Domašov nad Bystřicí

Sborník, podzim 2012

Michael „Majkl“ Bílý
Filip Hlásek
Anča Chejnovská
Jakub „Roman“ Klemsa
Peter „πtr“ Korcsok
Kuba Krásenský
Vít „Vejtek“ Musil
Mirek Olšák
Alexander „Olin“ Slávik
Helča Svobodová
Viktor Szabados
Martina Vaváčková
Lukáš Zavřel

AUTOŘI: Michael „Majkl“ Bílý, Filip Hlásek, Anča Chejnovská, Jakub „Roman“ Klemsa, Peter „πtr“ Korcsok, Kuba Krásenský, Vít „Vejtek“ Musil, Mirek Olšák, Alexander „Olin“ Slávik, Helča Svobodová, Viktor Szabados, Martina Vaváčková, Lukáš Zavřel
EDITOR: Alexander „Olin“ Slávik
vydání první, náklad 45 výtisků
listopad 2012
Díky za pomoc všem, kterým je za co děkovat.

Příklady z teorie čísel

Michael „Majkl“ Bílý

Abstrakt. Příspěvek ukazuje různorodé těžké úlohy z teorie čísel využívající ne zcela standardní známé věty.

Nejprve příklad na práci s odhady.

Příklad 1. Jakých hodnot nabývá posloupnost

$$a_n = \left\lfloor n + \sqrt{n} + \frac{1}{2} \right\rfloor ?$$

Pak procvičení práce se zbytky.

Příklad 2. Nechť $t(k)$ je největší lichý dělitel k. Najděte všechna přirozená a taková, že existuje přirozené n, pro které jsou všechny výrazy

$$t(n+a) - t(n),\ t(n+a+1) - t(n+1),\ \ldots,\ t(n+2a-1) - t(n+a-1)$$

dělitelné 4.

Tady budeme potřebovat trochu teorie o cyklotomických polynomech – pokud $3 \nmid n$, pak $x^2 + x + 1 \mid x^{2n} + x^n + 1$.

Příklad 3. Pokud je $4^n + 2^n + 1$ prvočíslo, pak je n mocnina trojky. Dokažte.

Věta 4. *Pro libovolné číslo $k \in \mathbb{N}$ existuje v posloupnosti 2^n člen ve tvaru $\overline{k\ldots}$.*

K důkazu této věty budeme potřebovat známé tvrzení.

Tvrzení 5. *Množina $\{\{\alpha n\} \mid n \in \mathbb{N}\}$ je hustá na intervalu $\langle 0, 1\rangle$, pokud je α iracionální číslo.*

Poznámka 6. $\{x\}$ značíme desetinnou část čísla x, tedy $x - \lfloor x \rfloor$.

Teď už můžeme snadno vyřešit následující úlohu.

Příklad 7. Na tabuli je napsáno číslo 2010. V každém kroku můžeme buď číslo vynásobit dvěma, nebo umazat poslední cifru. Dokažte, že

(a) po konečně mnoha krocích může být na tabuli číslo 2008,
(b) po konečně mnoha krocích může být na tabuli libovolné číslo.

Zde budeme potřebovat tvrzení, že řád prvku mod p dělí $p - 1$.

Příklad 8. Buď p prvočíslo a n, q přirozená čísla taková, že $q \mid (n+1)^p - n^p$. Ukažte, že $p \mid q - 1$.

V dalším příkladu budeme potřebovat Čínskou větu o zbytcích a Dirichletovu větu.

Příklad 9. Nazvěme n *suprové*, pokud existují a, b, c tak, že

$$n = (b,c)(a,bc) + (c,a)(b,ca) + (a,b)(c,ab).$$

Dokažte, že

(a) existuje 2011 po sobě jdoucích suprových čísel,
(b) existuje libovolně mnoho po sobě jdoucích suprových čísel.

Zde (a,b) značí největší společný dělitel čísel a, b.

Tady si půjčíme těleso velikosti 4.

Příklad 10. Pokud existuje posloupnost a_n přirozených čísel, splňujících

$$a_n = \frac{a_{n-1} + n^k}{n},$$

pak $3 \mid k - 2$.

V obou následujících příkladech využijeme vzorečku pro níže definovanou funkci τ.

Příklad 11. Nechť $\tau(n)$ značí počet dělitelů n. Najděte řešení rovnice

$$\frac{\tau(n^2)}{\tau(n)} = m$$

pro celá čísla m, n. (IMO-98-3)

Příklad 12. Pokud $\tau(a) = \tau(b)$ a $\tau(a^2) = \tau(b^2)$, platí $\tau(a^3) = \tau(b^3)$? (MEMO-2012-T8)

Následují dva příklady na Pellovu rovnici.

Příklad 13. Pokud $x(y+1)$ a $y(x+1)$ jsou čtverce, pak x nebo y je čtverec. Dokažte.

Příklad 14. Dokažte, že existuje nekonečně mnoho n takových, že $p = nr$, kde p je polovina obvodu trojúhelníku s celočíselnými stranami a r je poloměr kružnice tomuto trojúhelníku vepsané.

Jeden příklad na Lifting The Exponent lemma.

Příklad 15. Najděte všechny dvojice přirozených čísel (m,n), které splňují

$$m^2 + 2 \cdot 3^n = m(2^{n+1} - 1).$$

Zajímavé využití Hallovy věty.

Příklad 16. Přirozená čísla k a n splňují $k > n!$. Dokažte, že existují po dvou různá prvočísla $p_1, p_2, \ldots, p_n$, které jsou postupně dělitele čísel $k+1, k+2, \ldots, k+n$.

Na závěr příklad na jednu triviálnější větu.

Věta 17. (Chicken McNugget theorem) *Nechť a, b jsou nesoudělná přirozená čísla, pak všechna čísla větší než $(a-1)(b-1)$ se dají vyjádřit ve tvaru $ka+lb$ pro nějaká přirozená k, l.*

Příklad 18. Mějme n takové, že $3 \nmid n$. Dokažte, že existuje přirozené číslo m takové, že $\forall k > m$ lze k vyjádřit jako součet cifer nějakého násobku n.

Goniometrie

MICHAEL „MAJKL“ BÍLÝ

ABSTRAKT. Příspěvek si klade za cíl ukázat jak základní, tak i složitější vlastnosti goniometrických funkcí nutné k jejich úplnému porozumění. Představíme některá různá zavedení goniometrických funkcí a některé známé věty, které buď s goniometrií souvisí, nebo ji využívají ke svému důkazu.

Goniometrické funkce jste všichni už jistě poznali na středních školách při základním kurzu pravoúhlého trojúhelníka. Toto zavedení je praktické a dají se z něj ihned usuzovat některé jejich vlastnosti. Nelze tak ale spočítat hodnotu funkce v záporných hodnotách, nebo pokud je úhel větší než $90°$. Někteří se pak už dostali i k zavedení jednotkové kružnice a k oné záhadné definici goniometrických funkcí přes ni. Na vysoké škole se pak už jen několik lidí dostává k definicím, kterým nejde vůbec rozumět, ale nakonec z nich opravdu vypadne vše potřebné.

Goniometrická funkce přiřazuje jistému úhlu číslo. Naskýtá se tedy otázka, co je to úhel.

První definice, à la pravoúhlý trojúhelník

Definice. (Úhel) Mějme body A, $B \neq A$ a $C \neq A$. Úhel $\sphericalangle BAC$ je číslo rovné délce oblouku na jednotkové kružnici se středem v bodě A, kterou vytne polopřímka AB při otočení na polopřímku AC proti směru hodinových ručiček.

Pokud si kružnici rozdělíme na 360 dílků, pak můžeme místo délky oblouků zaznamenávat počet dílků, které musí polopřímka AB urazit.

Jednotkám, které vyjdou při prvním způsobu, se říká *radiány*, v druhém pak *stupně*. Celá jednotková kružnice měří 2π, a proto budou všechny úhly měřit méně než 2π radiánů a 360 stupňů. Jak ale víme, chceme definovat naše funkce i pro jiné úhly. Proto se některé úhly ztotožňují – platí $\alpha + k \cdot 2\pi \approx \alpha$, kde $\alpha \in \langle 0, 2\pi)$ a $k \in \mathbb{Z}$. Obdobně pro stupně.

Všimněte si, že teď už může úhel nabývat libovolných reálných hodnot, přičemž číslo k vyjadřuje, kolikrát musí polopřímka AB z naší definice oběhnout navíc kolem celé kružnice (v případě záporných hodnot pak po směru hodinových ručiček).

Teď, když už víme, co je úhel, se můžeme pustit do práce.

Definice. Nechť ABC je pravoúhlý trojúhelník s pravým úhlem při vrcholu C, úhel u vrcholu A označme α. Pak při standardním značení stran trojúhelníka definujeme

$$\sin\alpha := \frac{b}{c}, \qquad \cos\alpha := \frac{a}{c},$$
$$\operatorname{tg}\alpha := \frac{\sin\alpha}{\cos\alpha} = \frac{b}{a}, \qquad \operatorname{cotg}\alpha := \frac{1}{\operatorname{tg}\alpha} = \frac{\cos\alpha}{\sin\alpha} = \frac{a}{b}.$$

Protože úhel α je větší než 0, ale menší než pravý, definovali jsme naše goniometrické funkce pouze pro úhly z intervalu $(0, \frac{\pi}{2})$, respektive $(0, 90°)$. To nám zatím bude stačit.

Úloha. (Na zamyšlení) Pokud ještě označíme úhel při vrcholu B jako β, co můžeme říct o $\sin\beta$, $\cos\beta$, $\operatorname{tg}\beta$ a $\operatorname{cotg}\beta$?

Úloha. Dokažte

$$\sin^2\alpha + \cos^2\alpha = 1,$$
$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha,$$
$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\beta\sin\alpha.$$

A co takhle něco obdobného pro tg?

Hint. Zkuste namalovat obrázek s pravoúhlými trojúhelníky, kde budou vystupovat všechny zmiňované úhly.

Úloha. Odvoďte vzorce pro dvojnásobný úhel.

Úloha. Z vhodných obrázků pravoúhlých trojúhelníků odvoďte hodnoty goniometrických funkcí $\frac{\pi}{3}$, $\frac{\pi}{4}$ a $\frac{\pi}{6}$. Jaké další hodnoty jsme schopni odvodit?

Úloha. Ukažte, že $\sin\alpha(1+\cos 2\alpha) = \sin 2\alpha\cos\alpha$.

To je všechno moc pěkné, ale teď se chceme osvobodit od toho hrozného omezení pravým úhlem. Proto si zavedeme kartézský systém souřadnic a podíváme se na jednotkovou kružnici kolem jeho středu.

Druhá definice, à la jednotková kružnice

Definice. Mějme standardní systém souřadnic Oxy a sestrojme kružnici jednotkového poloměru se středem v O. Označme A bod $[1,0]$ a X libovolný bod $[x,y]$ na naší kružnici. Dále označme $\alpha := |\sphericalangle AOX|$. Pak definujeme:

$$\sin\alpha := y, \qquad \cos\alpha := x,$$
$$\operatorname{tg}\alpha := \frac{\sin\alpha}{\cos\alpha}, \qquad \operatorname{cotg} := \frac{\cos\alpha}{\sin\alpha}.$$

Díky ztotožnění, které jsme provedli na začátku, máme teď goniometrické funkce definované pro všechna reálná čísla. Jak nám ale pomůže veškeré to dokazování z první definice?

Úloha. Jak souvisí první definice s druhou? Platí všechny vztahy z první definice i pro všechny reálné úhly? Dokažte.

Hint. Stačí v kružnici hledat pravoúhlé trojúhelníky a pak vhodně využít toho, že naše kružnice se zachová při různých otočeních a osových symetriích.

Úloha. Jaký je definiční obor funkcí tg a cotg?

Úloha. Pro $\alpha \in (0, \frac{\pi}{2})$ dokažte

$$\sin\alpha < \alpha < \operatorname{tg}\alpha.$$

Úloha. Teď už snadno odvodíme

$$\begin{aligned}\sin(\alpha-\beta) &= \sin\alpha\cos\beta - \sin\beta\cos\alpha,\\ \cos(\alpha-\beta) &= \cos\alpha\cos\beta + \sin\beta\sin\alpha.\end{aligned}$$

Dokázali byste odtud odvodit vzorce pro součty a rozdíly goniometrických funkcí?

$$\begin{aligned}\sin\alpha + \sin\beta &= 2\sin\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2},\\ \sin\alpha - \sin\beta &= 2\sin\frac{\alpha-\beta}{2}\cos\frac{\alpha+\beta}{2},\\ \cos\alpha + \cos\beta &= 2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2},\\ \sin\alpha - \sin\beta &= -2\sin\frac{\alpha+\beta}{2}\sin\frac{\alpha-\beta}{2}.\end{aligned}$$

Odvoďte podobná tvrzení pro tangens a kotangens.

Trochu méně známé vzorce, ale podle mě ty nejužitečnější:

Tvrzení.

$$\begin{aligned}\sin\alpha\sin\beta &= \frac{1}{2}[\cos(\alpha-\beta) - \cos(\alpha+\beta)],\\ \cos\alpha\cos\beta &= \frac{1}{2}[\cos(\alpha-\beta) + \cos(\alpha+\beta)],\\ \sin\alpha\cos\beta &= \frac{1}{2}[\sin(\alpha-\beta) - \sin(\alpha+\beta)].\end{aligned}$$

Opět odvoďte obdobná tvrzení pro tangens a kotangens.

Úloha. Dokažte tyto vlastnosti goniometrických funkcí:

(i) Funkce sinus a kotangens jsou liché a periodické.
(ii) Funkce kosinus a tangens jsou sudé a periodické.

Jaké jsou jejich periody?

Pomocí rotací a symetrií ukažte:

$$\begin{aligned} \sin(\alpha \pm \pi) &= -\sin\alpha, & \cos(\alpha \pm \pi) &= -\cos\alpha, \\ \sin(\alpha + \tfrac{\pi}{2}) &= \cos\alpha, & \cos(\alpha + \tfrac{\pi}{2}) &= -\sin\alpha, \\ \sin(\alpha - \tfrac{\pi}{2}) &= -\cos\alpha, & \cos(\alpha - \tfrac{\pi}{2}) &= \sin\alpha, \\ \sin(\pi - \alpha) &= \sin\alpha, & \cos(\pi - \alpha) &= -\cos\alpha. \end{aligned}$$

Úloha. Nechť $a, b \in \mathbb{R}^+$. Dokažte, že rovnice $\sin x + a\cos x = b$ má řešení právě tehdy, když $a^2 - b^2 + 1 \geq 0$.

Předpokládejme, že $\sin x + a\cos x = b$. Vyjádřete $|a\sin x - \cos x|$ pouze pomocí a a b.

Trocha trigonometrie

Následuje několik slíbených tvrzení bez důkazu. Budeme vždy hovořit o trojúhelníku ABC se stranami a, b, c, úhly α, β, γ a poloměrem kružnice opsané R.

