Sborník
Rapotín 2007

Káťa Fišerová
Jarda Hančl
Víťa Kala
Saša Kazda
Franta Konopecký
Anša Lauschmannová
Rasťo Oľhava
Jakub „šnEk“ Opršal
Pavel Paták
Zuzka Pôbišová
Michal Rušin
Zuzka Safernová
Pavel Šalom
Martin Tancer

editor : Saša Kazda
vydání první, náklad 40 výtisků
duben 2007
Díky za pomoc všem, kterým je za co děkovat.

Něco málo z kvantové mechaniky

Káťa Fišerová

V úvodu přednášky si připomeneme historické pozadí vzniku kvantové teorie. Které experimentálně zjištěné skutečnosti nebylo možné na konci 19. a na začátku 20. st. vysvětlit pomocí znalostí klasické fyziky? Co s ní bylo dokonce v přímém rozporu? Kteří pánové přispěli při budování nové teorie svou troškou do mlýna a jak? Pak si povíme, co to je **operátor**[1]. Co to znamená, když dva operátory komutují a když naopak nekomutují. (*Dvě fyzikální veličiny je možné současně přesně změřit právě tehdy, když spolu operátory těchto veličin komutují*[2].) Jak se v měření projevují charakteristické rozměry přístrojů a zkoumaných částic? Jaké přesnosti lze dosáhnout? Jaká je v případě nesouměřitelných veličin (tzn. není možné je obě zároveň přesně změřit) nejmenší možná chyba? Zjednodušeně si odvodíme tzv. **relaci neurčitosti**[3].

Nelekejte se, že v tomto sborníčkovém textu narážíte na mnoho zcela neznámých slov či značek. Většinou neznamenají nic extrémně složitého. Podle složení účastníků přednášky se budu více či méně snažit vyvarovat se používání nástrojů integrálního a diferenciálního počtu. Spousta věcí se dá říct bez toho nebo prostě fikaně obejít ...

Následující **přehled základních postulátů QM** uvádím v kompromisní formě tak, aby vás moc nevyděsil a aby tam zároveň byla ta nejpodstatnější fakta (kromě Schrödingerovy rovnice) řečena. Nebojte se, všechno si vysvětlíme a něco třeba přeskočíme. V krajním případě, pokud budete chtít, mohou informace zde sepsané zůstat pěkně zavřené ve sborníčku a můžeme si spíš tak povídat a složité matematice se úplně vyhnout.

Postulát o vlnové funkci

Veškeré informace o stavu částice jsou popsány vlnovou funkcí, což je komplexní funkce reálných proměnných x, y, z a t (prostorové souřadnice a čas). Kvadrát absolutní hodnoty vlnové funkce udává hustotu pravděpodobnosti výskytu částice v místě r a čase t. Díky této interpretaci musí být vlnová funkce normovaná a kvadraticky integrabilní, navíc také spojitá a při konečných změnách potenciálu spojitě derivovatelná.

---

[1] Operátor je jakousi analogií k funkci. Do funkce „hodíte“ nějaké číslo a „vypadne“ zas nějaké číslo. Do operátoru (značí se obvykle velkým tiskacím písmenem se stříškou) „hodíte“ nějakou funkci a „vypadne“ zas nějaká funkce. Říkáme například, že operátor $\hat{A}$ působí na funkci f, zapisujeme $\hat{A}f$.

[2] Dva operátory komutují, pokud $\hat{A}\hat{B}f = \hat{B}\hat{A}f$, zkráceně často jen $\hat{A}\hat{B} = \hat{B}\hat{A}$, tj. $\hat{A}\hat{B} - \hat{B}\hat{A} = 0$. Tento rozdíl označujeme jako **komutátor** operátorů $\hat{A}$ a $\hat{B}$, zapisujeme $[\hat{A}, \hat{B}]$.

[3] $\delta F \cdot \delta G \geq \frac{1}{2} |\langle \hat{K} \rangle|$, kde $i\hat{K} = [\Delta\hat{F}, \Delta\hat{G}]$ je tzv. **komutátor**.

Postulát o operátorech
Každé fyzikální veličině, kterou můžeme pro danou částici naměřit, je přiřazen operátor, který působí na vlnovou funkci. Tyto operátory jsou lineární a hermitovské[4]. Lineárnost souvisí s principem superpozice. Hermitovské operátory se vyznačují tím, že mají reálná vlastní čísla, což je významné z hlediska měření fyzikálních veličin.

Postulát o kvantování
Jediné hodnoty, které může měřená fyzikální veličina A při jednotlivých měření nabývat, jsou vlastní čísla A_n odpovídajícího operátoru $\hat{A}$. Je-li systém popsán v okamžiku měření normovanou vlnovou funkcí ψ , pak je výsledkem měření střední hodnota veličiny A daná vztahem $\bar{A} = \langle\psi|\bar{A}\psi\rangle$.

