ je násobkem n (díky a^2+b^2+1). Jediná možnost je $|z|^2 = n$, a tedy n je součtem čtyř čtverců. ■

8 Dokažte Chebyshevovy meze pro $p_i(x)$.

Věta 8.1. ***(Chebyshev, 1850).*** *Pro každé $x \geq 2$ existují kladné konstanty c_1, c_2 tak, že platí*

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x}.$$

Důkaz. **(Erdős, 1936)** Nechť $n \in \mathbb{N}$. Máme odhad:

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq 4^n,$$

protože $4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$ a $\binom{2n}{n}$ je největší z $2n+1$ binomických koeficientů v součtu. Chebyshevovy meze získáme zkombinováním tohoto odhadu s dalším odhadem středního binomického koeficientu:

$$\prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

Dolní mez plyne z toho, že ve jmenovateli zlomku

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

jsou všechna prvočísla z intervalu $(n, 2n]$, která nemohou být zrušena, protože ve jmenovateli se vyskytují pouze prvočísla $\leq n$.

Pro horní mez odhadneme nejvyšší mocninu prvočísla p, která dělí $\binom{2n}{n}$:

$$a = \sum_{i=1}^{\infty} \lfloor 2n/p^i \rfloor - 2\lfloor n/p^i \rfloor.$$

To plyne z obecného vzorce

$$b = \sum_{i \geq 1} \lfloor m/p^i \rfloor$$

pro nejvyšší exponent b, pro který p^b dělí $m!$. Každý sčítanec počítá násobky p^i mezi čísly $1, 2, \ldots, m$. Protože pro každé $\alpha \in \mathbb{R}$ platí $0 \leq \lfloor 2\alpha \rfloor - 2\lfloor \alpha \rfloor \leq 1$, dostáváme:

$$a \leq \sum_{i, p^i \leq 2n} 1.$$

Tedy $p^a \leq 2n$. Překvapivě prvočíselné mocniny ve faktorizaci $\binom{2n}{n}$ nejsou větší než faktorizace samotného $2n$. Každé prvočíslo ve faktorizaci je $\leq 2n$, čímž dostáváme:

$$\prod_{n < p \leq 2n} p \leq (2n)^{\pi(2n)}.$$

Spojením obou odhadů dostáváme:

$$(2n)^{\pi(2n)} \geq \frac{4^n}{2n+1}.$$

Po zlogaritmování dostáváme:

$$\pi(2n) \geq \frac{2n \log 2}{\log(2n)} - \frac{\log(2n+1)}{\log(2n)}.$$

A pro $n \geq 2$ platí:

$$\pi(2n-1) = \pi(2n) \geq \frac{2n \log 2}{\log(2n)} - 2 \geq \frac{(2n-1)\log 2}{\log(2n-1)} - 2.$$

To dává dolní mez Chebyshevovy věty.
Horní mez získáme tak, že sečteme logaritmy prvočísel na intervalech $(2^k, 2^{k+1}]$. Pro největší $m \in \mathbb{N}$ takové, že $2^m \leq x$, platí:

$$\sum_{p \leq x} \log p \leq \sum_{k=0}^{m} \sum_{2^k < p \leq 2^{k+1}} \log p.$$

Použitím předchozího odhadu dostáváme:

$$\sum_{p \leq x} \log p \leq (2^0 + 2^1 + \cdots + 2^m) \log 4 < 2^{m+1} \log 4.$$

Protože $2^{m+1} > x$, máme:

$$\sum_{p \leq x} \log p \leq (2 \log 4) x.$$

Odtud dostáváme:

$$(2 \log 4) x \geq \sum_{p \leq x} \log p \geq \sum_{\sqrt{x} < p \leq x} \log p.$$

Použitím dolní meze dostáváme:

$$\sum_{\sqrt{x} < p \leq x} \log p \geq (\pi(x) - \pi(\sqrt{x})) \log \sqrt{x} \geq (\pi(x) - \sqrt{x}) \log \sqrt{x}.$$

Tedy

$$\pi(x) \leq \frac{(2 \log 4) x}{\log \sqrt{x}} + \sqrt{x}.$$

Tím je dokázána horní mez a celá věta. ■

9 Uveďte několik důkazů o nekonečnosti prvočísel.

Definice 9.1. ***(Funkce počítající prvočísla)****:* Hodnota funkce $\pi(x)$ pro $x \in \mathbb{R}$ je definována jako počet prvočísel nepřevyšujících x:

$$\pi(x) = \#\{p : p \leq x\}.$$

Například $\pi(-3) = \pi(1.9) = 0$ a $\pi(18) = 7$.