Tvrzení. (Obsah trojúhelníka) *Obsah trojúhelníka je*

$$S = \frac{1}{2}ab\sin\gamma = \frac{1}{2}ac\sin\beta = \frac{1}{2}bc\sin\alpha.$$

Věta. (Sinová věta) *Platí*

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R.$$

Tvrzení. (O ose úhlu) *Osa úhlu u vrcholu A protne stranu a v bodě D. Platí*

$$\frac{|AB|}{|AC|} = \frac{|BD|}{|CD|}.$$

Věta. (Cevova věta) *Nechť jsou D, E, F body na přímkách určených postupně stranami a, b, c, různé od vrcholů trojúhelníku. Pak přímky AD, BE, CF procházejí jedním bodem tehdy a jen tehdy, když platí*

$$\frac{|BD|}{|CD|} \cdot \frac{|CE|}{|AE|} \cdot \frac{|AF|}{|BF|} = 1.$$

Věta. (Kosinová věta) *Platí*

$$a^2 = b^2 + c^2 - 2bc\cos\alpha$$

a cyklické záměny.

Věta. (Stewartova věta) *Nechť D je bod na straně a. Pak*

$$a(|AD|^2 + |BD| \cdot |CD|) = c^2|CD| + b^2|BD|.$$

Tvrzení. (Brahmaguptův vzorec) *Mějme čtyřúhelník $ABCD$ se stranami a, b, c, d. Označme $s = \frac{a+b+c+d}{2}$. Pak obsah čtyřúhelníku je*

$$\sqrt{(s-a)(s-b)(s-c)(s-d)}.$$

Komplexní čísla

Definice. (Komplexní číslo a polární souřadnice) Pro každý bod roviny $A = [a, b]$ existuje právě jedno číslo $\varphi \in \langle 0, 2\pi)$ takové, že $\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}$ a $\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}$. To udává úhel, který svírá polopřímka OA s kladnou poloosou x. Každý bod je tedy jednoznačně určen takovýmto úhlem φ a vzdáleností od počátku $\sqrt{a^2+b^2}$. Těmto dvěma číslům říkáme polární souřadnice bodu A.

Nechť $i^2 = -1$. Pak $z = a + bi$ nazveme komplexním číslem. Bod $[a, b]$ má polární souřadnice $[r, \varphi]$. Pak $r = \sqrt{a^2+b^2}$ nazýváme velikost komplexního čísla z a φ jeho argument. Platí $z = r(\cos\varphi + i\cdot\sin\varphi)$.

Tvrzení. *Nechť $z_1 = r_1(\cos\varphi_1 + i\cdot\sin\varphi_1)$ a $z_2 = r_2(\cos\varphi_2 + i\cdot\sin\varphi_2)$ jsou komplexní čísla. Pak*

$$\begin{aligned} z_1\cdot z_2 &= r_1 r_2\big(\cos(\varphi_1+\varphi_2) + i\cdot\sin(\varphi_1+\varphi_2)\big),\\ \frac{z_1}{z_2} &= \frac{r_1}{r_2}\big(\cos(\varphi_1-\varphi_2) + i\cdot\sin(\varphi_1-\varphi_2)\big). \end{aligned}$$

Věta. (Moivreova věta) *Pro každé $n \in \mathbb{Z}$ a $\varphi \in \langle 0, 2\pi)$ platí*

$$(\cos\varphi + i\cdot\sin\varphi)^n = \cos n\varphi + i\cdot\sin n\varphi.$$

Tvrzení. *Platí*

$$\begin{aligned} \sin n\alpha &= \binom{n}{1}\cos^{n-1}\alpha\sin\alpha - \binom{n}{3}\cos^{n-3}\alpha\sin^3\alpha + \binom{n}{5}\cos^{n-5}\alpha\sin^5\alpha + \cdots,\\ \cos n\alpha &= \binom{n}{0}\cos^{n}\alpha\sin\alpha - \binom{n}{2}\cos^{n-2}\alpha\sin^2\alpha + \binom{n}{4}\cos^{n-4}\alpha\sin^4\alpha + \cdots. \end{aligned}$$

Na přednášce se pokusím nastínit, proč vlastně ani poslední zavedení není nejšťastnější. Proto vám ještě poskytnu pohled pod vysokoškolskou pokličku.

Třetí definice, ta nejlepší

Věta. *Existuje právě jedna dvojice funkcí $f\colon \mathbb{R}\to\mathbb{R}$, $g\colon \mathbb{R}\to\mathbb{R}$ splňující:*

(i) *f je lichá, g je sudá,*
(ii) *pro všechna $x, y \in \mathbb{R}$ platí $f(x+y) = f(x)g(y) + g(x)f(y)$ a $g(x+y) = g(x)g(y) - f(x)f(y)$,*
(iii) *existuje kladné reálné číslo π takové, že f je rostoucí na intervalu $\langle 0, \frac{\pi}{2}\rangle$, $f(\frac{\pi}{2}) = 0$ a $f(0) = 0$,*
(iv) $\lim\limits_{x\to 0}\frac{f(x)}{x} = 1$.

Definice. Funkci f z předchozí věty nazvu *sinus* a funkci g *kosinus*. *Tangens* a *kotangens* nadefinuji stejně jako předtím.

Tvrzení. *Předcházející větu splňuje dvojice funkcí*

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!},$$
$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}.$$

Následují příklady *silně* subjektivně srovnané podle obtížnosti.

Příklady aneb to, proč jsme tu

Lehké

Úloha 1. Spočtěte

(i) $\sin \frac{\pi}{12}$, $\cos \frac{\pi}{12}$ a $\operatorname{tg} \frac{\pi}{12}$,
(ii) $\cos^4 \frac{\pi}{24} - \sin^4 \frac{\pi}{24}$,
(iii) $\cos 36^\circ - \cos 72^\circ$,
(iv) $\sin 10^\circ \sin 50^\circ \sin 70^\circ$.

Úloha 2. Nechť x je reálné číslo takové, že $\frac{1}{\cos x} - \operatorname{tg} x = 2$. Spočtěte $\frac{1}{\cos x} + \operatorname{tg} x$.

Úloha 3. V oboru reálných čísel řešte soustavu

$$\sin x + \cos y = \sin(x+y),$$
$$\sin y + \cos x = \cos(x+y).$$

Úloha 4. Dokažte

$$(1 - \operatorname{cotg} 23^\circ)(1 - \operatorname{cotg} 22^\circ) = 2.$$

Úloha 5. Na intervalu $(0, \frac{\pi}{2})$ řešte rovnici

$$\frac{\sqrt{3}-1}{\sin x} + \frac{\sqrt{3}+1}{\cos x} = 4\sqrt{2}.$$

Úloha 6. Zjednodušte

$$\sqrt{\sin^4 x + 4\cos^2 x} - \sqrt{\cos^4 x + 4\sin^2 x}.$$

Úloha 7. V oboru reálných čísel řešte rovnici

$$1 + \sin\frac{x+\pi}{5} \cdot \sin\frac{x-\pi}{11} = 0.$$

(MO 55-A-s-3)

Úloha 8. V oboru reálných čísel řešte soustavu nerovnic

$$\sin x + \cos y \geq \sqrt{2},$$
$$\sin y + \cos z \geq \sqrt{2},$$
$$\sin z + \cos x \geq \sqrt{2}.$$

(MO 50-A-I-4)

Úloha 9. Najděte taková $x, y \in \mathbb{R}$, aby rovnice

$$\sin a = x \sin\left(\frac{\pi}{2} + a\right) + y \sin\left(\frac{\pi}{6} + a\right)$$

byla splněna pro všechna $a \in \mathbb{R}$. (MKS 29-6-6)

Úloha 10. Na intervalu $(0, \frac{\pi}{2})$ řešte rovnici

$$\sin x + \cos y = \sin(xy).$$

Úloha 11. Určete obsah množiny dané podmínkami $x^2+y^2 \leq 100$ a $sin(x+y) \geq 0$.

Úloha 12. Pro všechna x reálná dokažte

$$3(\sin^4 x + \cos^4 x) - 2(\sin^6 x + \cos^6 x) = 1.$$

Úloha 13. Pro všechna přípustná x dokažte

$$\operatorname{tg} 3x - \operatorname{tg} 2x - \operatorname{tg} x = \operatorname{tg} 3x \operatorname{tg} 2x \operatorname{tg} x.$$

Úloha 14. Dokažte

$$(4\cos^2 9^\circ - 3)(4\cos^2 27^\circ - 3) = \operatorname{tg} 9^\circ.$$

Úloha 15. Pro přípustná x dokažte

$$\frac{\operatorname{tg} 3x}{\operatorname{tg} x} = \operatorname{tg}\left(\frac{\pi}{3} - x\right) \operatorname{tg}\left(\frac{\pi}{3} + x\right).$$

Na substituci

Úloha 16. Nechť $x_0 = 2003$ a $x_{n+1} = \frac{1+x_n}{1-x_n}$ pro $n \geq 1$. Spočtěte x_{2004}.

Úloha 17. Dokažte, že mezi každými pěti různými reálnými čísly lze najít dvě (a a b) taková, že $|ab + 1| > |a - b|$.

Úloha 18. Vyřešte v reálných číslech soustavu

$$\begin{aligned} y &= \frac{4x^2}{1 + 4x^2}, \\ z &= \frac{4y^2}{1 + 4y^2}, \\ x &= \frac{4z^2}{1 + 4z^2}. \end{aligned}$$

(MKS 27-1-7)

Úloha 19. Dokažte, že mezi 101 reálnými čísly existují dvě čísla u, v, pro něž platí

$$100|u - v| \cdot |1 - uv| \leq (1 + u^2)(1 + v^2).$$

(MO 61-A-III-3)

Úloha 20. Mějme čtyři reálná čísla větší než jedna. Dokažte, že vždy umíme vybrat dvě z nich (x a y) takové, že výraz

$$\frac{\sqrt{(x^2 - 1)(y^2 - 1)} + 1}{xy}$$

nabývá hodnoty alespoň $\frac{\sqrt{3}}{2}$. (MKS 27-8-5b)

Těžší

Úloha 21. Označme $f(x) = \sin x + \sin 2x + \cdots + \sin 1000x$. Dokažte, že součet kořenů této funkce na intervalu $\langle 0, \frac{\pi}{2} \rangle$ je 2001π. (MKS 21-3-4)

Úloha 22. Najděte všechna řešení rovnice

$$\sin^2 x + \sin 2x \sin 4x + \cdots + \sin nx \sin n^2 x = 1.$$

(MKS 4-1-4)

Úloha 23. V oboru reálných čísel řešte soustavu rovnic

$$\sin^2 x + \cos^2 y = \operatorname{tg}^2 z,$$
$$\sin^2 y + \cos^2 z = \operatorname{tg}^2 x,$$
$$\sin^2 z + \cos^2 x = \operatorname{tg}^2 y.$$

(MO 62-A-I-6)

Úloha 24. V oboru reálných čísel řešte soustavu

$$2 \sin x \cos(x + y) + \sin y = 1,$$
$$2 \sin y \cos(x + y) + \sin x = 1.$$

(MO 58-A-I-1)

Úloha 25. Určete vnitřní úhly v trojúhelníku α, β, γ, pokud splňují

$$2 \sin \beta \sin(\alpha + \beta) - \cos \alpha = 1,$$
$$2 \sin \gamma \sin(\gamma + \beta) - \cos \beta = 0.$$

(MO 58-A-II-3)

Úloha 26. V oboru reálných čísel řešte rovnici

$$\sqrt{2}\,(\sin t + \cos t) = \operatorname{tg}^3 t + \operatorname{cotg}^3 t.$$

(MO 55-A-I-1)

Úloha 27. V oboru reálných čísel řešte soustavu

$$\sin^2 x + \cos^2 y = y^2,$$
$$\sin^2 y + \cos^2 x = x^2.$$

(MO 55-A-II-4)

Úloha 28. Dokažte, že pro libovolná reálná čísla $\alpha, \beta \in \langle 0, \frac{\pi}{2})$ platí nerovnost

$$\frac{1}{\cos \alpha} + \frac{1}{\cos \beta} \geq 2\sqrt{\operatorname{tg} \alpha + \operatorname{tg} \beta}.$$

(MO 51-A-II-1)

Úloha 29. Předpokládejme, že reálná čísla a, b splňují

$$\sin a + \sin b = \frac{\sqrt{2}}{2},$$
$$\cos a + \cos b = \frac{\sqrt{6}}{2}.$$

Spočtěte $\sin(a + b)$.

Úloha 30. Spočtěte

$$\cos a \cdot \cos 2a \cdots \cos 999a,$$

kde $a = \frac{2\pi}{1999}$.

Pár macků

Úloha 31. Spočtěte

$$(1+\operatorname{tg} 1^\circ)(1+\operatorname{tg} 2^\circ)\cdots(1+\operatorname{tg} 45^\circ).$$

(AMC12P 2002)

Úloha 32. Však už víte, co s tím

$$\begin{aligned}\operatorname{tg}^2 x + 2\operatorname{cotg}^2 2y &= 1,\\ \operatorname{tg}^2 y + 2\operatorname{cotg}^2 2z &= 1,\\ \operatorname{tg}^2 z + 2\operatorname{cotg}^2 2x &= 1.\end{aligned}$$

(MO 55-A-III-6)

Úloha 33. Najděte nejmenší hodnotu výrazu

$$\left|\sin x + \cos x + \operatorname{tg} x + \operatorname{cotg} x + \frac{1}{\sin x} + \frac{1}{\cos x}\right|$$

pro $x \in \mathbb{R}$. (Putnam 2003)

Úloha 34. Předpokládejme, že reálná čísla $a, x, y, z \in \mathbb{R}$ splňují

$$\frac{\cos x + \cos y + \cos z}{\cos(x+y+z)} = \frac{\sin x + \sin y + \sin z}{\sin(x+y+z)} = a.$$

Dokažte, že pak platí

$$\cos(x+y) + \cos(y+z) + \cos(z+x) = a.$$

O goniometrických funkcích by se dala napsat ještě spousta věcí – už jen proto, že souvisí s trigonometrii, které jsem se snažil co možná nejvíce vyhnout. Trigonometrie se pak dá vztáhnout na část geometrie, a to už je opravdu velké téma. Každopádně by se slušelo říci, že jsem vynechal témata „O pohybu na kouli“ a „Skalární součin vektorů“, které si může čtenář doplnit ze skvělé knihy [1], ze které jsem čerpal.

Zdroje

[1] Titu Andreescu, Zuming Feng, *103 Trigonometry Problems*
[2] Archiv Matematického korespondenčního semináře
[3] Stránky české Matematické olympiády

Trojúhelníkové nerovnosti

FILIP HLÁSEK

ABSTRAKT. V příspěvku si ukážeme několik pozoruhodných nerovností ze světa trojúhelníků. Jejich důkaz je často trikový nebo používá hlubší znalost tématu, takže úloh bude málo, ale o to vydatnějších.