Postulát o redukci vlnové funkce
Měření fyzikální veličiny A s výsledkem měření A_n, kde A_n je vlastní číslo odpovídající operátoru $\hat{A}$, převádí měřený systém do stavu s vlnovou funkcí ψ_n, která je vlastní funkcí operátoru $\hat{A}$ s vlastním číslem A_n[5]. Při měření tedy nedochází ke změně vlnové funkce pouze tehdy, je-li systém v některém z vlastních stavů operátoru $\hat{A}$.

Úlohy k zamyšlení

Příklad. Nechť φ a ψ jsou normované vlnové funkce. Jaké vlastnosti musí splňovat koeficienty $c_1, c_2 \in \mathbb{C}$, aby $c_1\varphi + c_2\psi$ byla normovaná vlnová funkce?

Příklad. V jedné dimenzi mějme operátor souřadnice $\hat{x} = x$ a operátor hybnosti $\hat{p} = -ih\frac{d}{dx}$. Spočtěte komutátor $[\hat{x}, \hat{p}]$. Co z něj vyplývá pro souměřitelnost polohy a hybnosti částice? (Pozn.: Na tu konstantu ih můžete na chvíli zapomenout, na nulovost či nenulovost komutátoru nebude mít vliv, stačí spočítat $[\hat{x}, \frac{x}{dx}]$.)

Příklad. Které z následujících operátorů jsou lineární?

(a) $\hat{A}f = af$, $a \in \mathbb{C}$

(b) $\hat{B}f = f^2$

(c) $\hat{C}f = f^*$ (komplexní sdružení)

Příklad. Předpokládejme, že máme dva systémy, které se nacházejí ve stavu popsaném stejnou vlnovou funkcí. Na každém systému jednou změříme veličinu A a získáme různé hodnoty. Je to možné? Co můžeme říci o stavu obou systému před a po měření?

[4]Operátor $\hat{L}$ je lineární, jestliže pro něj platí: $\forall a \in \mathbb{C} : \ \hat{L}(af) = a\hat{L}(f)$ a $\hat{L}(f_1 + f_2) = \hat{L}(f_1) + \hat{L}(f_2)$. Hermitovskost operátoru souvisí s jeho chováním ve skalárním součinu, který je v QM definován pomocí integrálu. Víc si zatím raději netroufám odtajnit :-)

[5]Vlastní čísla A_n a vlastní funkce ψ_n operátoru $\hat{A}$ jsou dány netriviálním řešením *vlastního problému* $\hat{A}\psi_n = A_n\psi_n$.

Soustavy rovnic

Jarda Hančl

Úvod

Ideou této přednášky je seznámit podrobněji posluchače s problematikou řešení složitějších (nestředoškolských) soustav rovnic. Úlohy jsou podobné těm, které se vyskytují v MO, a proto se přednáška bude hodit především těm, kteří umí řešit rovnice jen standardními způsoby.

Pomineme-li základní metody řešení soustav rovnic, jejichž jedinou myšlenkou je dosadit do nějakého vzorce, či upravovat hnusnou matici až do svítání, zbude pár metod, které všechny vyžadují myšlenku.

Za prvé se nabízí metoda substituce. Tu však budeme používat jen okrajově a vrhneme se přímo na zajímavější metody, kterýmižto jsou následující:

Symetrické mnohočleny

Tato metoda se používá pouze v případě, je-li rovnice symetrická vzhledem ke všem proměnným. Jinak řečeno, zaměníme-li proměnné dostaneme stejnou rovnici. Poté používáme substituci $s_1 = x_1 + x_2$, $s_2 = x_1 x_2$ (tvar substituce závisí na počtu neznámých).

Příklad 1. Řešte v reálných číslech:

$$\frac{x_1}{x_2} + \frac{x_2}{x_1} = \frac{13}{6}$$

$$x_1 + x_2 = 5$$

Iracionální rovnice

Zde ukáži jen jednu metodu, která se může hodit, pokud člověk nechce strávit s jednou rovnicí mládí. Metodu budu demonstrovat na příkladu.

Příklad 2.

$$\sqrt{2x^2 + 5x - 9} - \sqrt{2x^2 + 5x - 2} = 1$$

Odhady nerovnostmi

Tato metoda je hodně intuitivní. Využívá se většinou v soustavách, které nám tak trochu připomínají nějakou známou nerovnost. Neexistuje tedy pravidlo, musí nám vystačit první pohled.

Příklad 3. V reálných číslech vyřešte:

$$x_1 + x_2 + \cdots + x_n = \frac{1}{4}$$

$$\frac{1}{x_1} + \frac{4}{x_2} + \cdots + \frac{n^2}{x_n} = n^2(n+1)^2$$

Určení minim a maxim funkcí, hledání hodnot výrazů

Následující téma není přímo o řešení soustav, ale metody, které se při nich používají, se často mohou při řešení soustav rovnic hodit.