Věta 9.1. *Existuje nekonečně mnoho prvočísel.*

Důkaz. **(Eukleidův důkaz)** Každé $n \in \mathbb{N}$ větší než 1 je dělitelné nějakým prvočíslem (vezměme nejmenšího dělitele n většího než 1). Předpokládejme, že prvočísel je konečně mnoho: $p_1, p_2, \ldots, p_r$. Zvažme číslo

$$N = p_1 p_2 \ldots p_r + 1.$$

Nechť p je prvočíselný dělitel čísla N. Pak nutně $p = p_i$ pro nějaké i, tedy p_i dělí také 1, což je spor. Proto musí existovat nekonečně mnoho prvočísel. ■

Věta 9.2. *Existuje nekonečně mnoho prvočísel.*

Důkaz. **(Goldbachův důkaz)** Definujeme rekurentní posloupnost $(G_n)_{n\geq 0}$ jako

$$G_0 = 2, \quad G_n = G_0 G_1 \ldots G_{n-1} + 1 \text{ pro } n \in \mathbb{N}.$$

Hodnoty prvních členů jsou:

$$G_0 = 2, \quad G_1 = 3, \quad G_2 = 7, \quad G_3 = 43, \ldots$$

Je zřejmé, že pokud $m < n$, pak G_m a G_n jsou nesoudělná čísla (protože G_m dělí $G_n - 1$). Volbou libovolného prvočíselného dělitele každého G_n dostáváme nekonečně mnoho různých prvočísel. ■

Věta 9.3. *Existuje nekonečně mnoho prvočísel.*

Důkaz. **(Eulerův důkaz, první varianta)** Použijeme Eulerovu identitu:

$$\prod_p \frac{1}{1 - 1/p^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

pro každé reálné $s > 1$. Levá strana je součinem geometrických řad a pravá strana harmonickou řadou. Předpokládejme, že prvočísel je konečně mnoho: $p_1, \ldots, p_r$. Pak při limitě $s \to 1^+$ levá strana konverguje k

$$\frac{1}{(1 - p_1^{-1})(1 - p_2^{-1}) \ldots (1 - p_r^{-1})}.$$

Avšak pravá strana diverguje, což je spor. Proto musí existovat nekonečně mnoho prvočísel. ■

Věta 9.4. *Existuje nekonečně mnoho prvočísel.*

Důkaz. **(Erdősův důkaz)** Každé $n \in \mathbb{N}$ lze jednoznačně zapsat jako $n = r^2 s$, kde $r, s \in \mathbb{N}$ a s je bezčtvercové číslo. Pokud $n \leq N$, pak r nabývá nejvýše $\sqrt{N}$ hodnot a s nabývá nejvýše $2^{\pi(N)}$ hodnot (protože s lze tvořit jako součin různých prvočísel $\leq N$). Musí tedy platit:

$$\sqrt{N} \cdot 2^{\pi(N)} \geq N.$$

Po úpravě dostáváme odhad:

$$\pi(N) \geq \frac{1}{2} \log_2 N.$$

Z toho plyne, že $\pi(x) \to \infty$ pro $x \to \infty$, což dokazuje nekonečnost prvočísel. ■

10 Vysvětlete teorii kvadratických zbytků a zákona reciprocity.

Definice 10.1. (Kvadratický zbytek). Nechť $p > 2$ je liché prvočíslo a $a \in \mathbb{Z}$. Říkáme, že a je *kvadratický zbytek modulo p*, pokud kongruence

$$x^2 \equiv a \pmod{p}$$

má řešení $x \in \mathbb{Z}$. Pokud řešení neexistuje, nazýváme a **kvadratický nezbytek** modulo p.

Příklad: Pro $p = 11$ jsou kvadratické zbytky čísla $1, 3, 4, 5, 9$, protože $1^2 \equiv 1, \ldots, 9^2 \equiv 4 \pmod{11}$. Ostatní čísla $(2, 6, 7, 8, 10)$ jsou kvadratické nezbytky.