Geometrické nerovnosti je souhrnný název pro úlohy, ve kterých se dokazuje platnost nerovnosti mezi geometrickými veličinami (obvykle se jedná o délky úseček nebo velikosti úhlů). Při jejich dokazování je potřeba chytře skloubit znalosti z oblasti algebraických nerovností s poznatky z planimetrie. Proto patří tato problematika mezi nejnáročnější partie elementární matematiky. Přesto se občas úlohy tohoto typu vyskytují ve středoškolských soutěžích, a proto si jich zkusíme několik vyřešit.

Úloha. Mějme trojúhelník ABC, délky jeho stran označme a, b, c, velikosti odpovídajících úhlů α, β, γ a poloměr jeho kružnice opsané r. Dále $2s = a + b + c$ a S je jeho obsah. Navíc bod P je libovolný bod uvnitř trojúhelníku a d_1, d_2, d_3 jeho vzdálenosti od jednotlivých stran. Dokažte, že potom platí následující nerovnosti:

(1) (Trojúhelníková) $a + b > c$, $b + c > a$, $c + a > b$,

(2) $3(ab + bc + ca) \le (a + b + c)^2 < 4(ab + bc + ca)$,

(3) $8(s - a)(s - b)(s - c) \le abc$,

(4) $ab(a + b) + bc(b + c) + ca(c + a) \le 48(s - a)(s - b)(s - c)$,

(5) $\frac{a}{b+c-a} + \frac{b}{c+a-b} + \frac{c}{a+b-c} \ge 3$,

(6) $3a^2 + 3b^2 - c^2 \ge 4\sqrt{3}S$,

(7) (Weitzenböck) $a^2 + b^2 + c^2 \ge 4\sqrt{3}S$,

(8) (Finsler-Hadwiger) $a^2 + b^2 + c^2 \ge 4\sqrt{3}S + (a - b)^2 + (b - c)^2 + (c - a)^2$,

(9) $\sin^2 \alpha + \sin^2 \beta + \sin^2 \gamma \le \frac{9}{4}$,

(10) $\sin \alpha + \sin \beta + \sin \gamma \ge \sin 2\alpha + \sin 2\beta + \sin 2\gamma$,

(11) (Odo) $27(b^2 + c^2 - a^2)^2(c^2 + a^2 - b^2)^2(a^2 + b^2 - c^2)^2 \le (4S)^6$, ABC ostroúhlý,

(12) (Erdös-Mordell) $2(d_1 + d_2 + d_3) \le |PA| + |PB| + |PC|$,

(13) (Schreiber) $d_1 + d_2 + d_3 \ge 6r$,

(14) (Neuberg-Pedoe) $A^2(-a^2+b^2+c^2)+B^2(a^2-b^2+c^2)+C^2(a^2+b^2-c^2) \ge 16ST$, kde A, B, C jsou délky stran nějakého trojúhelníku s obsahem T.

Catalanova čísla

Anča Chejnovská

Abstrakt. Catalanova čísla jsou posloupnost 1, 1, 2, 5, 14, 42, ..., na kterou vedou zdánlivě nesouvisející kombinatorické úlohy. Na přednášce si povíme, jak je odvodit a co s nimi počítat.

Definice. Obdélníkem $m \times n$ rozumíme obdélník vysoký m políček a široký n políček. Jeho levý spodní vrchol označíme jako začátek a jeho pravý horní vrchol jako konec. Úhlopříčka pak je úsečka mezi začátkem a koncem. Dále cestou v takovém obdélníku rozumíme trasu ze začátku do konce, která vede po mřížce, a to pouze nahoru a doprava.

Cvičení. Ukažte, že v daném obdélníku $m \times n$ existuje přesně $\binom{m+n}{m}$ různých cest.

K tomuto celkem snadnému příkladu si však přidáme dodatečnou podmínku na cesty týkající se úhlopříčky.

Definice. n-té Catalanovo číslo je počet cest ve čtverci $n \times n$, které jsou celé pod úhlopříčkou (smí se jí dotýkat). Tento počet budeme značit symbolem C_n.

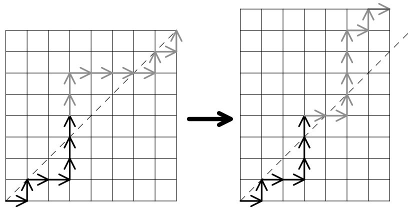
Vyčíslení

Tvrzení. *Platí vzorec*

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}.$$

K tomuto vzorci můžeme dospět různými způsoby. Uvedeme dva z nich, každý spočívá v jistém zobecnění úlohy spočítat Catalanovo číslo.

Příklad. Jsou dána čísla $m \leq n$. Kolik existuje cest v obdélníku $m \times n$, které jsou celé pod úhlopříčkou levého čtverce $m \times m$? Catalanova čísla dostaneme, volíme-li $m = n$.



Návod. Spočtěte ty cesty, které úhlopříčku překročí. U každé takové vezměte první bod nad diagonálou a překlopte zbytek cesty (místo doprava jděte nahoru a obráceně). Které cesty ve kterých obdélnících se takto dají dostat? Hledaný počet cest vyjde

$$\binom{m+n}{m} - \binom{m+n}{m-1}.$$

Příklad. Jsou dána nesoudělná čísla m, n. Kolik existuje cest v obdélníku $m \times n$, které jsou celé pod úhlopříčkou tohoto obdélníka? Catalanova čísla dostaneme, volíme-li $m = n + 1$. (MKS 26–5–8)

Návod. Řekneme, že si dvě cesty odpovídají, pokud je možné jednu vytvořit z druhé tak, že se rozdělí na dvě a složí v opačném pořadí. Ukažte, že odpovídající si cesty budou tvořit $(m+n)$-tice, přičemž vždy právě jedna cesta z takové $(m+n)$-tice vede pod diagonálou.

Rekurentní vzorec

Tvrzení. *Mějme posloupnost* $(a_n)_{n=0}^{\infty}$*, která splňuje vztahy*

$$a_0 = 1,$$
$$a_{n+1} = \sum_{i=0}^{n-1} a_i a_{n-i}.$$

Pak $a_n = C_n$.

Příklady

Příklad 1. Spočítejte počet korektních uzávorkování n párů závorek.

Příklad 2. Kolik je možností pořadí, ve kterém vyhodnotit výraz skládající se z n čísel a $n-1$ operací mezi nimi? Předpokládáme, že ve výrazu nejsou závorky a že neznáme priority operací.

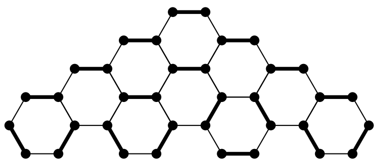
Příklad 3. Kolik existuje lomených čar délky n takových, že na každém celočíselném úseku délky 1 vedou šikmo (pod úhlem $45°$) doprava nahoru nebo dolů, končí ve stejné výšce jako začínají a nikdy přitom neklesnou níž.

Příklad 4. Určete počet konečných posloupností čísel $(a_1, \ldots, a_n)$ takových, že pro každé $k = 1, 2, \ldots, n$ platí

$$\sum_{i=1}^{k} a_i \geq k \quad \text{a přitom} \quad \sum_{i=1}^{n} a_i = n.$$

Příklad 5. Kolik existuje permutací na n prvcích, které žádné trojici nezachovají pořadí?

Příklad 6. Kolik existuje úplných párování vrcholů na šestiúhelníkové pyramidě šířky n? Úplné párování na šestiúhelníkové pyramidě může vypadat například takto:



Příklad 7. Kolika způsoby se dá vyplnit tabulka $2 \times n$ čísly $1, 2, \ldots, 2n$ tak, aby oba řádky i všechny (dvouprvkové) sloupce byly rostoucí?

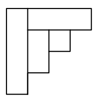
Příklad 8. Kolik lze vytvořit binárních stromů na n vrcholech tak, že rozlišujeme „pravé“ a „levé“ syny?

Příklad 9. Kolik zbude stromů v předchozí úloze, pokud přidáme podmínku, že každý vrchol musí mít dva syny, nebo žádného?

Příklad 10. Kolik je rovinných stromů na n vrcholech s vrcholy obarvenými dvěma barvami a jednou hranou určenou jako „význačnou“? Navíc dva stromy považujeme za různé, pokud se liší (cyklickým) pořadím hran kolem některého vrcholu.

Příklad 11. Kolika způsoby jde pravidelný n-úhelník rozdělit na trojúhelníky?

Příklad 12. Kolika způsoby je možné vyskládat schodiště velikosti n pomocí n obdélníků? Na obrázku vidíte schodiště velikosti 4 vyskládané čtyřmi obdélníky.



Příklad 13. Kolika způsoby si může podat $2n$ lidí ruce přes kulatý stůl tak, aby se jim nekřížily?

Literatura a zdroje

[1] Stanley, Richard P., *Catalan addendum to Enumerative Combinatorics* *www-math.mit.edu/~rstan/ec/catadd.pdf*
[2] Math Images, *http://mathforum.org/mathimages/index.php/Catalan_Numbers*
[3] Wikipedie, *http://en.wikipedia.org/wiki/Catalan_number*

Redundantní číselné soustavy pro pokročilé

Jakub „Roman“ Klemsa

Abstrakt. Problém, jak zapisovat čísla, se táhne s lidstvem od nepaměti. Dnes známý poziční zápis, kdy stejný symbol (např. „5“) použitý na různých místech umožňuje zapsat jednou pět, jednou padesát, byl podmíněn vynálezem symbolu „0“ pro „nic“. Každému je jasné, že úloha vynásobení čísel 42 a 27 zapsaných v desítkové soustavě je jednodušší, než násobení XLII a XXVII zapsaných římským způsobem. Přesto se desítkový zápis prosadil v Evropě až ve 13. století.

I dnes má smysl číselné soustavy zkoumat. Jejich renesance přišla s nástupem procesorů – důvodem byla potřeba vyvinout algoritmus pro paralelní sčítání.

Definice. Poziční numerační systém je určen bazí $\beta \in \mathbb{R}$, $\beta > 1$, a konečnou množinou celočíselných cifer nazývanou abeceda $\mathcal{A} \subset \mathbb{Z}$. β-rozvojem čísla x pak rozumíme

$$x = \sum_{k=-\infty}^{n} x_k \beta^k\,, \quad x_k \in \mathcal{A}.$$

„Naše“ desítková soustava má bázi $\beta = 10$ a abecedu $\mathcal{A} = \{0, 1, \ldots, 9\}$. Ukážeme si dva algoritmy, jak čísla mezi standardními soustavami převádět.

První algoritmus využívá modula. Dá se použít jen na celá čísla a měl by v pseudokódu těžkopádný zápis, ukážeme si ho proto jen na přednášce.

Algoritmus. (Hladový)
`najdi` k`, aby platilo` $\beta^k \le x < \beta^{k+1}$ `(nespecifikováno jak)`
`repeat`
  $x_k := \lfloor \frac{x}{\beta^k} \rfloor$
  $y := x - x_k \beta^k$
  $k := k - 1$
`until` $y = 0$

Cvičení.

(1) Převeďte $(10010110111)_2$ do osmičkové soustavy. Dokážete to bez myšleného převodu do desítkové? (malá finta)
(2) Zapište prvních n číslic čísla π v sedmičkové soustavě. Který algoritmus použijete?

Základ soustavy nemusí být nutně celočíselný. Dostáváme hned několik otázek:

(1) Jakou volit abecedu, aby byl možný zápis všech reálných čísel?
(2) V kladném případě, bude zápis jednoznačný?

Odpovědi zní:

(1) Pokud zvolíme standardní abecedu nejbližšího vyššího přirozeného čísla, zápis možný bude (hladový algoritmus ho najde). Pokud zvolíme o jedna menší, najdou se čísla, která nepůjdou zapsat (hladový algoritmus se „trefí“ mimo abecedu, de facto ji vynucuje).
(2) Nebude!

Důkaz. Provedeme na přednášce.

Dostali jsme třídu soustav, ve kterých mají některá čísla nejednoznačný zápis! Jako konkrétní příklad si uveďme soustavu o základu $\beta^2 = 9\beta + 1 \Rightarrow 9 < \beta < 10$. Máme tedy abecedu $\mathcal{A} = \{0, 1, \ldots, 9\}$ a můžeme psát $\beta^2 = (1\,0\,0\,\bullet)_\beta = (9\,1\,\bullet)_\beta$. Tento „jev“ můžeme vytvořit i pro přirozené báze, stačí uměle zvětšit abecedu.

Cvičení. Zapište číslo 10 v soustavě o základu 4 s abecedou $\mathcal{A} = \{-2, -1, 0, 1, 2\}$. Najdete více možných zápisů?

Paralelní sčítání jako lokální funkce

Definice. Buďte $\mathcal{A}$, $\mathcal{B}$ abecedy a $\mathcal{A}^{\mathbb{Z}}$, $\mathcal{B}^{\mathbb{Z}}$ množiny slov na těchto abecedách. Buďte $r, t \in \mathbb{N}_0$, $p = r + t + 1 \in \mathbb{N}$ a funkce $\Phi\colon \mathcal{B}^p \to \mathcal{A}$. Funkce $\varphi\colon \mathcal{B}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$, $\varphi(u) = v$, kde $v_j = \Phi(u_{j+t} \ldots u_j \ldots u_{j-r})$, se nazývá p-lokální funkce.

Uvažujme konečné β-reprezentace čísel v abecedě $\mathcal{A}$:

$$\mathrm{Fin}_{\mathcal{A}}(\beta) = \left\{ x = \sum\nolimits_{k \in I} x_k \beta^k \;\middle|\; I \subset \mathbb{Z},\, |I| < \infty,\, x_k \in \mathcal{A} \right\}.$$

Hledáme algoritmus, který umožní sečíst dvě taková čísla v konstantním čase:

$$\sum_{k \in I_1} (\underbrace{x_k + y_k}_{\in \mathcal{A}+\mathcal{A}=\mathcal{B}})\beta^k = \sum_{k \in I_1} \underbrace{u_k}_{\in \mathcal{B}} \beta^k = \sum_{k \in I_2} \underbrace{v_k}_{\in \mathcal{A}} \beta^k. \tag{$\clubsuit$}$$

K tomu potřebujeme znát p-lokální funkci φ takovou, že funkce Φ (dle definice) přiřadí p-tici dvojic cifer $(u_{j+t} \ldots u_j \ldots u_{j-r})$ cifru v_j tak, aby platila rovnost ($\clubsuit$) a $v_j \in \mathcal{A}$. Na příkladu si ukážeme, že standardní číselné soustavy nám nestačí.

$$\begin{array}{r} 1999\ldots99999 \\ 0000\ldots00001 \\ \hline 20000\ldots00000 \end{array}$$

Na vznik dvojky na začátku součtu má vliv každá cifra horního čísla. Takové situaci se chceme vyhnout. Algoritmus, jak to udělat, byl objeven až při použití redundantní číselné soustavy. První takový algoritmus navrhl Avizienis r. 1961. Pracoval s desítkovou soustavou a abecedou $\{-6, -5, \ldots, 5, 6\}$. Své aplikace se podobný algoritmus dočkal v aritmetických jednotkách procesorů, například Pentium používá soustavu se základem $\beta = 4$ a pěti ciframi $\mathcal{A} = \{-2, -1, 0, 1, 2\}$. Nyní ale zpět k algoritmu.