Příklad 4. Určete maximum výrazu:

$$(1 + \sin x)(1 + \cos x)$$

Příklad 5. Pro $x + y + z = 8$ určete minimum výrazu

$$\sqrt{1 + x^2} + \sqrt{4 + y^2} + \sqrt{9 + z^2}$$

Příklad 6. Určete všechny hodnoty výrazu

$$\frac{x + y}{x^2 + y^2}$$

pro x, y reálné splňující $1 \leq x + y$.

Invarianty v rovnicích

Jednoduše řečeno, invariant je něco, co se za určitých podmínek nemění. V rovnicích budeme chápat invariant jako vlastnost výrazu. Tato vlastnost je specifická tím, že za určitých změn podmínek v zadání je hodnota výrazu stále stejná. Pro srozumitelnost zase uvedu na příkladu.

Příklad 7.

$$x = \frac{1}{y} + \frac{1}{z}$$

$$y = \frac{1}{z} + \frac{1}{x}$$
$$z = \frac{1}{x} + \frac{1}{y}$$

Příklady

V reálných číslech řešte následující soustavy:

Příklad 8.

$$\sin x = \cos y$$
$$\sin y = \cos z$$
$$\sin z = \cos x$$

Příklad 9.

$$x^2 = y + z + 2$$
$$y^2 = z + x + 2$$
$$z^2 = x + y + 2$$

Příklad 10.

$$\frac{1}{x} + \frac{4}{y} + \frac{9}{z} = 3$$
$$x + y + z \leq 12$$

Příklad 11.

$$(1+x)(1+x^2)(1+x^4) = 1 + y^7$$
$$(1+y)(1+y^2)(1+y^4) = 1 + x^7$$

Příklad 12. Určete p, pro které má následující soustava právě 1 řešení.

$$(x-y)^2 = p^2$$
$$x^3 - y^3 = 16$$

Příklad 13. Pro $xyz = 1$ určete hodnoty výrazu

$$V = \frac{1}{1+x+xy} + \frac{1}{1+y+yz} + \frac{1}{1+z+zx}$$

Nestandardní metody

Víťa Kala

V 60. letech minulého století jistý pan Robinson vymyslel, že celý matematický svět je možné rozšířit o spoustu dalších, takzvaných nestandardních prvků. S těmito nestandardními prvky pak do matematiky přijdou i nejrůznější nesmírně divné principy, které najednou začnou platit. My si na přednášce některé z nich uvedeme a seznámíme se s tím, jak se dá těchto podivností využít k řešení praktických příkladů.[6]

Jak je vlastně toto rozšíření možné? Vždyť přece NIC nemůže být větší, než CELÝ matematický svět? To je sice pravda, ale ono se to dá obejít takovouto fintou:[7] celý matematický svět (někdy se mu říká taky univerzum) je tak velký, že je možné jej zkopírovat do sebe sama (existuje jeho část, která je úplně stejná, jako celek). Tuto část budeme od teď považovat za naše standardní univerzum. Najednou máme ale kolem tohoto standardního matematického světa ještě spousta místa, kam ho můžeme rozšiřovat! Vhodnou část tedy zvolíme za náš rozšířený svět (ten se nazývá internální univerzum). A hle: hnedle máme rozšíření standardního světa (který je úplně stejný, jako původní svět) do internálního univerza. No a celému původnímu světu se občas taky říká externální univerzum.

Tento postup se dá provést za předpokladu, že platí následující axiom, který za pravdivý sice většina matematiků nepovažuje, je ale dokázané, že jeho přidáním k ostatním matematickým axiomům nic nezkazíme. Jakmile jej přijmeme, můžeme už z něj dokázat všechna další tvrzení, která v našem nestandardním světě platí.

Axiom. (Superuniverzality[8]) *Existuje libovolně šílená množina.*[9]

Co že to znamená ta libovolně šílená množina? No přece přesně to, že může být libovolně šílená (: Třeba existuje množina x, jejímž jediným prvkem je ona sama (tedy $x = \{x\}$). Anebo existují dvě množiny x, y takové, že $x \in y$ a $y \in x$. Anebo cokoli dalšího, na co si jen vzpomeneš ...

[6] K tomu, aby tato teorie mohla být vykládaná precizně, je potřeba znát velké množství vysokoškolské matematiky. Smiř se proto s tím, že skoro žádné tvrzení neplatí přesně tak, jak je zde ve sborníčku napsané nebo jak si je uvedeme na přednášce. Na této přednášce se tedy budeme bavit o tvrzeních, která neplatí v teorii, jež je sama o sobě v zásadě šílená a nesmyslná (:

[7] Nic si z toho nedělej, pokud zbytku tohoto odstavce neporozumíš. Pro pochopení zbytku přednášky to není vůbec potřeba.

[8] Většina tvrzení, se kterými se potkáme, bude mít podobně vtipné názvy (:

[9] Pozorná čtenářka si možná všimla, že tato formulace není zcela matematicky korektní. Pro zájemce ale můžu uvést i exaktní formulaci tohoto axiomu, z které možná bude patrná výhoda neformálního přístupu: Buďte $t \subseteq a$ množiny takové, že t je tranzitivní. Buď r extenzionální relace na a taková, že (a, r) je koncové rozšíření $(t, \in)$. Pak existuje tranzitivní množina t' a izomorfismus $f : (t', \in) \simeq (a, r)$ takový, že $f \restriction t = id$.