Tvrzení 10.1. *Pro každé liché prvočíslo $p > 2$ existuje právě $\frac{p-1}{2}$ kvadratických zbytků a $\frac{p-1}{2}$ kvadratických nezbytků.*

Definice 10.2. (Legendreův symbol). Pro liché prvočíslo $p > 2$ a $a \in \mathbb{Z}$ definujeme *Legendreův symbol* jako:

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

Tvrzení 10.2. *Nechť $p > 2$ je liché prvočíslo a $a, b \in \mathbb{Z}$:*

1. ***Kongruence:*** *Pokud $a \equiv b \pmod{p}$, pak $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. ***Eulerovo kritérium:*** $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
3. ***Multiplikativita:*** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Lemma 10.1. ***(Gaussovo).*** *Pro liché prvočíslo $p > 2$ a $a \in \mathbb{Z}$ nesoudělné s p definujeme:*

$$m(a) = \#\left\{k \;\middle|\; 1 \le k \le \frac{p-1}{2}, \quad ka \equiv m_k \pmod{p},\ m_k < 0\right\}.$$

Potom platí:

$$\left(\frac{a}{p}\right) = (-1)^{m(a)}.$$

Příklad: Pro $p = 17$ a $a = 6$ dostaneme $m(6) = 3$, tedy $\left(\frac{6}{17}\right) = (-1)^3 = -1$.

Tvrzení 10.3. ***(Doplňky k zákonu reciprocity).*** *Nechť $p > 2$ je liché prvočíslo. Potom:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \textit{pokud } p \equiv 1 \pmod{4}, \\ -1 & \textit{pokud } p \equiv 3 \pmod{4}. \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \textit{pokud } p \equiv 1 \textit{ nebo } 7 \pmod{8}, \\ -1 & \textit{pokud } p \equiv 3 \textit{ nebo } 5 \pmod{8}. \end{cases}$$

Věta 10.1. ***(Gauss, 1796).*** *Pro dvě různá lichá prvočísla p a q platí zákon kvadratické reciprocity:*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right) = \begin{cases} +\left(\frac{q}{p}\right) & \textit{pokud } p = 4m+1 \textit{ nebo } q = 4n+1, \\ -\left(\frac{q}{p}\right) & \textit{pokud } p = 4m+3 \textit{ nebo } q = 4n+3. \end{cases}$$

Důkaz. Důkaz je založen na *Gaussově lemmatu* a *aritmetických vlastnostech* celých čísel. Klíčovým krokem je vyjádření Legendreova symbolu pomocí sumy:

$$\left(\frac{a}{p}\right) = (-1)^{S(p,a)},$$

kde $S(p,a)$ je počet celočíselných bodů v určité oblasti. Pomocí této sumy a geometrických úvah se dokáže, že:

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

■

Příklad: Pro $p = 5$ a $q = 7$ platí: $\left(\frac{5}{7}\right) = (-1)^{\frac{(5-1)(7-1)}{4}}\left(\frac{7}{5}\right) = (-1)^6\left(\frac{7}{5}\right) = \left(\frac{7}{5}\right)$.
Dále $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$, tedy $\left(\frac{5}{7}\right) = -1$.

11 Uveďte a dokažte Eulerovu identitu pro celočíselné partitions.

Definice 11.1. (Partitions). Vyjádření n jako součtu přirozených čísel, v němž pořadí součtů není důležité, se nazývá *partition n*.
Jejich počet označujeme $p(n)$ a výrazem $p(n,k)$ označujeme počet rozdělení n na k částí.

Věta 11.1. ***(Eulerova identita).*** *Pro každé $n \in \mathbb{N}$ se počet rozkladů $r(n)$ čísla n na navzájem různé části stejný jako počet rozkladů $l(n)$ čísla n na liché části (které se mohou opakovat).*

Důkaz. **(1. generující funkce.)** Počet rozkladů $l(n)$ odpovídá počtu způsobů, jak rozdělit n pouze na liché části, tedy $l(n) = p(n, \{1,3,5,\dots\})$, což lze vyjádřit generující funkcí:

$$\sum_{n\geq 0} l(n)x^n = \frac{1}{(1-x)(1-x^3)(1-x^5)\dots}$$

Tento výraz lze upravit jako:

$$\frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8)\dots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\dots}$$

což, protože platí $\frac{(1-x^{2k})}{(1-x^k)} = 1 + x^k$, se dá upravit na

$$(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots = \prod_{k\geq 1}(1+x^k),$$

což je přesně generující funkce pro počet rozkladů $r(n)$ s různými částmi:

$$\sum_{n\geq 0} r(n)x^n = \prod_{k\geq 1}(1+x^k) = \sum_{n\geq 0} l(n)x^n.$$

Porovnáním obou funkcí dostáváme $l(n) = r(n)$ pro každé n. ■

Důkaz. **(2. bijektivní.)** Konstruujeme bijekci mezi rozklady n na navzájem různé části a rozklady n na liché části. To ukáže, že jich je stejně mnoho.
Nechť κ je rozklad čísla n na navzájem různé části a a je jedna z jeho částí. Zapíšeme ji ve tvaru

$$a = 2^b c,$$

kde $b \in \mathbb{N}_0$ a $c \in \mathbb{N}$ je liché (tento zápis a je jednoznačný). Poté nahradíme a za 2^b částí c. Provedeme tento krok pro každou část κ a získáme rozklad λ čísla n na pouze liché části.
Naopak, nechť λ je rozklad čísla n na liché části a a je jedna z jeho částí. Spočítáme počet jejích výskytů v λ, označíme jej m. Číslo m lze vyjádřit (jednoznačně) jako součet různých mocnin dvou:

$$m = 2^{u_1} + 2^{u_2} + \cdots + 2^{u_r}$$

pro nějaká celá čísla $u_1 > u_2 > \cdots > u_r \geq 0$ (to je binární rozvoj m). Nahradíme výskyty čísla a v λ, tedy $a + a + \cdots + a$ (m-krát), částmi

$$2^{u_1}a + 2^{u_2}a + \cdots + 2^{u_r}a.$$

Provedeme tento krok pro každou část λ a získáme rozklad κ čísla n na navzájem různé části (části jsou navzájem různé, protože zápis „mocnina dvou × liché číslo“ je jednoznačný).
Obě definované transformace jsou vzájemně inverzní a určují požadovanou bijekci.

■

12 Uveďte a dokažte Cohenovu–Remmelovu větu o identitách pro celočíselné oddíly a uveďte některé její důsledky.

Věta 12.1. ***(Cohen–Remmel).*** *Nechť $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \ldots)$ a $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \ldots)$ jsou dvě nekonečné posloupnosti multimnožin (částí), které pro každou konečnou množinu $I \subset \mathbb{N}$ splňují podmínku*

$$\left\| \bigcup_{i \in I} \mathcal{A}_i \right\| = \left\| \bigcup_{i \in I} \mathcal{B}_i \right\|.$$

Pak pro každé $n \in \mathbb{N}$ platí:

$$\#\{\lambda \vdash n : \lambda \not\supset \mathcal{A}_i \text{ pro } i = 1, 2, \ldots\} = \#\{\lambda \vdash n : \lambda \not\supset \mathcal{B}_i \text{ pro } i = 1, 2, \ldots\},$$

tedy počet oddílů čísla n, které neobsahují žádný oddíl z posloupnosti $\mathcal{A}$, je roven počtu oddílů čísla n, které neobsahují žádný oddíl z posloupnosti $\mathcal{B}$.

Důkaz. Nechť $n \in \mathbb{N}$ je pevné a U je množina všech oddílů λ čísla n. Definujme

$$X_i = \{\lambda \in U : \lambda \supset \mathcal{A}_i\} \quad \text{a} \quad Y_i = \{\lambda \in U : \lambda \supset \mathcal{B}_i\}.$$

Pro konečnou množinu indexů $1 \leq i_1 < i_2 < \ldots < i_k$ uvažujme množiny

$$R = X_{i_1} \cap X_{i_2} \cap \ldots \cap X_{i_k} \quad \text{a} \quad S = Y_{i_1} \cap Y_{i_2} \cap \ldots \cap Y_{i_k}.$$

Podle předchozího pozorování platí

$$R = \{\lambda \in U : \lambda \supset \mathcal{A}_{i_1} \cup \ldots \cup \mathcal{A}_{i_k}\}$$

a

$$S = \{\lambda \in U : \lambda \supset \mathcal{B}_{i_1} \cup \ldots \cup \mathcal{B}_{i_k}\}.$$