Mějme $x, y \in \mathrm{Fin}_{\mathcal{A}}(4)$. Cílem je spočítat $z \in \mathrm{Fin}_{\mathcal{A}}(4)$ tak, aby platilo

$$\sum x_i 4^i + \sum y_i 4^i = \sum z_i 4^i.$$

Algoritmus. (♠)

```
for i in I_1 ∪ I_2 do
    w_i := x_i + y_i
    if (w_i ≥ 3 or (w_i = 2 and w_{i-1} ≥ 2))
        q_i := 1
    elseif (w_i ≤ −3 or (w_i = −2 and w_{i-1} ≤ −2))
        q_i := −1
    else
        q_i := 0
    end
    z_i := w_i − 4q_i + q_{i-1}
end
```

Cvičení.

(1) Ověřte, že $z_i \in \mathcal{A}$.
(2) Určete p-lokální funkci z algoritmu (♠). Jaké je p?

Dané číslo však musíme nejdříve do nové soustavy převést. To lze provést paralelně. Číslo rozložíme na součet dvou čísel tak, že 0, 1 a 2 zůstanou, 3 rozepíšeme na 1 a 2. Tím se oběma čísly dostaneme do naší abecedy, v níž paralelně sčítat umíme. Převod zpět už paralelně provést nelze.

Dále potřebujeme umět čísla porovnávat, což na první pohled paralelně nelze. Běžné lexikografické porovnávání v tomto případě selže – například $(1\,\overline{2}\,\overline{2}\,\bullet)_{4,\mathcal{A}} < (2\,2\,\bullet)_{4,\mathcal{A}}$, protože $6 < 10$. Čísla musíme nejdříve paralelně odečíst a pak už první cifra rozhodne.

Literatura a zdroje

[1] E. Pelantová, Š. Starosta, *Nestandardní zápisy čísel*, Pokroky matematiky, fyziky a astronomie, JČMF, Praha, 2011,

[2] E. Pelantová, *prezentace Redundantní číselné soustavy*, FJFI ČVUT, Praha, 2011.

Konečné projektívne roviny a latinské štvorce

PETER „πTR“ KORCSOK

ABSTRAKT. V tejto prednáške sa zoznámime s konceptom konečných projektívnych rovín a latinských štvorcov a ukážeme si, ako tieto objekty navzájom súvisia. V druhej časti prednášky si predstavíme ich aplikáciu pri takzvaných samoopravných kódoch. Tieto kódy sa využívajú pri prenose informácií menej spoľahlivým spôsobom, kde môže dochádzať k zmene niektorých z prenášaných znakov.

Kde sa to tu vzalo?

Už okolo roku 300 pred naším letopočtom napísal Euklides dielo *Základy*, v ktorom v trinástich knihách uviedol vtedajšie poznatky o geometrii a číslach formou axiómov a vecí z nich odvodených. V prvej z týchto kníh zaviedol aj päť postulátov (axiómov), ktoré následne tvorili základ množstva geometrických dôkazov.

Piaty postulát – najznámejší asi v podaní od Playfaira „pre daný bod a priamku ním neprechádzajúcu existuje maximálne jedna rovnobežka prechádzajúca daným bodom“ – je odlišný od zvyšných, preto sa ho mnoho matematikov snažilo dokázať s využitím iba predchádzajúcich štyroch. Všetky tieto pokusy ale boli neúspešné, dnes je už dokonca známe, že taký dôkaz ani existovať nemôže.

Miesto toho sa v geometrii zostrojil nový „model“ – predpokladá platnosť prvých štyroch postulátov, ten posledný je nahradený predpokladom „pre ľubovoľný bod a priamku ním neprechádzajúcu existujú aspoň dve rovnobežky prechádzajúce daným bodom“. Takýto systém priamok a bodov zvyknú matematici označovať ako *hyperbolickú rovinu*, tou sa ale na tejto prednáške nebudeme zaoberať.

Podobne sa ale môžeme dopracovať k *projektívnej* alebo aj *eliptickej rovine*, ktorá využíva mierne voľnejšie Euklidove postuláty, pričom posledný je nahradený podmienkou „každé dve rôzne priamky sa pretínajú“.

Pomoooc! Čo to je?!

Už sme zistili, prečo sa začali projektívne roviny skúmať. Aby sme ich mohli lepšie spoznať, musíme si ich trochu presnejšie popísať.

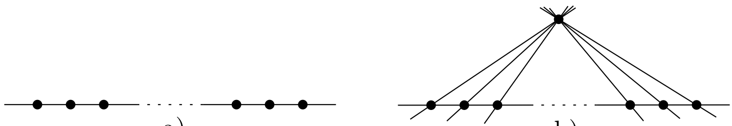
Definícia. *Projektívnou rovinou* budeme nazývať množinový systém $(B, \mathcal{P})$, kde $\mathcal{P} \subseteq 2^B$ a platia nasledujúce axiómy:

(1) $(\forall\, P, Q \in \mathcal{P},\, P \neq Q)\ |P \cap Q| = 1$,
(2) $(\forall\, x, y \in B,\, x \neq y)\ (\exists!\, P \in \mathcal{P})\ x, y \in P$,
(3) $(\exists\, \check{S} \subseteq B, |\check{S}| = 4)\ (\forall\, P \in \mathcal{P})\ |P \cap \check{S}| \leq 2$.

Prvky množiny B potom nazývame *bodmi PR*, prvky $\mathcal{P}$ sú tiež *priamky PR*. Ak navyše platí, že B má len konečne veľa bodov, hovoríme o *konečnej projektívnej rovine*.

Poznámka. Axióm (3) môžeme ekvivalentne nahradiť ľubovoľným z nasledujúcich dvoch:

(3′) $(\forall\, P, Q \in \mathcal{P})\ B \setminus (P \cup Q) \neq \emptyset$,
(3″) $(B, \mathcal{P})$ netvorí systém ako na obrázku:



a) b)

Cvičenie. Nájdite najmenšiu projektívnu rovinu.

Tvrdenie. *Majme KPR $(B, \mathcal{P})$, potom všetky priamky $P \in \mathcal{P}$ obsahujú rovnako veľa bodov.*

Definícia. *Rádom KPR* $(B, \mathcal{P})$ budeme rozumieť hodnotu $|P| - 1$ pre $P \in \mathcal{P}$.

Tvrdenie. *Nech $(B, \mathcal{P})$ je KPR rádu n. Potom platia nasledujúce vlastnosti:*

(0) $(\forall\, P \in \mathcal{P})\ |P| = n + 1$,
(1) $(\forall\, x \in B)\ |\{P \in \mathcal{P}; x \in P\}| = n + 1$,
(2) $|B| = n^2 + n + 1$,
(3) $|\mathcal{P}| = n^2 + n + 1$.

Kde to rastie?

V predchádzajúcej časti sme si popísali, čo to konečné projektívne roviny sú a aké sú ich základné vlastnosti, v cvičení sme si dokonca skúsili nejakú KPR aj nájsť. Je ale možné, že je to jediný exemplár, ktorý spĺňa našu definíciu? Na to sa teraz pozrieme.

Jednou z možností je využitie vhodných algebraických telies:

Tvrdenie. *Pre každé $n = p^k$, kde p je prvočíslo a $k \in \mathbb{N}$, existuje KPR rádu n.*

Hypotéza. *KPR rádu n existuje práve pre $n = p^k$ pre nejaké prvočíslo p a $k \in \mathbb{N}$.*

Druhú možnosť nám dávajú tzv. *latinské štvorce*:

Definícia. *Latinským štvorcom rádu* n budeme označovať maticu $L \in [n]^{n\times n}$ spĺňajúcu podmienku

$$(\forall\, i \neq i', j \neq j' \in [n])\; L_{i'j} \neq L_{ij} \neq L_{ij'},$$

kde $[n] = \{1, \dots, n\}$. Pre $k < n$ nazveme *latinským obdĺžnikom* maticu tvaru $k \times n$ spĺňajúcu predchádzajúcu podmienku pre každú dvojicu $i \neq i' \in [k]$

Tvrdenie. *Každý latinský obdĺžnik je možné doplniť na latinský štvorec.*

Cvičenie. Z balíčka kariet vyberte všetky štyri esá, kráľov, dámy aj chlapcov a rozmiestnite ich do mriežky 4×4 tak, aby žiadny riadok ani stĺpec neobsahoval dve karty rovnakej farby alebo hodnoty.

Definícia. Latinské štvorce L a L' rádu n nazveme *ortogonálnymi* ($L \perp L'$), ak platí podmienka

$$(\forall\, i, i', j, j' \in [n])\; (i, j) \neq (i', j') \Rightarrow (L_{i,j}, L'_{i,j}) \neq (L_{i',j'}, L'_{i',j'}).$$

Skupinu latinských štvorcov rovnakého rádu nazveme *navzájom ortogonálnymi*, ak každé dve z nich sú ortogonálne.

Príklad. Nasledujúci príklad ilustruje dve ortogonálne latinské štvorce rádu 3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \to \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

Tvrdenie. *Nech $L_1, \dots, L_m$ sú NOLŠ rádu n. Potom $m \leq n - 1$.*

Veta. *Pre $n > 2$ existuje KPR rádu n, práve keď existuje $n - 1$ NOLŠ rádu n.*

Dá sa to jesť?

Už sme si ukázali, ako vieme niektoré konečné projektívne roviny, prípadne latinské štvorce tvoriť, poďme sa teda zamyslieť, aký majú význam v bežnom živote.

Definícia. *Slovom w dĺžky n nad abecedou* Σ ($w \in \Sigma^n$) nazveme ľubovoľnú postupnosť n znakov z danej abecedy Σ. Vo väčšine prípadov sa používa $\Sigma = \{0, 1\}$, prípadne obecnejšie $\Sigma = \{0, \dots, q\}$ pre nejaké $q \in \mathbb{N}$.

Definícia. *Hammingovu vzdialenosť* dvoch slov $u, v \in \Sigma^n$ definujeme nasledovne:

$$d_H(u, v) = |\{i \in [n];\, u_i \neq v_i\}|\,.$$

Definícia. Podmnožinu $K \subseteq \Sigma^n$, $|K| = |\Sigma|^k$, kde platí $d_H(u, v) \geq d$ pre ľubovoľné $u \neq v \in K$, nazveme (n, k, d)-*kódom* a hovoríme o kóde dĺžky n, veľkosti $|\Sigma|^k$ a vzdialenosti d.

Pozorovanie. (n,k,d)*-kód dokáže rozpoznať až* $d-1$ *a opraviť až* $\left\lfloor \frac{d-1}{2} \right\rfloor$ *chýb.*

Tvrdenie. *Ak existuje* (n,k,d)*-kód pre* $d \geq 2$*, potom existuje aj* $(n-1,k,d-1)$*-kód.*

Tvrdenie. *Ak existuje KPR rádu* n*, potom existuje aj kód nad abecedou* $\Sigma = \{0,1\}$ *dĺžky* n^2+n+1*, veľkosti* n^2+n+2 *a vzdialenosti* $2n$*.*

Problém. Akú najväčšiu veľkosť môže mať kód nad abecedou $\Sigma = \{0,\dots,q\}$ dĺžky 4 a vzdialenosti 3?

V nasledujúcich tvrdeniach budeme predpokladať abecedu $\Sigma = \{0,\dots,q\}$.

Tvrdenie. *Pre každý* $(4,k,3)$*-kód určite platí* $k \leq 2$*.*

Tvrdenie. $(4,2,3)$*-kód existuje práve vtedy, ak existujú dve ortogonálne latinské štvorce rádu* q*.*

A teraz trochu obecnejšie:

Tvrdenie. *Pre každý* (n,k,d)*-kód určite platí* $k \leq n-d+1$*.*

Tvrdenie. $(n,2,n-1)$*-kód existuje práve vtedy, ak existuje* $n-2$ *NOLŠ rádu* q*.*

Dôsledok. $(n,2,n-1)$*-kód nad abecedou* $\Sigma = \{0,\dots,n-1\}$ *existuje pre každé* $n = p^k+1$*, kde* p *je prvočíslo a* $k \in \mathbb{N}$*. Ak by platila spomínaná hypotéza, takýto kód pre žiadne iné* n *neexistuje.*

Literatúra a zdroje

Pri príprave tejto prednášky som čerpal prevažne z nasledujúcich materiálov:

[1] Connelly, Robert. *Classical Geometries* (texty k prednáške). Cornell University, Ithaca, NY, 2010. *www.math.cornell.edu/~web4520/*

[2] Bartlett, Padraic. *Latin Squares* (texty k prednáške). Mathcamp 2012. *www.its.caltech.edu/~padraic/mathcamp_2012/mathcamp_2012.html*

[3] zápisky z prednášok *Kombinatorika a grafy I*, *Kombinatorika a grafy II* a *Kombinatorické struktury* na MFF UK

Dělitelnost pro začátečníky

Kuba Krásenský

Během přednášky se budeme zabývat dělitelností, což je jeden z ústředních pojmů teorie čísel. Probereme její známé i méně známé vlastnosti, některé z nich se naučíme i dokázat. Při té příležitosti si procvičíme různé techniky důkazu – přímý, sporem, indukcí. Ukážeme si, proč funguje Eukleidův algoritmus. Zavedeme pojem kongruence a naučíme se s ním pracovat. Zavadíme i o kvadratické zbytky a Malou Fermatovu větu, kterou si také dokážeme. Posléze ji zobecníme na větu Eulerovu a probereme i větu Wilsonovu.

Úvodní pojmy

Úmluva. Pokud nebude výslovně uvedeno jinak, myslí se v tomto příspěvku pod pojmem „číslo“ vždy číslo celé.

Definice. Řekneme, že číslo a je *dělitelné* číslem b právě tehdy, když existuje číslo k takové, že $k \cdot b = a$. Druhé možné vyjádření stejné skutečnosti je, že b *dělí* a. Také lze říci, že b je *dělitelem* čísla a nebo číslo a *násobkem* b. Zapisujeme $b \mid a$.

Poznámka. (Základní vlastnosti) Pro libovolná celá a, b, c platí:

(i) $1 \mid a$,
(ii) $a \mid a$,
(iii) $a \mid 0$,
(iv) $a \mid b \wedge b \mid c \Rightarrow a \mid c$,
(v) $a \mid b \wedge a \mid c \Rightarrow a \mid b + c$,
(vi) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$.