Princip saturovanosti

Princip. *Ať jsou $M_1, M_2, \ldots$ množiny*[10] *takové, že když si vyberu konečně z nich, mají neprázdný průnik (takovému systému množin se říká centrovaný). Pak všechny množiny mají neprázdný průnik.*

Tento princip je zcela zásadní a má nedozírné důsledky. Představme si třeba množinu $\mathbb{N}$ všech přirozených čísel a označme $A_i = \mathbb{N} - \{i\}, i = 1, 2, 3, \ldots$ (množinu, kterou dostaneme, když z $\mathbb{N}$ vyhodíme číslo i). Průnik konečně mnoha z těchto množin je jistě neprázdný (obsahuje nekonečně mnoho nevyhozených přirozených čísel), a tedy podle principu saturovanosti musí mít všechny množiny neprázdný průnik. Musí tedy existovat přirozené číslo n, které není rovné žádnému z čísel 1, 2, 3, ... ! S takovým číslem se člověk na ulici jen tak nepotká.

Setkáváme se tedy se zvláštní situací – množina $\mathbb{N}$ standardních přirozených čísel se nám s přechodem do nového světa nafoukla a přibyla do ní nová nestandardní přirozená čísla. Tuto množinu všech (i nestandardních) přirozených čísel budeme značit N. Jak už to tak v matematice bývá, za konečné se považují ty množiny, jejichž počet prvků je rovný nějakému přirozenému číslu. S novými přirozenými čísly se nám tedy najednou objevily i nové konečné množiny (které jsou větší, než libovolná standardní konečná množina).

Stejně tak, jako jsme dokázali, že množina přirozených čísel je větší, než jsme si mysleli, bychom mohli podobné tvrzení dokázat třeba o racionálních nebo reálných číslech. V tomto případě bychom zjistili, že musí existovat nekonečně malá reálná čísla, což má také spoustu zajímavých důsledků (najednou totiž třeba půjde v jistém smyslu mluvit o „sousedních“ reálných číslech, což mnohé úvahy značně zjednoduší, ale ve standardní matematice bohužel nejde).

Princip přenosu

Princip. *Nějaké tvrzení (o standardních množinách) platí ve standardním matematickém světě právě tehdy, když platí v našem rozšíření.*

Tím, že jsme přešli do našeho většího světa, jsme tedy opravdu nic neztratili – platí tu přesně totéž, co v běžném nudném světě většiny matematiků.

[10] Tady si přece jen neodpustím jednu upřesňující poznámku pro znalé. Toto tvrzení platí jen pokud množin není příliš mnoho – je-li jich méně než nějaký libovolně velký, ale předem zvolený kardinál κ.

Princip finitarizace

Princip. *Každá množina*[11] *je podmnožinou nějaké konečné množiny.*

Tak teď už se ale ten Víťa musel úplně zbláznit, ne? Jak by mohla být nějaká *nekonečná* množina částí nějaké *konečné*?! Světe div se, ono to opravdu jde ... Aby si člověk mohl aspoň trochu představit, jak je to možné, je dobré si uvědomit, že v rozšířeném světě je konečných množin mnohem víc, než kolik jich bylo v tom původním standardním. Takže není divu, že je víc i těch množin, které jsou částí nějaké konečné množiny.

Tento tvrzení je jedním z nejzajímavějších důsledků nestandardního rozšíření. Umožňuje totiž snadno a bezbolestně rozšířit platnost některých tvrzení, která platí pro konečné množiny, i na množiny, které jsou nekonečné. Jedním takovým příkladem, který vyřešíme na přednášce, je tento:

Příklad. Buď G (nekonečný) graf takový, že každá konečná množina vrcholů jde obarvit k barvami tak, že žádné dva vrcholy spojené hranou nemají stejnou barvu. Dokaž, že potom jde takto obarvit celý graf.

[11] Toto platí opět jen pro množiny (externálně) menší než náš známý kardinál κ.

Neměnky

Víťa Kala

Použití neměnků (neboli invariantů) je nesmírně užitným postupem pro řešení rozličných často velmi obtížných příkladů. V zásadě jde o to, že pokud se v zadání něco **mění**, je dobré zkusit najít něco, co se naopak **nemění** nikdy, tedy nějaký **neměnek**. Zadání příkladů, v kterých se hodí nějaký hledat, tedy často obsahují výrazy jako „Je možné po několika krocích dostat . . . “

Vhodným neměnkem může být třeba součet nebo rozdíl nějakých čísel, jeho parita (jestli je sudý nebo lichý), zbytek po dělení 3 nebo jiným číslem, vzdálenost od nějakého bodu, . . .