Pro každý oddíl $\lambda \in R$ definujme oddíl

$$\lambda' = (\lambda - \mathcal{A}_{i_1} \cup \ldots \cup \mathcal{A}_{i_k}) + \mathcal{B}_{i_1} \cup \ldots \cup \mathcal{B}_{i_k},$$

který leží v S. Podobně pro každý oddíl $\kappa \in S$ definujme oddíl

$$\kappa' = (\kappa - \mathcal{B}_{i_1} \cup \ldots \cup \mathcal{B}_{i_k}) + \mathcal{A}_{i_1} \cup \ldots \cup \mathcal{A}_{i_k},$$

který leží v R. (Podmínka na posloupnosti $\mathcal{A}$ a $\mathcal{B}$ zajišťuje, že norma multimnožiny se nezmění, když odečteme $\mathcal{A}_i$ a přidáme odpovídající $\mathcal{B}_i$.) Tyto zobrazení $\lambda \mapsto \lambda'$ a $\kappa \mapsto \kappa'$ jsou vzájemně inverzní a vytvářejí bijekci mezi R a S. Tedy pro každou konečnou množinu indexů platí $|R| = |S|$. Podle principu inkluze a exkluze (PIE) dostáváme

$$|U \setminus (X_1 \cup X_2 \cup \ldots)| = |U \setminus (Y_1 \cup Y_2 \cup \ldots)|,$$

což jsme chtěli dokázat. ■

Důsledky Cohenovy–Remmelovy věty

Existuje jednoduchá metoda, jak konstruovat netriviální dvojice posloupností $\mathcal{A}$ a $\mathcal{B}$, které splňují podmínku věty. Pokud jsou multinásobky $\mathcal{A}_1, \ldots, \mathcal{A}_k$ vzájemně disjunktní (tj. $\mathcal{A}_i \cap \mathcal{A}_j = \emptyset$ pro $i \neq j$), pak sjednocení je rovno součtu a norma sjednocení je součtem norem. Pokud jsou tedy $\mathcal{A}$ a $\mathcal{B}$ posloupnosti po dvou disjunktních multinásobků, pak podmínka je splněna právě tehdy, když $\|\mathcal{A}_i\| = \|\mathcal{B}_i\|$ pro každé $i \in \mathbb{N}$. Tuto situaci nazýváme *disjunktním splněním podmínky.*
Následují čtyři příklady aplikace této věty:

1. **Glaisherova identita:** Pro $d \in \mathbb{N}$, $d \geq 2$, uvažujme

$$\mathcal{A} = (\{d\}, \{2d\}, \{3d\}, \ldots) \quad \text{a} \quad \mathcal{B} = (\{1, 1, \ldots, 1\}, \{2, 2, \ldots, 2\}, \{3, 3, \ldots, 3\}, \ldots),$$

kde v $\mathcal{B}$ jsou všechny násobnosti rovny d. *Každé číslo n má stejný počet oddílů na části, které nejsou dělitelné d, jako oddílů, ve kterých se žádná část neopakuje více než $d-1$ krát.* Pro $d = 2$ se jedná o Eulerovu identitu.

– Uvažujme

$$\mathcal{A} = (\{1\}, \{4\}, \{9\}, \{16\}, \ldots) \quad \text{a} \quad \mathcal{B} = (\{1\}, \{2, 2\}, \{3, 3, 3\}, \{4, 4, 4, 4\}, \ldots).$$

Každé číslo n má stejný počet oddílů, ve kterých žádná část není čtverec, jako oddílů, ve kterých se každá část m opakuje nejvýše $m - 1$ krát.

2. **Schurova identita:** Uvažujme

$$\mathcal{A} = (\{2\}, \{3\}, \{4\}, \{6\}, \{8\}, \{9\}, \{10\}, \{12\}, \{14\}, \ldots)$$

a

$$\mathcal{B} = (\{1, 1\}, \{3\}, \{2, 2\}, \{6\}, \{4, 4\}, \{9\}, \{5, 5\}, \{12\}, \{7, 7\}, \ldots).$$

Každé číslo n má stejný počet oddílů na části $\equiv \pm 1 \pmod 6$ jako oddílů na různé části $\equiv \pm 1 \pmod 3$.

– Uvažujme

$$\mathcal{A} = (\{1, 1, 1, 1\}, \{1, 1, 2, 2\}, \{2, 2, 2, 2\}, \{2, 2, 3, 3\}, \{3, 3, 3, 3\}, \ldots)$$

a

$$\mathcal{B} = (\{2, 2\}, \{2, 4\}, \{4, 4\}, \{4, 6\}, \{6, 6\}, \ldots).$$

Každé číslo n má stejný počet oddílů, ve kterých se části opakují nejvýše třikrát a ve kterých se v každých dvou po sobě jdoucích částech jedna z nich neopakuje, jako oddílů, ve kterých se sudé části liší alespoň o 4 (a neopakují se, liché části nejsou omezeny).