Věta. *Pro každá přirozená m a n existuje právě jedna dvojice nezáporných celých čísel k a r, $r < m$, tak, že platí $n = km + r$. Říkáme, že k je celočíselný podíl m a n a že r je zbytek n po dělení m.*

Příklady

Příklad 1. O přirozeném čísle n řekneme, že je magické, jestliže dělí každé číslo vzniklé tak, že před n napíšeme jednu nebo několik nových číslic. Najdi všechna magická čísla.

Příklad 2. Dokaž, že $6 \mid n^3 - n$ pro každé přirozené n.

Příklad 3. Dokažte, že pro každá celá x, y platí

$$50 \mid 19x + 3y \Leftrightarrow 50 \mid 23x + y.$$

Příklad 4. Najděte všechna čísla x, pro která platí

$$x - 3 \mid x^3 - 3.$$

Příklad 5. Určete počet deseticiferných čísel, ve kterých je možno škrtnout dvě sousední cifry a dostat tak číslo 99krát menší.

Příklad 6. Dokažte, že pro každé přirozené n platí $133 \mid 11^{n+1} + 12^{2n-1}$.

Eukleidův algoritmus

Definice. Nechť jsou a a b nezáporná celá čísla, alespoň jedno z nich nenulové. Jejich *největším společným dělitelem* – značíme $\mathrm{NSD}(a, b)$ – je největší přirozené číslo d takové, že $d \mid a \wedge d \mid b$. Čísla a, b nazýváme nesoudělná, když $\mathrm{NSD}(a, b) = 1$.

Definice. Podobně nazveme *nejmenším společným násobkem* a a b nejmenší číslo, které je dělitelné jak číslem a, tak i b. Značíme ho $\mathrm{nsn}(a, b)$ pro snadnější odlišení od $\mathrm{NSD}(a, b)$.

Věta. *Pro každou dvojici a, b ($a \geq b$) platí:* $\mathrm{NSD}(a, b) = \mathrm{NSD}(a - b, b)$.

Díky tomu funguje tzv. Eukleidův algoritmus hledání největšího společného dělitele. Dvojici a, b nahradíme dvojicí $a - b$, b. Tu opět uspořádáme podle velikosti, větší číslo označíme a a menší b. Poté znovu odečítáme. Skončíme ve chvíli, kdy bude jedno z čísel rovno nule. Tehdy je druhé číslo právě rovno hledanému NSD.

Příklady

Příklad 7. Najděte $\mathrm{NSD}(3k + 1, 2k - 1)$.

Příklad 8. Máme množinu čísel $\{1, 2, \ldots, 2n - 1, 2n\}$. Dokažte, že mezi každými $n + 1$ vybranými prvky je nějaká dvojice nesoudělných čísel.

Příklad 9. Ukažte, že dva po sobě jdoucí členy Fibonacciho posloupnosti jsou nesoudělné.

Příklad 10. Dokažte, že pro každá přirozená m, n platí

$$\mathrm{NSD}(2^m - 1, 2^n - 1) = 2^{\mathrm{NSD}(m,n)} - 1.$$

Prvočísla

Definice. *Prvočíslem* nazveme takové přirozené číslo, které má právě dva kladné dělitele. Číslo, které má dělitelů více, je *složené*.

Poznámka. Všimněte si, že jednička není ani prvočíslo, ani číslo složené.

Věta. *Číslo p je prvočíslo právě tehdy, když pro všechna čísla b, c platí*

$$p \mid bc \Rightarrow (p \mid b \vee p \mid c).$$

Věta. (Základní věta aritmetiky) *Každé $n \geq 2$ lze rozložit na součin prvočísel jednoznačně až na pořadí činitelů.*

Věta. *Existuje nekonečně mnoho prvočísel.*

Příklady

Příklad 11. Máme číslo n, které lze zapsat ve tvaru $m^6 - m^2$, kde m je přirozené číslo. Jakým nejvyšším číslem bude n jistě dělitelné?

Příklad 12. Najděte všechny dvojice prvočísel p, q, pro které existuje přirozené číslo n tak, že platí

$$p(p+1) + q(q+1) = n(n+1).$$

Příklad 13. Máme přirozené n vyjádřené jako součin prvočísel. Jak určíme, kolik má dělitelů?

Příklad 14. Známe $\mathrm{NSD}(a, b)$ i $\mathrm{nsn}(a, b)$. Jsou tím a a b jednoznačně dána?

Příklad 15. Čemu se rovná $\mathrm{nsn}(a, b) \cdot \mathrm{NSD}(a, b)$?

Příklad 16. Pro prvočísla p, q platí $p \mid q^3 - 1$ a $q \mid p - 1$. Dokažte, že $p = q^2 + q + 1$.

Příklad 17. Ukažte, že pro každé přirozené n existuje řada alespoň n po sobě jdoucích přirozených čísel, neobsahující žádné prvočíslo.

Kongruence

Definice. Říkáme, že a je *kongruentní* s b modulo n právě tehdy, když $n \mid a - b$. Značíme $a \equiv b \pmod{n}$.

Poznámka. To znamená, že a a b dávají stejný zbytek po dělení n.

Příklady

Příklad 18. Určete poslední cifru čísel $17^{17^{17}}$ a $23^{23^{23^{23}}}$.

Příklad 19. Najděte taková celá čísla x, y, že $x^2 = 4y + 2$.

Těžké věty na závěr

Věta. (Malá Fermatova) *Pro každé prvočíslo p a s ním nesoudělné přirozené číslo a platí*

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

Definice. Zavedeme Eulerovu funkci $\varphi\colon \mathbb{N} \to \mathbb{N}$. Její funkční hodnotou bude počet všech přirozených čísel, která jsou s n nesoudělná a zároveň jsou menší než n.

Věta. (Eulerova) *Pro každou dvojici přirozených nesoudělných čísel a, n platí:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Věta. (Wilsonova) *Přirozené číslo n je prvočíslo právě tehdy, když*

$$(n-1)! \equiv -1 \pmod{n}.$$

Příklady

Příklad 20. Dokažte, že neexistuje žádné přirozené číslo n takové, aby platilo $n \mid 2^n - 1$.

Příklad 21. Dokažte, že pro lichá n platí $n \mid 2^{n!} - 1$.

Poděkování

Chtěl bych poděkovat Pepovi Tkadlecovi za poskytnutí materiálů, ze kterých jsem při přípravě přednášky částečně čerpal. Dále svému cvičícímu z předmětu Diskrétní matematika, inženýru Tomáši Vávrovi, za to, že zadává i na VŠ příklady, které se podobají olympiádní matematice a dají se využít na takovéto přednášce. Také děkuji Jiřímu Růžičkovi, z jehož diplomové práce „Teorie čísel – sbírka příkladů“ jsem přebral několik cvičení.

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* $B = \{v_1, \ldots, v_n\}$, 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*

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

kde $\operatorname{Vol}(M)$ *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

Orientované úhlení

Mirek Olšák

Abstrakt. Úhel je jedním ze základních pojmů geometrie. Přitom jeho nešikovná definice mnohdy způsobí zbytečný rozpad argumentace na více možností. Příspěvek ukazuje, jak vystavět geometrii na orientovaných úhlech, a předvádí jejich použití v úlohách.

Orientované úhly modulo $360°$

Definice. Mějme čtveřici bodů $A \neq B$, $C \neq D$. Dvojice AB, CD je možné chápat jako „orientované přímky“, tedy přímky, u kterých je pořadím bodů A, B řečeno „z kterého směru přichází a kam míří“. Orientovaným úhlem orientovaných přímek AB a CD (v tomto pořadí) rozumíme úhel, o který je třeba otočit orientovanou přímku AB proti směru hodinových ručiček, aby měla stejný směr jako přímka CD. Tento úhel je určen jednoznačně až na násobek $360°$ a značíme ho $\sphericalangle(\overrightarrow{AB}, \overrightarrow{CD})$.

Tvrzení. *Pro orientované úhly orientovaných přímek platí:*

(i) $\sphericalangle(\overrightarrow{AB}, \overrightarrow{AB}) = 0$,

(ii) $\sphericalangle(\overrightarrow{AB}, \overrightarrow{CD}) = \sphericalangle(\overrightarrow{BA}, \overrightarrow{CD}) + 180° = \sphericalangle(\overrightarrow{BA}, \overrightarrow{DC})$,

(iii) $\sphericalangle(\overrightarrow{AB}, \overrightarrow{CD}) = -\sphericalangle(\overrightarrow{CD}, \overrightarrow{AB})$,

(iv) *pokud body A, B leží na jedné kružnici se středem S, pak $\sphericalangle(\overrightarrow{AS}, \overrightarrow{AB}) = \sphericalangle(\overrightarrow{BA}, \overrightarrow{BS})$; opačná implikace platí za předpokladu, že tento úhel není nulový,*

(v) $\sphericalangle(\overrightarrow{AB}, \overrightarrow{CD}) + \sphericalangle(\overrightarrow{CD}, \overrightarrow{EF}) = \sphericalangle(\overrightarrow{AB}, \overrightarrow{EF})$.

Důsledek. (součet úhlů v trojúhelníku) *Buďte A, B, C tři různé body v rovině. Pak*

$$\sphericalangle(\overrightarrow{AB}, \overrightarrow{AC}) + \sphericalangle(\overrightarrow{BC}, \overrightarrow{BA}) + \sphericalangle(\overrightarrow{CA}, \overrightarrow{CB}) = 180°.$$

Věta. (o středovém a obvodovém úhlu) *Body A, B, C leží na kružnici se středem S. Pak*

$$2 \cdot \sphericalangle(\overrightarrow{CA}, \overrightarrow{CB}) = \sphericalangle(\overrightarrow{SA}, \overrightarrow{SB}).$$

Věta. (o středovém a úsekovém úhlu) *Přímka AT se dotýká kružnice se středem S v bodě A. Dále na této kružnici leží bod B. Pak*

$$2 \cdot \sphericalangle(\overrightarrow{AT}, \overrightarrow{AB}) = \sphericalangle(\overrightarrow{SA}, \overrightarrow{SB}).$$

Orientované úhly modulo $180°$

Při zacházení s orientovanými přímkami je potřeba vědět, v jakém pořadí se nachází body na příslušných přímkách. Proto bývá často vhodnější volit orientované úhly modulo $180°$.

Definice. Orientovaným úhlem dvou (neorientovaných) přímek p, q (opět v tomto pořadí) rozumíme úhel, o který je třeba otočit přímku p proti směru hodinových ručiček, aby byla rovnoběžná s přímkou q. Tento úhel je dán jednoznačně až na násobek $180°$ a značíme jej $\sphericalangle(p, q)$. Je-li přímka p, resp. q určena body A, B, resp. C, D, pak úhel značíme obdobně jako úhel orientovaných přímek, tedy $\sphericalangle(AB, CD)$.

Tvrzení. *Pro orientované úhly neorientovaných přímek opět platí (i), (iii), (iv), (v) z tvrzení předchozí kapitoly.*

Tvrzení. (o tětivových čtyřúhelnících) *V rovině jsou dány 4 různé body A, B, C, D. Tyto body leží na jedné kružnici, právě když platí*

$$\sphericalangle(AC, AD) = \sphericalangle(CB, BD).$$

Úloha. Přímky p, q se protínají v bodě S. Dále jsou dány body A, B takové, že $\sphericalangle(p, SA) = \sphericalangle(SB, q)$. Paty kolmic z bodů A, B na přímku p označme postupně A_p, B_p a obdobně paty kolmic na přímku q jako A_q, B_q. Dokažte, že body A_p, A_q, B_p, B_q leží na jedné kružnici.

Úloha. (Miquelova věta) Je dán trojúhelník ABC. Na přímkách BC, CA, AB leží postupně body X, Y, Z. Dokažte, že kružnice opsané trojúhelníkům AYZ, XBZ a XYC prochází jedním bodem.

Úloha. Je dán rovnoramenný trojúhelník SAC se základnou AC. Na přímkách SA, SC leží postupně body X, Z tak, že přímka XZ je rovnoběžná s přímkou AC. Buď O střed kružnice opsané trojúhelníku AZS. Ukažte, že přímky XC a SO jsou na sebe kolmé.

Úloha. (Švrčkův bod) V trojúhelníku ABC označme $\check{S}$ druhý průsečík osy vnitřního úhlu u vrcholu A s kružnicí opsanou ABC. Dále označme $\check{S}'$ druhý průsečík osy vnějšího úhlu u vrcholu A s kružnicí opsanou. Nakonec označme středy kružnic připsaných ke stranám BC, CA, AB postupně I_a, I_b, I_c a střed kružnice vepsané I. Dokažte

(i) $|\check{S}B| = |\check{S}C| = |\check{S}I| = |\check{S}I_a|$,
(ii) $|\check{S}'B| = |\check{S}'C| = |\check{S}'I_c| = |\check{S}'I_b|$.

Úloha. Buď H průsečík výšek trojúhelníku ABC a H' obraz H v osové souměrnosti podle osy AB. Dokažte, že H' leží na kružnici opsané ABC.

Úloha. Skrz průsečík výšek H trojúhelníku ABC vedeme přímku p. Označme p_a, p_b osové obrazy přímky p podle přímek BC, CA. Dokažte, že se přímky p_a, p_b protínají na kružnici opsané.

Úloha. (Simsonova přímka) Buď P bod na kružnici opsané trojúhelníka ABC. Dokažte, že paty kolmic z P na strany trojúhelníka (3 body) leží v jedné přímce.

Přímka z předchozí úlohy se nazývá Simsonova přímka trojúhelníku ABC vzhledem k bodu P.

Úloha. Jsou dány body A, B, C, P na jedné kružnici. Kružnice k se dotýká přímky PA v bodě A a prochází bodem B. Druhý průsečík této kružnice s přímkou AC označme X. Dokažte, že přímka BX je kolmá na Simsonovu přímku trojúhelníku ABC vzhledem k bodu P.

Velká přirozená čísla

MIREK OLŠÁK

ABSTRAKT. Příspěvek se zamýšlí nad otázkou, jak definovat „co největší“ přirozené číslo. Začíná s několika pohledy na Ackermannovu funkci a dostává se do míst, na která konečná kombinatorika nestačí.

Motto: Vesmír je prťavý... oproti většině přirozených čísel.

Definice. Mějme dvě rostoucí posloupnosti přirozených čísel a_n, b_n. Řekneme, že posloupnost *a roste stejně rychle jako* posloupnost b, pokud najdeme k takové, že pro všechna n platí

$$a_n < b_{n+k} < a_{n+2k}.$$

Definice. Při mocnění a^{b^c} provádíme s vyšší prioritou mocnění výše a více vpravo, tedy $a^{(b^c)}$. Mocninnou věží o délce $n \in \mathbb{N}$ a základu $x \in \mathbb{N}$ rozumíme výraz

$$x^{x^{x^{\cdot^{\cdot^{\cdot^{x}}}}}},$$

ve kterém se vyskytuje x právě n-krát.