V souvislosti s neměnky v podstatě nejde rozvíjet žádná velká teorie; jediný způsob, jak se je naučit používat, je počítat příklady, v kterých se vyskytnou. Tak hurá do toho! (:

Příklad 1. Nechť je n liché přirozené číslo. Na tabuli jsou napsaná čísla $1, 2, \ldots$ $\ldots, 2n$. V každém kroku si vybereme dvě čísla a, b, která smažeme a nahradíme absolutní hodnotou jejich rozdílu. Dokažte, že na konec zůstane na tabuli liché číslo.

Příklad 2. Na obvodu kruhu je napsáno 6 čísel, po řadě 1, 0, 1, 0, 0, 0. V každém kroku můžeme zvýšit libovolná dvě sousední čísla o 1. Je možné po několika krocích dostat všechna čísla stejná?

Příklad 3. Každý poslanec tramtárijského parlamentu má nejvýše 3 nepřátele. Dokažte, že je možné parlament rozdělit na dvě komory (ne nutně stejně velké) tak, že každý poslanec má nejvýše 1 nepřítele ve své komoře.

Příklad 4. Předpokládejme, že celá čísla a, b, c, d nejsou všechna stejná. Začněme se čtveřicí (a, b, c, d) a nahraďme ji $(a-b, b-c, c-d, d-a)$. Dokažte, že opakováním tohoto postupu se aspoň jedno číslo stane libovolně velkým.

Příklad 5. Začněme se celými čísly $1, 2, 3, \ldots, 4n-1$. V každém kroku nahradíme libovolná dvě čísla jejich rozdílem. Dokažte, že poslední číslo bude sudé.

Příklad 6. Začněme s množinou (3, 4, 12). V každém kroku vybereme dvě z čísel a, b a nahradíme je čísly $0{,}6a - 0{,}8b$ a $0{,}8a + 0{,}6b$. Je možné dosáhnout stavu (4, 6, 12)?

Příklad 7. Mějme normálně obarvenou šachovnici 8×8. V každém kroku můžeme přebarvit všechna pole nějakého řádku či sloupce nebo čtverce 2×2. Je možné dostat šachovnici s jen jedním černým políčkem?

Příklad 8. Na stole je a červených, b bílých a c černých piškotů. V jednom kroku můžeme sníst dva piškoty různých barev a nahradit je dvěma piškoty třetí barvy.

Na začátku bylo $a = 13, b = 15, c = 17$. Je možné po několika krocích dosáhnout stavu, v němž mají všechny piškoty stejnou barvu? Jak je tomu v obecném případě?

Příklad 9. Na kružnici je napsáno 5 jedniček a 4 nuly v libovolném pořadí. Potom mezi dvě sousední stejná čísla napíšeme 0 a mezi dvě různá 1. Nakonec původní čísla vymažeme. Je takto možné po několika krocích dostat samé nuly?

Příklad 10. Každé z čísel 1 až 1 000 000 je opakovaně nahrazované svým ciferným součtem, dokud nedostaneme milión jednociferných čísel. Bude mezi nimi víc jedniček nebo dvojek?

Příklad 11. Obsahuje posloupnost čtverců přirozených čísel nekonečnou aritmetickou podposloupnost?

Příklad 12. Nechť $d(n)$ značí ciferný součet čísla n. Řešte rovnici $n + d(n) + d(d(n)) = 2005$.

Příklad 13. Mějme čísla $a, b, 0 < b < a$. Nechť $x_0 = a, y_0 = b, x_{n+1} = (x_n + y_n)/2, y_{n+1} = 2x_n y_n/(x_n + y_n)$. Jak se chovají posloupnosti x_n, y_n?

Příklad 14. Škrtneme první cifru čísla 7^{2004} a potom ji přičteme ke zbývajícímu číslu. Tento postup opakujeme tak dlouho, dokud nedostaneme deseticiferné číslo. Je možné, aby obsahovalo všechny číslice $0, 1, \ldots, 9$?

Příklad 15. Na každém políčku obdélníkové šachovnice je napsané přirozené číslo. V každém tahu můžeme zdvojnásobit každé číslo v nějakém řádku nebo odečíst 1 od každého z čísel v nějakém sloupci. Je možné dostat po několika tazích tabulku obsahující samé nuly?

Příklad 16. Vrcholy n-úhelníka jsou očíslované reálnými čísly. Buďte a, b, c, d čtyři sousední čísla. Je-li $(a - d)(b - c) < 0$, můžeme vyměnit b a c. Může být tato operace prováděna nekonečně dlouho?

Příklad 17. Čísla $1, 2, \ldots, 2n$ jsou libovolně uspořádaná na pozicích očíslovaných $1, 2, \ldots, 2n$. Přičtěme ke každému z čísel číslo jeho pozice. Dokažte, že dva ze součtů dávají stejný zbytek po dělení n.

Příklad 18. Řešte rovnici $(x^2 - 3x + 3)^2 - 3(x^2 - 3x + 3) + 3 = x$.

Příklad 19. Množinu S bodů v prostoru můžeme rozšířit o obraz libovolného bodu $X \in S$ ve středové souměrnosti se středem v $A \in S$, $A \neq X$. Na začátku S obsahuje 7 vrcholů krychle. Může se časem stát i 8. vrchol prvkem S?

Příklad 20. Na tabuli jsou na začátku čísla 18 a 19. V jednom kroku můžeme napsat na tabuli číslo rovné součtu dvou libovolných čísel, jež byla předtím na tabuli. Může být někdy na tabuli napsané číslo 1994?

Příklad 21. Každý člen posloupnosti 1, 0, 1, 0, 1, 0, ... počínaje sedmým je součtem předchozích šesti mod 10. Dokažte, že se v posloupnosti nikdy nevyskytne šestice ... , 0, 1, 0, 1, 0, 1, ...

Příklad 22. Řešte rovnici $f(f(x)) = x$, kde $f(x)$ je libovolný kvadratický mnohočlen.

Příklad 23. Dvě políčka na obrázku jsou sousední, jestliže mají společnou hranu. V jednom kroku můžeme k libovolným dvěma sousedním políčkům přičíst stejné celé číslo. Je možné první tabulku převést několika tahy na druhou?

1	2	3
4	5	6
7	8	9

7	8	9
6	2	4
3	5	1

Příklad 24. $2n$ velvyslanců je pozvaných na kongres. Každý z nich má nejvýše $n - 1$ nepřátel. Dokažte, že je můžeme usadit kolem kulatého stolu tak, že nikdo nesedí vedle svého nepřítele.

Příklad 25. Na každém políčku šachovnice 8×8 je napsané přirozené číslo. V jednom tahu si vybereme tabulku 4×4 nebo 3×3 a přičteme 1 ke každému z jejích políček. Můžeme vždy dostat tabulku se všemi čísly dělitelnými (a) dvěma, (b) třemi?

Úvod do TEXu

Saša Kazda

Co je TEX

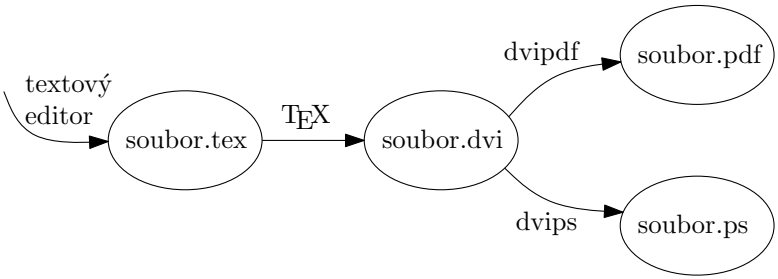
TEX (vyslovuje se tech) je typografický systém: způsob, jak vytvářet hezky vytištěné dokumenty (především matematické, ale klidně i poezii).

Je to zároveň programovací jazyk i program, který vezme soubor v tomto jazyce a vytvoří z něj grafický dokument. Neexistuje žádná „TEX Office“, ve které jediné by bylo možné psát soubory; zdrojový kód můžete psát v libovolném textovém editoru (i když existují editory pro psaní TEXových zdrojáků určené). Dokonce existuje i více programů, které všechny splňují náležitosti, aby je bylo možno nazvat TEXem.

TEX a synové

Krom „čistokrevného“ TEXu existují různé odvozeniny a rozšíření, nejpopulárnější (populárnější než původní TEX) je LATEX. Dále vzniklo mnoho programů, které umí s TEXem či LATEXem spolupracovat (například grafický editor Ipe), nemluvě o tom, že se jazyk sám často používá pro popis matematiky na počítači (v mailech mezi matematiky, na Wikipedii, ...).

Krom znalosti jazyka je dobré mít základní povědomí o dobrých a špatných typografických nápadech. TEX je sice hodně dobrý (umí rozdělovat slova, snaží se zabránit výskytu osamělých řádků a jiných neplech), ale není to typografický expertní systém – nesnaží se zvolit sazbu podle nějakých estetických měřítek, jenom za sebe chytře skládá znaky. I netypograf s TEXem ale obvykle vyrobí hezčí dokument než pomocí Office (ať už Open nebo Microsoft).



TEXnické podrobnosti

Jak si TEX nainstalovat
Pod Windows: Distribuce MiKTEXnebo TEX Live a spousta trpělivosti. Další možné distribuce (nezkoušel jsem) jsou XEmTEXa proTEXt.
Pod Linuxem: teTEX, TEX Live
Na editovaní: Specializované editory jako WinEdt, TEXnic Center, Lyx nebo kvalitní univerzální editory vim a Emacs, v nouzi nejvyšší notepad nebo Office (uložit jako čistý text).

Pracovní cyklus
DVI soubory jsou dobré pro náhledy, při posílání hotových dokumentů dál se (z dobrých důvodů) používá PostScript nebo PDF formát.