Cvičení. Pro $x \geq 2$ označme $v_x(n)$ posloupnost mocninných věží délky $n = 1, 2, \ldots$ Ukažte, že pro všechna možná x rostou posloupnosti v_x stejně rychle.

Definice. Pro $m, n \in \mathbb{N}_0$ definujeme m-tou Ackermannovu funkci $A_m(n)$ rekurentním předpisem

$$A_m(n) = \begin{cases} n+1 & \text{pro } m = 0, \\ A_{m-1}(1) & \text{pro } m > 0 \text{ a } n = 0, \\ A_{m-1}(A_m(n-1)) & \text{jinak.} \end{cases}$$

Dále definujeme Ackermannovu funkci (bez pořadového čísla) jako $A(n) = A_n(n)$.

Cvičení. Ukažte, že čtvrtá Ackermannova funkce roste stejně rychle jako mocninná věž.

Cvičení. Ukažte, že $A(n)$ roste stejně rychle jako $A_n(1)$.

Úloha. (IMO 2010) V každé ze šesti schránek B_1, B_2, B_3, B_4, B_5 a B_6 je na počátku jedna mince. Se schránkami můžeme provádět následující dvě operace:

(i) Vybrat neprázdnou schránku B_j , kde $1 \leq j \leq 5$, odebrat z ní jednu minci a přidat dvě mince do schránky $B_j + 1$.
(ii) Vybrat neprázdnou schránku B_k, kde $1 \leq k \leq 4$, odebrat z ní jednu minci a navzájem vyměnit obsahy (případně prázdných) schránek B_{k+1} a B_{k+2}.

Rozhodněte, zda je možné pomocí konečného počtu těchto operací dosáhnout toho, aby schránky B_1, B_2, B_3, B_4 a B_5 byly prázdné a schránka B6 obsahovala právě $2010^{2010^{2010}}$ mincí.

Návod. Ukažte, že maximální dosažitelný počet mincí roste v závislosti na počtu schránek stejně rychle jako Ackermannova funkce.

Definice. Je dáno přirozené číslo n. Pan Goodstein si toto číslo rozepíše na součet bodle binární soustavy, dále exponenty, exponenty exponentů, ... Například číslo 35 rozepíše jako

$$2^{2^2+1} + 2 + 1.$$

Nyní všechny dvojky nahradí trojkami a následně odečte jedničku. Rozepíše toto číslo v trojkové soustavě, všechny trojky změní na čtyřky a opět odečte jedničku. Takto postupně zvyšuje soustavu a odečítá jedničku, až nakonec odbourá všechny členy tohoto čísla a získá nulu. Definujeme Goodsteinovu funkci $G(n)$, která vrátí číslo pozice, na níž se v Goodsteinově postupu jako první objevila nula.

Tvrzení. *Goodsteinův postup vždy skončí, tedy Goodsteinova funkce je dobře definovaná.*

Definice. Goodsteinův postup je možné vnímat formálně jako „odbourávání“ z jistého výrazu obsahujícího proměnnou x (základ soustavy). Při každém odbourání se přitom některá x promění na číslo kroku, ve kterém k tomu došlo. Představme si tedy, že Goodstein začíná s výrazem $V(x)$, kde x je na začátku rovno n a v každém kroku vzroste o 1. Definujeme pseudo-Goodsteinovo číslo $g_{V(x)}(n)$ jako první nulu v takovém postupu.

Cvičení. Ukažte, že g_{x^x} roste rychle jako Ackermannova funkce.

Návod. Dokažte $A_{k+1}(n) < g_{x^k}(n + 2) < A_{k+1}(2n + 2)$.

Definovatelnost

Všechna doposud jmenovaná čísla jsme definovali pomocí vcelku krátkého českého textu. Když je chceme přebít, co takhle si vzít největší číslo definovatelné tisíci nebo méně českými slovy.

Toto má jistý zádrhel, pokud bychom vzali „největší číslo definovatelné tisíci nebo méně českými slovy plus jedna“, získali bychom číslo, které se méně než tisíci českými slovy definovat nedá. Přesto jsme ho tak definovali. Dostáváme spor, jenže s čím?

Problém je v tom, že čeština (stejně jako jiné přirozené jazyky) je málo exaktní na to, aby se o ni opírala matematická definice (například může mluvit sama o sobě). Můžeme však vytvořit jiný jazyk, u kterého bude vždy jasné, které číslo definuje. Ukážeme si dva příklady.

Definice. Turingův stroj je automat, který stojí na jednom políčku nekonečné (na obě strany) pásky. Na začátku je na všech políčkách nula. Stroj může v průběhu měnit číslo, na kterém stojí, a posouvat se po pásce. Současně je tento stroj v každém okamžiku v jednom z k stavů. Kód Turingova stroje spočívá v popsané instrukci pro každou dvojici (stav, číslo pod strojem). Instrukce má tři části: 1) změň nebo ponechej číslo pod sebou, 2) posuň se doprava, doleva, nebo zůstaň stát, 3) přepni se do jiného stavu nebo se vypni.

Číslo definované Turingovým strojem, který se někdy vypne, se dá chápat například jako počet kroků, které do té doby udělal.

Tvrzení. *Turingův stroj umí provést všechno, co umí provést počítač.*

Definice. (číslo definovatelné v aritmetice $\mathbb{N}_0$) Mějme formuli, tedy „syntakticky správnou“ konečnou posloupnost kvantifikátorů, znamének (plus, krát, mocnění), logických spojek, rovnítek, jedniček, nul, neznámých a závorek. Předpokládáme, že v této formuli je pouze proměnná x nekvantifikovaná. Pak určíme číslo definované touto formulí jako nejmenší takové x (existuje-li), pro které daná formule platí. Například formule

$$\exists a\, \exists b\, (x = a \cdot a \cdot a \wedge x = b \cdot b + 1 + 1)$$

definuje číslo 27.

Tvrzení. *Pomocí aritmetiky v $\mathbb{N}_0$ je možné definovat Turingův stroj.*

Pokud přijmeme teorii množin za základ matematiky, umožní nám to popsat ještě mnohem větší (stále však přirozené) číslo. Bohužel však vysvětlovat všechny pojmy jeho definice by bylo příliš zdlouhavé, takže je zde neuvádím.

Definice. Uvažujme všechny sentence φ v jazyce teorie množin, pro které je třída všech množin tvaru V_α (pro α ordinál), ve kterých φ platí, množinou. Označme S sjednocení všech těchto množin. Jako TeMné číslo označíme největší přirozené číslo definovatelné v S v jazyce teorie množin pomocí formule délky nejvýše $A(4)$.

Tělesa

Alexander „Olin“ Slávik

Úvod

Tělesa jsou algebraické struktury, které mají velmi příjemné vlastnosti – jsou „šité na míru“ tak, aby se s nimi dalo počítat podobně jako třeba s reálnými čísly. I přes to, jak je jejich struktura striktně zadána, lze u nich pozorovat zajímavé odlišnosti a jevy.

Definice. Množinu $\mathbb{F}$ spolu s binárními operacemi $+$ a $\cdot$ a „význačnými“ prvky 0 a 1 nazveme *(komutativním) tělesem*, pokud pro všechna $x, y, z \in \mathbb{F}$ platí následující vztahy:

(i) $x + (y + z) = (x + y) + z$,
(ii) $x + y = y + x$,
(iii) $x + 0 = x$,
(iv) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
(v) $x \cdot y = y \cdot x$,
(vi) $x \cdot 1 = x$,
(vii) $x \cdot (y + z) = x \cdot y + x \cdot z$,
(viii) existuje prvek $-x \in \mathbb{F}$ takový, že $x + -x = 0$,
(ix) je-li $x \neq 0$, pak existuje prvek $x^{-1} \in \mathbb{F}$ takový, že $x \cdot x^{-1} = 1$.

Příklady. Uveďme pár (více či méně obvyklých) příkladů těles:

(i) reálná čísla $\mathbb{R}$,
(ii) komplexní čísla $\mathbb{C}$,
(iii) racionální čísla $\mathbb{Q}$,
(iv) zbytky modulo p s operacemi modulo p $\mathbb{Z}_p$,
(v) čtyřprvkové těleso (množina $\{0, 1, a, b\}$ s operacemi danými vztahy $0 = 1 + 1 = a + a = b + b$, $a + b = 1$, $a \cdot b = 1$, $a \cdot a = b$, $b \cdot b = a$),
(vi) racionální funkce (tj. podíly polynomů),
(vii) Laurentovy řady (tj. formální sumy tvaru $\sum_{k=n}^{\infty} a_k x^k$, kde $n \in \mathbb{Z}$ a a_k jsou prvky nějakého předem zvoleného tělesa).

Vlastnosti těles

Definice. *Charakteristika tělesa* $\mathbb{F}$ je nejmenší přirozené číslo n takové, že v $\mathbb{F}$ platí rovnost

$$\underbrace{1+1+\cdots+1}_{n} = 0.$$

Pokud takové $n \in \mathbb{N}$ neexistuje, říkáme, že $\mathbb{F}$ má charakteristiku 0.

Cvičení. Je-li charakteristika tělesa nenulová, pak je to již nutně prvočíslo.

Cvičení. Zřejmě má každé konečné těleso nenulovou charakteristiku. Ukažte, že opačná implikace nemusí platit, tj. najděte nekonečné těleso s nenulovou charakteristikou.

Definice. Řekneme, že těleso $\mathbb{F}$ je algebraicky uzavřené, pokud každý nekonstantní polynom s koeficienty z $\mathbb{F}$ má v $\mathbb{F}$ aspoň jeden kořen.

Věta. (Základní věta algebry) *Těleso $\mathbb{C}$ je algebraicky uzavřené.*

Pozorování. *Na rozdíl od reálných čísel není možné komplexní čísla „přirozeně“ uspořádat, tj. není možné na nich zavést nějaké uspořádání $\preceq$ takové, že by pro všechna $x, y, z \in \mathbb{C}$ platilo:*

(i) *je-li $x \preceq y$, pak také $x + z \preceq y + z$,*
(ii) *platí-li $0 \preceq x$ a $0 \preceq y$, pak také $0 \preceq xy$.*

Cvičení. Ukažte, že žádné konečné těleso není algebraicky uzavřené.

Konstrukce těles

Cvičení. Mějme strukturu podobnou tělesu, ve které platí všechny podmínky z úvodní definice kromě poslední (existence inverzních prvků)[1] – takovou strukturou jsou například celá čísla. Je možné tuto strukturu doplnit o další prvky (a dodefinovat na této větší množině operace $+$, $\cdot$) tak, aby výsledná množina byla tělesem?

Cvičení. Ukažte, že racionální funkce je možné vnořit jakožto podtěleso do Laurentových řad.

Cvičení. Představme si, že máme těleso $\mathbb{F}$ a někdo nám „přinese“ úplně nový prvek x, který chce do tělesa „přidat“. Co všechno ještě musíme k $\mathbb{F} \cup \{x\}$ přidat, abychom dostali zase těleso?

Cvičení. Situace jako v předchozím cvičení, ale požadavek navíc je, aby x splňovalo $x^2 + 1 = 0$, případně nějakou jinou polynomiální rovnici. Která známá tělesa takto umíme získat?

[1] Takové struktury se nazývají *okruhy*.

Definice. Mějme těleso $\mathbb{F}$ a jeho podtěleso $\mathbb{T}$. Prvek $x \in \mathbb{F}$ se nazývá *algebraický nad* $\mathbb{T}$, pokud je kořenem nějakého polynomu s koeficienty z $\mathbb{T}$, v opačném případě je *transcendentní nad* $\mathbb{T}$.

Příklad. $\sqrt{2}$ je algebraická nad $\mathbb{Q}$, ovšem například π není.

Věta. *Pro každé těleso $\mathbb{F}$ existuje nadtěleso $\overline{\mathbb{F}}$ s následujícími vlastnostmi:*

(i) *$\overline{\mathbb{F}}$ je algebraicky uzavřené,*
(ii) *pokud těleso $\mathbb{T}$ splňuje $\mathbb{F} \subseteq \mathbb{T} \subseteq \overline{\mathbb{F}}$ a je algebraicky uzavřené, pak $\mathbb{T} = \overline{\mathbb{F}}$ (neboli $\overline{\mathbb{F}}$ je „nejmenší“ algebraicky uzavřené nadtěleso $\mathbb{F}$),*
(iii) *je-li $\mathbb{S}$ nadtěleso $\mathbb{F}$ splňující body (i) a (ii), pak jsou $\mathbb{S}$ a $\overline{\mathbb{F}}$ isomorfní (tj. algebraicky „stejná“).*

Výše uvedené těleso $\overline{\mathbb{F}}$ se nazývá algebraický uzávěr $\mathbb{F}$.

Příklad. $\overline{\mathbb{R}} = \mathbb{C}$. $\overline{\mathbb{Q}}$ je tvořeno právě všemi komplexními čísly algebraickými nad $\mathbb{Q}$.

Pickova formule

Helča Svobodová

Abstrakt. Příspěvek seznamuje čtenáře se zněním Pickovy formule pro počítání obsahů mnohoúhelníků s vrcholy v mřížových bodech. Dále je zde nastíněn důkaz tvrzení a uvedeno několik příkladů na toto téma.

Určitě už ses mnohokrát setkal(a) s takovýmto příkladem: Vypočítej obsah mnohoúhelníku nakresleného na obrázku! Obvykle se snažíme útvar vhodně rozdělit na obdélníky a trojúhelníky a sečíst jejich obsah. Pro mnohoúhelník, jehož vrcholy leží v takzvaných mřížových bodech, tedy v bodech s celočíselnými souřadnicemi, ale existuje mnohem elegantnější metoda. Vymyslel ji v roce 1899 pan George Pick a umožňuje nám spočítat hledaný obsah jen pomocí znalosti počtu mřížových bodů, které v mnohoúhelníku leží. V přednášce se na tuto formuli blíže podíváme a kromě počítání obsahů pak dokážeme vyřešit i pár zajímavých problémů.

Tvrzení. (Pickova formule) *Mějme jednoduchý mnohoúhelník s vrcholy v mřížových bodech. Označme V počet mřížových bodů, které jsou uvnitř mnohoúhelníku, a H buď počet mřížových bodů, které jsou na jeho hranici. Hledaný obsah je pak roven $V + \frac{H}{2} - 1$.*

Důkaz provedeme na přednášce, zde jen nastíníme, kudy se ubírá:

(i) Platí-li Pickova formule pro nějaké dva mnohoúhelníky se společnou částí obvodu, platí i pro mnohoúhelník, který dostaneme, když je spojíme.
(ii) Vzoreček platí pro jednotkový čtverec, a tedy i pro libovolný obdélník.
(iii) Vzoreček platí i pro jakýkoli trojúhelník.
(iv) Pickova formule platí pro všechny mnohoúhelníky.

Příklad 1. Mějme mřížku o hraně délky $\sqrt{2}$. Dokažte, že každý mnohoúhelník s vrcholy v bodech této mřížky má celočíselný obsah.