Příkazy a ukázky

Nejprve uvedeme pár pozorování:

(i) V TEXu není (na rozdíl od LATEXu) potřeba na začátku psát nějakou speciální hlavičku dokumentu. Dokument končíme pomocí `\bye` nebo `\end`.
(ii) Násobné mezery a konce řádků TEX obvykle převádí na jednu mezeru, odstavce se oddělují prázdnou řádkou.
(iii) Matematika se píše mezi dolarové značky $. Pokud má být na samostatný řádek, píšeme ji mezi $$.
(iv) Značky `{ a }` umožňují vytvářet skupiny.
(v) Mezeru je možné si vynutit příkazem `\space`, nový odstavec příkazem `\par`, vertikální mezeru příkazem `\smallskip`,`\medskip`,`\bigskip` nebo `\vskip` a délkovým údajem (třeba `\vskip 15 cm`).
(vi) Za většinou maker zmizí mezery. Například `\TeX u` dá TEXu. Pokud chceme TEX u, píšeme třeba `\TeX{} u`.

Následující tabulka obsahuje výběr nejčastěji používaných příkazů ze základního českého TEXu (styl csplain). Existují různé modifikace stylů (například se často používá `\frac{a}{b}` místo `{a \over b}`). Rozšiřující balíčky maker nahrajete pomocí `\input [jméno]`. Například `\input amssym` nahraje dodatečná makra pro matematické symboly.

`\bf tučné`	**tučné**
`\it kurzíva`	*kurzíva*
`\uv{uvozovky}`	„uvozovky“
`~z`	před „z“ nebude ukončen řádek
`${a\over b}$`	$\frac{a}{b}$
`$(a+b)\cdot c=a\cdot c+b\cdot c$`	$(a+b)\cdot c=a\cdot c+b\cdot c$

`$a_1^2+a_2^2+\dots+a_{k+l}^2$`	$a_1^2 + a_2^2 + \dots + a_{k+l}^2$
`$\sin(x)$`	$\sin(x)$ (porovnej se $sin(x)$)
`$\sqrt{x}$`	$\sqrt{x}$
`$\alpha, \beta, \gamma$`	α, β, γ
`$\|\sphericalangle ABC\|$`	$\|\sphericalangle ABC\|$
`$\sum_{i=1}^n {n\choose i}$`	$\sum_{i=1}^{n} \binom{n}{i}$

Literatura

Pokud si nemůžete vzpomenout na nějaký příkaz, doporučuji si na internetu najít referenční karty: TEX Reference Card, $\mathcal{AMS}$-TEX Reference Card a podobně. Google je váš přítel.

Učebnice (v pořadí od nejjednodušších po nejdrsnější):

(1) O LaTeXu pro nedočkavé
`http://www.latex-project.org/ftp.html`
(2) Kamil Toman: TEXtutor, První krůčky v (plain) TEXu
`http://artax.karlin.mff.cuni.cz/~toman/TeXtutor.ps`
(3) Michael Doob: Jemný úvod do TEXu (překlad Josef Daneš a Jiří Veselý)
`http://ftp.cstug.cz/pub/tex/local/cstex/doc/jemny.tar.gz`
(4) Donald E. Knuth: The TEXbook
(5) Petr Olšák: TEXbook naruby
`http://math.feld.cvut.cz/olsak/tbn.html`

Polynomy

Saša Kazda

Polynomy (mnohočleny) můžeme uvažovat nad různými množinami: $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n$ a dalšími. Pokaždé se chovají trochu jinak, ale některé vlastnosti mají společné. V tomto povídání se budeme zabývat především polynomy nad $\mathbb{Q}, \mathbb{R}$ a $\mathbb{C}$.

Definice. *Buď R množina s definovanými operacemi sčítání a násobení*[12]. *Potom* polynom stupně n nad R *je výraz* $r_n x^n + r_{n-1}x^{n-1} + \cdots + r_0$, *kde* $r_n \neq 0$ *a* $r_0, \ldots, r_n \in R$.

K polynomům přidáme ještě nulový polynom, jehož stupeň se obvykle klade roven divným číslům jako -1 nebo $-\infty$. Násobení a sčítání polynomů definujeme „člen po členu“.

Všimni si, že polynom je zároveň něco algebraického ($(n+1)$-tice koeficientů $r_0, r_1, \ldots, r_n$) a zároveň funkce. Tento rozdíl se stírá v případě polynomů nad reálnými čísly, kde každá polynomiální funkce odpovídá právě jedné sadě koeficientů. Ovšem třeba nad $\mathbb{Z}_2$ máme nenulové polynomy odpovídající nulovým funkcím, například $x^2 + x$.

Problém. Buď p polynom nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$. Je možné, aby $\forall x, p(x) = 0$, ale p nebyl nulový?