Příklad 2. Platí nějaká obdoba Pickovy formule i v prostoru?

Příklad 3. A co v trojúhelníkové mřížce?

Příklad 4. Půlbodem nazývejme libovolný bod v mřížce o souřadnicích $(k/2, l/2)$, kde k a l jsou lichá čísla. Každý půlbod lze určitě vyjádřit mnoha různými způsoby jako střed úsečky spojující dva mřížové body. Mějme půlbod ležící uvnitř nějakého mřížového mnohoúhelníku. Dokažte, že jej lze vyjádřit jako střed úsečky spojující dva mřížové body, které samy leží v tomto mnohoúhelníku.

Příklad 5. (Varianta Pickova vzorce pro nejednoduchý mnohoúhelník) Dokažte, že obsah mnohoúhelníku, který obsahuje D „děr“, je roven $V+H/2+D-1$. H je počet mřížových bodů na všech $D+1$ uzavřených křivkách tvořících hrany mnohoúhelníku.

Příklad 6. 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 pak těžištěm trojúhelníku ABC.

Literatura a zdroje

[1] přednáška Jardy Hančla, soustředění Staré Město 2009
[2] archiv PraSátka (20. ročník, povídání k 5. sérii)
[3] *http://www.mast.queensu.ca/~murty/murty-thain.pdf*
[4] *www.wikipedia.org*
[5] *www.math.kent.edu/~soprunova/64091f12/hw5.pdf*

Kružnicová inverzia

VIKTOR SZABADOS

ABSTRAKT. Prednáška je určená hlavne pre tých, čo o kružnicovej inverzii ešte nepočuli. Cieľom prednášky je oboznámiť poslucháča so základnými vlastnosťami kružnicovej inverzie a ponúknuť mu „nový nástroj“ na riešenie geometrických úloh, ktorého použitie si následne môže vyskúšať na príkladoch.

Sila tohto zobrazenia spočíva v tom, že dokáže previesť tvrdenia o kružniciach na tvrdenia o priamkach. Často sa komplikovaná geometrická situácia po vhodnom zobrazení inverziou zmení na jednoduchú a prístupnú klasickým metódam planimetrie. Inverzia má využitie nielen v matematických súťažiach, ale napríklad aj v algoritmoch počítajúcich prieniky kruhov.

Dohoda. Rovinu rozšírme o jediný bod ∞, o ktorom tvrdíme, že leží na všetkých priamkach.

Definícia. *Kružnicová inverzia* je geometrické zobrazenie určené kružnicou k so stredom O a polomerom r, ktoré bodu A priradí bod A' podľa nasledujúcich pravidiel:

(i) Ak je $A = O$, potom $A' = \infty$.
(ii) Ak je $A = \infty$, potom $A' = O$.
(iii) Inak je A' bod polpriamky OA, pre ktorú platí

$$|OA| \cdot |OA'| = r^2.$$

Cvičenie. Je takto určené geometrické zobrazenie bijektívne?

Cvičenie. Má takéto zobrazenie nejaký samodružný bod (tj. bod, ktorý sa zobrazí sám na seba)?

Pri riešení týchto cvičení ste možno prišli na to, ako sa inverzia správa k bodom „vnútri“ kružnice $k(O, r)$, a celkovo ste si mohli všimnúť nasledujúce vlastnosti:

(i) Body kružnice k sú samodružné.
(ii) Ak leží bod A „vnútri“ kružnice k, leží obraz A' „vonku“ a naopak.
(iii) Inverzia prevedená dvakrát podľa rovnakej kružnice je identita.

Tvrdenie. (Konštrukcia obrazu) *Pre zadanú kružnicu k a jej vonkajší bod A označme T, U body dotyku kružnice k s jej dotyčnicami vedenými bodom A. Potom obraz A' bodu A v kružnicovej inverzii podľa kružnice k je stred úsečky TU.*

Kružnicová inverzia nie je zhodné ani podobné zobrazenie. Napriek tomu dokážeme vyjadriť vzdialenosť obrazov dvoch bodov pomocou polohy ich vzorov a kružnice inverzie.

Lema. *Je zadaná kružnica $k(O, r)$ a body X, Y. Označme X', Y' obrazy bodov X, Y v inverzii podľa kružnice k. Platí:*

(i) $|\sphericalangle OX'Y'| = |\sphericalangle XYO|$,
(ii) $|X'Y'| = |XY|\frac{r^2}{|OX|\cdot|OY|}$,
(iii) $|XY| = |X'Y'|\frac{r^2}{|OX'|\cdot|OY'|}$.

Vyzerá to dosť komplikovane: vzdialenosť obrazov závisí od $|OX|$ aj $|OY|$ a nevidno z toho, ako inverzia mení vzdialenosti. Napriek tomu je tento vzťah na niečo užitočný, ako sa presvedčíme na príkladoch.

Tvrdenie. *Uvážme kružnicovú inverziu určenú kružnicou k so stredom O. Potom platí:*

(i) *Obrazom priamky prechádzajúcej bodom O je ona sama.*
(ii) *Obrazom priamky neprechádzajúcej bodom O je kružnica.*
(iii) *Obrazom kružnice prechádzajúcej bodom O je priamka.*
(iv) *Obrazom kružnice neprechádzajúcej bodom O je kružnica.*

Poznámka. Pozor! Kružnicová inverzia síce celkom často zobrazuje kružnice na kružnice, všeobecne ale neplatí, že by sa na seba zobrazili aj ich stredy.

Vyzbrojení týmito poznatkami si môžeme trúfnuť vyriešiť niekoľko úloh.

Príklad. V rovine sú dané dve kružnice k, ℓ s priesečníkmi A, B. Vezmime priamku p prechádzajúcu bodom B, jej druhý priesečník s kružnicou k označme C, jej druhý priesečník s kružnicou ℓ označme D. Dokážte, že veľkosť uhla CAD nezávisí od polohy priamky p.

Riešenie. Zaujíma nás veľkosť uhla zovretého priamkami AC a AD. Obe tieto priamky prechádzajú bodom A, navyše týmto bodom prechádzajú aj obe kružnice k, ℓ. Zobrazme teda celú situáciu v inverzii so stredom A a nejakým polomerom r. Obrazmi kružníc k, ℓ budú priamky k', ℓ' s priesečníkom B'. Obrazom priamky p je kružnica p', ktorá prechádza bodom A. Táto kružnica pretína priamku k' po druhýkrát v bode C' a priamku ℓ' po druhýkrát v bode D'.

Máme tri možné poradia, ako môžu na kružnici p' ležať tieto body: A, C', B', D', alebo A, B', C', D', alebo A', C', D', B'. Vo všetkých troch prípadoch je veľkosť uhla $C'AD'$ rovná veľkosti uhla zovretého priamkami k', ℓ' – toho, v ktorom neleží bod A. A to je presne to, čo sme chceli dokázať. $\square$

Cvičenie. Pomôcka k nasledujúcemu príkladu. Dokážte bez použitia inverzie. Je daný trojuholník ABC so stredom vpísanej kružnice I (v angličtine sa tento bod nazýva *incenter*). Dokážte, že os strany AB, os uhla ACB a kružnica opísaná trojuholníku ABC sa pretínajú v jednom bode. Označme tento bod S. Dokážte, že S je stred kružnice opísanej trojuholníku ABI.

Príklad 1. V rovine sú dané tri zhodné kružnice, ktoré prechádzajú spoločným bodom H. Označme druhé priesečníky týchto kružníc A, B, C (rôzne od H). Dokážte, že H je ortocentrum trojuholníka ABC.

Príklad 2. Priamka p pretne kružnicu k v bodoch X, Y. Označme R stred oblúku XY. Bodom R vedieme dve priamky, ktoré pretnú kružnicu k v bodoch A, B a priamku p v bodoch C, D. Ukážte, že body A, B, C, D ležia na jednej kružnici.

Príklad 3. (Ptolemaiova nerovnosť) Nech $ABCD$ je štvoruholník. Potom platí:

$$|AB| \cdot |CD| + |BC| \cdot |AD| \geq |AC| \cdot |BD|,$$

rovnosť nastáva práve vtedy, keď je štvoruholník $ABCD$ tetivový.

Príklad 4. Kružnice k_1, k_2 sa pretínajú v bodoch A, B. Kružnica k_3 sa zvonku dotýka kružníc k_1, k_2 po poradí v bodoch C, E. Kružnica k_4 sa zvonku dotýka kružníc k_1, k_2 po poradí v bodoch D, F. Dokážte, že kružnica opísaná trojuholníku ACE sa dotýka kružnice opísanej trojuholníku ADF. (Poľská MO 2004)

Príklad 5. V rovine sú dané dve kružnice k, ℓ s priesečníkmi A, C. V bode A spravíme dotyčnicu ku k, tá druhýkrát pretne kružnicu ℓ v bode D. Bod B je priesečníkom kružnice k s dotyčnicou ku kružnici ℓ v bode A. Dokážte, že $|AB| \cdot |CD| = |AC| \cdot |AD|$.

Príklad 6. Kružnica ℓ sa zvnútra dotýka kružnice k v bode A. Zvolíme bod B na kružnici ℓ. Dotyčnica ku ℓ v bode B pretne kružnicu k v bodoch D, E. Označme C stred toho oblúka DE kružnice k, ktorý neobsahuje bod A. Dokážte, že body A, B, C ležia na priamke.

Príklad 7. Dané sú kružnice k_1, k_2, k_3, k_4 tak, že k_i sa zvonka dotýka k_{i+1} pre $i = 1, 2, 3, 4$ ($k_5 = k_1$). Dokážte, že štyri dotykové body týchto kružníc ležia na jednej kružnici.

Príklad 8. Kružnice k_1, k_2 sa zvonka dotýkajú v bode D. Priamka p sa dotýka kružníc k_1, k_2 po rade v (rôznych) bodoch A, B. Úsečka AC je priemerom kružnice k_1. Priamka q prechádza cez bod C a dotýka sa kružnice k_2 v bode E. Dokážte, že trojuholník ACE je rovnoramenný. (Poľská MO 2004)

Zvyšné úlohy sú prevzaté a mali by sa dať riešiť inverziou, neskúmal som ich podrobne.

Príklad 9. Daný je trojuholník ABC. Vnútri strán CA, CB ležia v tomto poradí body Y, X. Nech P je priesečník uhlopriečok štvoruholníka $ABXY$. Nech Q je priesečník kružníc opísaných trojuholníkom BYC a AXC rôzny od bodu C. Dokážte, že body P, Q, C ležia na priamke práve vtedy, keď je štvoruholník $ABXY$ tetivový.

Príklad 10. Dané sú dve kružnice k, ℓ pretínajúce sa v bodoch D a A. Spoločná dotyčnica týchto kružníc bližšia k bodu A sa dotýka kružnice k v bode E a kružnice ℓ v bode F. Rovnobežka so spoločnou dotyčnicou prechádzajúca bodom D pretína kružnicu k v bode C a kružnicu ℓ v bode B (tieto body sú rôzne od bodu D). Dokážte, že druhý priesečník (rôzny od bodu D) kružníc opísaných trojuholníkom CDF a BDE leží na priamke AD.

Príklad 11. V rovine je daný trojuholník DEF a tri body A, B, C. Dokážte, že existuje kružnica taká, že keď podľa nej urobíme inverziu, tak obrazy A', B' C' bodov A, B, C vytvoria trojuholník $A'B'C'$ podobný trojuholníku DEF.

Príklad 12. Dve kružnice sa dotýkajú zvonka v bode A. Do krivočiareho trojuholníka určeného týmito kružnicami a ich spoločnou dotyčnicou vpíšeme kružnicu so stredom O a polomerom r. Dokážte, že $|AO| \le 3r$.

Príklad 13. Kružnice k_1, k_2 sa pretínajú v bodoch A, B. Priamka rôzna od AB pretína kružnicu k_1 v bodoch C, D, kružnicu k_2 v bodoch E, F a priamku AB v bode P ležiacom mimo úsečky AB. Dokážte, že priamka spájajúca stredy kružníc opísaných trojuholníkom ACE a BDF prechádza bodom P. (Poľská MO 2002)

Príklad 14. Nech ABC je trojuholník s opísanou kružnicou k a nech D je bod na strane BC. Dokážte, že kružnice dotýkajúce sa k, AD, AB a k, AD, DC sa navzájom dotýkajú práve vtedy, keď uhly BAD a CAD majú rovnakú veľkosť. (Rumunsko 1997)

Hinty k príkladom

Hint k pr. 1. Stačí ukázať, že AH je kolmé na BC a využiť predchádzajúce cvičenie.

Hint k pr. 2. Uvážte inverziu so stredom R, ktorá zobrazí p na k, a všimnite si, že body C, D prejdú na body A, B.

Hint k pr. 3. Čo pripomína dokazovaný vzťah?

Hint k pr. 4. Preč s kružnicami! Ako sa zmení dokazované tvrdenie?

Hint k pr. 5. Vieme sa vhodnou inverziou zbaviť nejakých kružníc?

Hint k pr. 6. Dá sa robiť inverzia tak, aby sa kružnica k zobrazila na priamku DE?

Hint k pr. 7. Za stred inverzie zvoľte ľubovoľný dotykový bod a využite rovnoľahlosť.

Hint k pr. 8. Skúste použiť inverziu so stredom v bode C a polomerom $|CA|$.

Literatúra a zdroje:

Pri tvorbe prednášky som väčšinu čerpal zo starších príspevkov Jozefa „Pepu“ Tkadleca a Michala „Kennyho“ Rolínka a z prednášok Jána „Maza“ Mazáka, ktorým by som týmto veľmi rád poďakoval.

[1] *http://www.mathlinks.ro*
[2] Archív MKS, *http://mks.mff.cuni.cz/archiv*
[3] *http://www.kms.sk/~mazo/matematika/matematika.php*

Konstrukce kružítkem

MARTINA VAVÁČKOVÁ

„Každou geometrickou konstrukci, kterou lze provést pravítkem a kružítkem, lze provést samotným kružítkem.“

Toto pozorování učinil již roku 1672 dánský matematik Georg Mohr, nikdo mu však v té době nevěnoval velkou pozornost. Stejnou větu dokázal v roce 1797 Lorenzo Mascheroni, jenž sklidil podstatně větší úspěch. Proto dnes mluvíme o konstrukcích pomocí kružítka jako o *mascheroniovských* konstrukcích.

Poznámka. Leckdo by mohl namítat, že výše zmíněný výrok neplatí, protože pouhým kružítkem přece nejsme schopni sestrojit přímku (neumíme totiž nakreslit rovnou čáru). My však budeme v tomto textu chápat přímku jako dvojici navzájem různých bodů, jimiž je jednoznačně určena.

Veškeré konstrukce pravítkem a kružítkem se dají poskládat ze tří elementárních konstrukcí:

(i) Sestrojení průsečíku dvou kružnic.
(ii) Sestrojení průsečíku přímky a kružnice.
(iii) Sestrojení průsečíku dvou přímek.

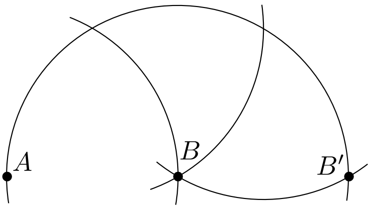
Naším cílem bude ukázat, že každou z nich zvládneme stejně dobře i bez pomoci pravítka. Pojďme na to!

Příklady

Budeme-li v následujících příkladech mluvit o úsečce AB, resp. přímce AB, máme vždy na mysli body A, B, které ji určují.

Příklad 1. K zadané úsečce AB sestrojte úsečku dvakrát delší.

Řešení. Sestrojíme kružnici se středem B procházející bodem A. Na ni naneseme z bodu A třikrát za sebe tutéž vzdálenost a dostaneme tak bod B'. Úsečka AB' je pak zřejmě dvakrát delší než úsečka AB.



Příklad 2. Mějme přímku AB a bod C, který na ní neleží. Sestrojte obraz bodu C v osové souměrnosti podle přímky AB.

Příklad 3. Jsou dány body A, B, C, které neleží v jedné přímce. Najděte bod D tak, aby $ABCD$ byl rovnoběžník.

Příklad 4. Je dána přímka AB a kružnice k se středem O. Předpokládejme, že bod O neleží na přímce AB. Najděte průsečík přímky AB a kružnice k.

Příklad 5. Zjistěte, zda dané tři body A, B a C leží na jedné přímce.

Příklad 6. K zadané úsečce AB najděte bod C tak, aby platilo $AC \perp AB$.

Příklad 7. Najděte střed zadané úsečky AB.

Příklad 8. Body A, B leží na kružnici se středem O. Rozdělte oblouk AB na poloviny.

Příklad 9. Je dána přímka AB a kružnice k se středem O tak, že O leží na AB. Najděte průsečík přímky AB a kružnice k.

Příklad 10. Sestrojte čtverec o straně AB.

Příklad 11. Nechť a, b, c jsou délky tří daných úseček. Najděte délku x tak, aby platilo $\frac{a}{b} = \frac{c}{x}$.

Příklad 12. Jsou dány přímky AB a CD. Najděte jejich průsečík.

Příklad 13. Sestrojte kružnici opsanou trojúhelníku ABC.

Příklad 14. Sestrojte pravidelný pětiúhelník.

Zdroje

[1] 1. série 10. ročníku MKS *http://mks.mff.cuni.cz/*
[2] *http://www.cut-the-knot.org/do_you_know/compass.shtml*
[3] *http://www.apolloniovyulohy.webz.cz/masch.htm*

Konečné součty

Martina Vaváčková

Konečnými součty rozumíme součty konečně mnoha sčítanců. Vedle konečných součtů existují i součty nekonečné, ale těmi se zde zabývat nebudeme.

Některé konečné součty lze spočítat standardními metodami, jiné vyžadují jistou dávku invence. Samozřejmě ne vždy se dá součet zapsat v „pěkném“ tvaru – dokonce ani v případě, že se na první pohled tváří velmi jednoduše (například $\sum_{k=1}^{n} \frac{1}{k}$).

Nyní si přiblížíme několik postupů, jež se při sčítání řad mohou hodit:

(i) představíme si daný součet v obráceném pořadí – aritmetická řada,
(ii) vhodně součet vynásobíme a získanou rovnost odečteme od té původní – geometrická řada,
(iii) využijeme Pascalův trojúhelník, binomickou větu a jiné kombinatorické identity,
(iv) pokusíme se každý člen vyjádřit jako rozdíl dvou podobně vypadajících členů – teleskopická řada.

Tvrzení. (Pascalův trojúhelník) *Pro nezáporná celá čísla n, k ($n \geq k$) platí*

$$\binom{n}{k} = \binom{n}{n-k},$$
$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Věta. (Binomická) *Pro libovolná $A, B \in \mathbb{R}$ platí*

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k},$$

speciálně $2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$.

Definice. Pro dané $k \in \mathbb{N}$ a $q \neq 0$ označme

$$R_{q,k}(n) = \sum_{i=1}^{n} i^k q^i.$$

Dále definujme $S_k = R_{1,k}$, tedy S_k vyjadřuje součet k-tých mocnin prvních n přirozených čísel.

Tvrzení. *Pro libovolná q, k je možné řady S_k a $R_{q,k}$ sečíst. Přesněji, $R_{q,k}$ je vyjádřitelné jako $q^n P(n)$, kde P je polynom stupně k.*

Cvičení. Určete S_1, S_2, $R_{q,1}$.

Příklady

Příklad 1. $S = 1 - 2 + 3 - 4 + \cdots + (-1)^{n+1} n$

Příklad 2. $S = (x + \frac{1}{x})^2 + (x^2 + \frac{1}{x^2})^2 + \cdots + (x^n + \frac{1}{x^n})^2$

Příklad 3. $S = 1\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n}$

Příklad 4. $S = 1\binom{n}{1} - 2\binom{n}{2} + \cdots + (-1)^{n+1} n\binom{n}{n}$

Příklad 5. $S = 1^2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + n^2\binom{n}{n}$

Příklad 6. $S = \frac{2^2}{2}\binom{n}{1} + \frac{2^3}{3}\binom{n}{2} + \cdots + \frac{2^{n+1}}{n+1}\binom{n}{n}$

Příklad 7. $S = \frac{1}{1!(2n-1)!} + \frac{1}{3!(2n-3)!} + \frac{1}{5!(2n-5)!} + \cdots + \frac{1}{(2n-1)!1!}$

Příklad 8. $S = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}$

Příklad 9. $S = \frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)}$

Příklad 10. $S = \frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \cdots + \frac{1}{n(n+1)(n+2)}$

Příklad 11.

$$S = \sum_{k=1}^{n} \frac{2k+1}{k^2(k+1)^2}$$

Zdroje

[1] Jiří Herman, Radan Kučera, Jaromír Šimša: *Metody řešení matematických úloh I.* Masarykova univerzita v Brně, 2001

[2] Pavel Šalom: *Konečné součty* (Sborník MKS, Rapotín 2007)

Vytvořující funkce

Lukáš Zavřel

Abstrakt. Cílem tohoto příspěvku je seznámit se základním využitím vytvořujících funkcí, a to zejména na kombinatorických úlohách. Dále uvede čtenáře do nejzákladnější problematiky práce s mocninnými řadami.

Co jsou to vlastně vytvořující funkce?

Vytvořující funkce jsou krásným odvětvím nebo spíše metodou matematiky. Oplývají spoustou teorie a zajímavých výsledků, které se s jejich použitím dají odvodit. Ale jsou také nečekaně účinné při boji s pro nás tak známými kombinatorickými úlohami. Použití vytvořujících funkcí je sice velký trik, ale práce s nimi nakonec není tak těžká a úlohu předtím nepřístupnou dokáží snadno vyřešit. Jdeme na to:

Definice. Nechť $(a_0, a_1, a_2, \dots)$ je posloupnost reálných čísel. Potom funkce daná předpisem

$$a(x) = \sum_{i=0}^{\infty} a_i \cdot x^i = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots$$

se nazývá vytvořující funkce posloupnosti $(a_0, a_1, a_2, \dots)$.

Příklad. Mějme dvě krabičky, ve kterých se nacházejí lístečky s čísly mezi 1 a 10. V první jsou pouze lístečky se sudými čísly a ve druhé s prvočísly. Ptejme se, kolika způsoby lze vybrat po jednom lístečku z každé krabičky tak, že součet čísel na těchto lístečcích je 11.

Příklad. Najděte vytvořující funkci ke geometrické řadě $1 + x + x^2 + \cdots$.

Operace s vytvořujícími funkcemi

Zatím známe vytvořující funkci jenom jedné nekonečné posloupnosti. Nyní si ukážeme několik operací, které nám dovolí určit vytvořující funkce mnoha dalších posloupností.

Násobení reálným číslem (O1). Mějme funkci $f(x)$, která je vytvořující funkcí posloupnosti $(a_0, a_1, \dots)$ a t reálné. Potom funkce $tf(x)$ je vytvořující funkcí posloupnosti $(ta_0, ta_1, \dots)$.

Sčítání (O2). Mějme dvě funkce $f(x)$ a $g(x)$, které jsou po řadě vytvořujícími funkcemi posloupností $(a_0, a_1, \dots)$ a $(b_0, b_1, \dots)$. Potom $f(x) + g(x)$ je vytvořující funkcí posloupnosti $(a_0 + b_0, a_1 + b_1, \dots)$.

Posouvání posloupnosti doprava (O3). Mějme funkci $f(x)$, která je vytvořující funkcí posloupnosti $(a_0, a_1, \dots)$. Potom $x^n f(x)$ je vytvořující funkcí posloupnosti $(\underbrace{0, 0, \dots, 0}_{n}, a_0, a_1, \dots)$.

Posouvání posloupnosti doleva (O4). Mějme funkci $f(x)$, která je vytvořující funkcí posloupnosti $(a_0, a_1, \dots)$. Tentokrát si ji už pro názornost rozepišme, tj.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots .$$

Potom

$$\frac{f(x) - a_0 - a_1 x - \cdots a_{n-1} x^{n-1}}{x^n} = a_n + a_{n+1} x + a_{n+2} x^2 + \cdots , \qquad (\star)$$

dostáváme tedy, že $(\star)$ je vytvořující funkcí posloupnosti $(a_n, a_{n+1}, \dots)$.

Dosazení x^n za x (O5). Mějme funkci $f(x)$, která je vytvořující funkcí posloupnosti $(a_0, a_1, a_2, \dots)$. Co se stane, když za x dosadíme x^n? Dostaneme

$$f(x^n) = a_0 + a_1 x^n + a_2 x^{2n} + \cdots .$$

Tedy $f(x^n)$ je vytvořující funkcí posloupnosti $(a_0, \underbrace{0, 0, \dots 0}_{n-1}, a_1, \underbrace{0, 0, \dots, 0}_{n-1}, a_2, \dots)$.

Dosazení tx za x (O6). Mějme funkci $f(x)$, která je vytvořující funkcí posloupnosti $(a_0, a_1, \dots)$ a t reálné. Potom $f(tx)$ je vytvořující funkce posloupnosti $(a_0, ta_1, t^2 a_2, \dots)$.

Násobení (O7). Pravděpodobně nejkomplikovanější operací, kterou zde zmíníme, je násobení funkcí. Mějme dvě funkce $f(x)$ a $g(x)$, které jsou po řadě vytvořujícími funkcemi posloupností $(a_0, a_1, \dots)$ a $(b_0, b_1, \dots)$. Naším cílem bude určit posloupnost, jejíž vytvořující funkce bude $f(x)g(x)$. Zapišme si tedy $f(x)$ a $g(x)$ jako mocninné řady, tj.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots , \quad g(x) = b_0 + b_1 x + b_2 x^2 \cdots .$$

Potom

$$\begin{aligned} f(x)g(x) = {} & a_0 b_0 + \\ & + (a_0 b_1 + a_1 b_0) x + \\ & + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \\ & \vdots \\ & + (a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0) x^n + \\ & \vdots \end{aligned}$$

Pokud ti to bude příjemnější, lze předchozí zápis zkrátit na

$$f(x)g(x) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) x^n.$$

Ukázali jsme si tedy, že $f(x)g(x)$ je vytvořující funkce posloupnosti $(a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \cdots)$.

Ještě dodejme terminologickou poznámku. Posloupnosti $(a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots)$ se obvykle říká *konvoluce* posloupností $(a_0, a_1, \dots)$ a $(b_0, b_1, \dots)$.

Příklad. Určete vytvořující funkci posloupnosti $(2, 3, 1, 2, 3, 1, 2, 3, 1, \dots)$. Určete, která posloupnost má vytvořující funkci $\frac{1}{(1-x)(1-2x)}$.

Příklad 1. Určete vytvořující funkce následujících posloupností:

(i) $(1, 0, 3, 0, 9, 0, 27, \dots)$,
(ii) $(2008, 134, 1, 1, 1, 1, 1, \dots)$,
(iii) $(1, -1, 1, -1, 1, -1, 1, -1, \dots)$,
(iv) $(1, 1, -2, 2, 4, 4, -8, 8, 16, 16, -32, 32, \dots)$,
(v) $(1, 4, 9, 16, 25, 36, 49, 64, \dots)$.

Příklad 2. K následujícím vytvořujícím funkcím nalezněte příslušné posloupnosti.

(i) $\frac{1}{1+2x}$,
(ii) $\frac{1}{1-x^2}$,
(iii) $\frac{1}{(1-x)^2}$,
(iv) $\frac{1}{(1-x)^3}$.

Hrátky s kostkami

V dalších úlohách se zaměříme na házení kostkami a pravděpodobnost, resp. počty možností, jak něco hodit.

Poznámka. Obyčejné hrací kostce můžeme přiřadit polynom $x + x^2 + x^3 + x^4 + x^5 + x^6$. Počet možností, jak hodit na dvou kostkách součet n, bude pak koeficient u n-té mocniny x, pokud polynomy obou kostek mezi sebou vynásobíme.

Příklad 3. Najděte dvě jiné než klasické šestistěnné kostky, pro které platí, že počet způsobů, jak může padnout libovolný součet ok, je stejný, jako kdyby se jednalo o klasické šestistěnné kostky (tj. kostky, které mají na stěnách 1, 2, 3, 4, 5 a 6 ok).

Příklad 4. Představte si, že můžete ovlivnit pravděpodobnost, s jakou padnou jednotlivé strany hrací kostky s $2k$ stranami (tj. takové, která má na stěnách $1, 2, \dots 2k$ ok). Můžete tyto pravděpodobnosti „našmelit“ tak, aby pravděpodobnost toho, že hodíme dvěma kostkami součet ok $2, 3, \dots, 4k$, byla stejná?

Za zmínku stojí zobecněná kombinační čísla a zobecněná binomická věta. Je-li r reálné a k přirozené, potom se zobecněné kombinační číslo definuje jako

$$\binom{r}{k} = \frac{r(r-1)(r-2)\cdots(r-k+1)}{k!}.$$

Zobecněná binomická věta říká, že pro r reálné je funkce $(1+x)^r$ vytvořující funkcí pro posloupnost

$$\left(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \dots\right),$$

tj.

$$(1+x)^r = \binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \cdots.$$

Tento vztah nám tedy umožňuje relativně jednoduše určit posloupnosti příslušející například vytvořujícím funkcím $\frac{1}{(1-x)^n} = (1-x)^{-n}$, nebo $\sqrt{1-x} = (1-x)^{\frac{1}{2}}$.

Příklad 5. Kolika způsoby může na šesti hracích kostkách padnout součet 13?

Literatura a zdroje

[1] 27. ročník MKS – seriál Kombinatorika

[2] Jiří Matoušek, Jaroslav Nešetřil: Kapitoly z diskrétní matematiky, Karolinum 2000

Obsah