Definice. *Řekneme, že polynom p je* dělitelem *polynomu q, píšeme $p|q$, pokud existuje polynom r takový, že $p \cdot r = q$.*

Ze školy možná znáte algoritmus pro dělení polynomů. S trochou šikovnosti z něj lze odvodit, že pokud r je polynom nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$, který není dělitelný žádným polynomem stupně vyššího než 0, a $r|pq$, tak buď $r|p$, nebo $r|q$. Tedy takzvané ireducibilní polynomy se chovají podobně jako prvočísla. Po další úvaze zjistíme, že polynomy nad $\mathbb{Q}, \mathbb{Z}, \mathbb{R}$ můžeme „rozložit na prvočinitele“ jednoznačně (až na pořadí a násobení konstantou).

Opět nic takového nemusí platit nad jinými množinami čísel: Nad $\mathbb{Z}_4$ je $x+2|x^2$, ale $\neg(x+2|x)$.

Definice. *Kořen polynomu p nad R je takové číslo $\alpha \in R$, že $p(\alpha) = 0$.*

Pozorování. Pokud má polynom $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_i \in \mathbb{Z}$, racionální kořen $q = \frac{r}{s}$ (r, s nesoudělná), tak platí $r|a_0$ a $s|a_n$.

Tvrzení. Pokud α je kořen polynomu p, tak $(x - \alpha)|p$.

[12] Úplně přesně bychom řekli, že R má být komutativní okruh, tedy chceme, aby ono sčítání a násobení byly komutativní a asociativní operace, abychom měli jednotku a nulu a platil distributivní zákon $a(b+c) = ab + ac$.

Důsledek. Pokud p je polynom nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$ stupně nejvýš n, který má $n+1$ kořenů, tak p je nulový polynom.

Důsledek. Polynom stupně nejvýš n nad $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$ je jednoznačně určený hodnotami v $n+1$ bodech.

Příklad. Dokažte, že pokud P je polynom s celočíselnými koeficienty a a, b, c různá celá čísla, tak se nemůže stát, aby $P(a) = b, P(b) = c, P(c) = a$.

Příklad. Dokažte, že pro všechna po dvou různá čísla $a, b, c \in \mathbb{R}$ platí:

$$\frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-a)(x-c)}{(b-a)(b-c)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} = 1$$

Věta. (Základní věta algebry) *Každý polynom řádu aspoň 1 s komplexními koeficienty má v $\mathbb{C}$ aspoň jeden kořen.*

Důsledek. Každý polynom nad $\mathbb{C}$ lze psát ve tvaru $c \prod_{i=1}^{n} (x - \alpha_i)$, kde α_i jsou komplexní čísla (kořeny) a c je nenulové komplexní číslo.

Tvrzení. (Viètovy vztahy) Buďte $\alpha_1, \alpha_2, \ldots, \alpha_n$ kořeny polynomu $p(x) = x^n + + c_{n-1}x^{n-1} \cdots + c_0$ nad $\mathbb{C}$. Potom platí:

$$\begin{aligned} c_{n-1} &= -\sum_{i=1}^{n} \alpha_i \\ c_{n-2} &= \sum_{\substack{i,j=1 \\ i<j}}^{n} \alpha_i \alpha_j \\ &\vdots \\ c_0 &= (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n \end{aligned}$$

Příklad. Buďte a, b, c reálná čísla taková, že

$$\begin{aligned} a + b + c &> 0 \\ ab + ac + bc &> 0 \\ abc &> 0. \end{aligned}$$

Dokažte, že pak $a > 0, b > 0, c > 0$.

Příklad. Mějme P, Q reálné polynomy, $P \neq 0$. Dokažte, že existuje polynom R s reálnými koeficienty takový, že $P(x) | R(Q(x))$.

Příklad. $P(x)$ buď polynom stupně nejvýš 6 nad $\mathbb{Z}$ takový, že $7 | P(x)$ pro každé $x \in \mathbb{Z}$. Ukažte, že potom 7 dělí všechny koeficienty $P(x)$.

Funkcionální rovnice

Franta Konopecký

Úvod

Na této přednášce si osvojíte práci s funkcionálními rovnicemi, jejich řešeními a možnostmi postupu. Systematicky jsou tu probrány jednotlivé zajímavé vlastnosti funkcí a jak se dají z funkcionální rovnice vyčíst. Příspěvek ve sborníčku by měl sloužit jako ucelený manuál, jak funkcionální rovnice řešit.

Co je funkcionální rovnice, co vyjadřuje?
Zadání funkcionální rovnice může vypadat například následovně:

Úloha 1. Najděte všechny funkce $f : \mathbb{Q} \to \mathbb{Q}$ splňující $f(x+y) = f(x) + f(y)$ pro všechna $x, y \in \mathbb{Q}$.

Úloha 2. Hledejte všechny spojité funkce $f : \mathbb{R} \to \mathbb{R}$ vyhovující rovnici

$$f(x+y) = f(x) + f(y)$$

pro $x, y \in \mathbb{R}$.

Úloha 3. Najděte všechny funkce definované na celé reálné ose splňující funkcionální rovnici

$$f(x+y) + 2f(x-y) - 4f(x) + xf(y) = 3y^2 - x^2 - 2xy + xy^2;\ x, y \in \mathbb{R}.$$

Úloha 4. Najděte všechny funkce splňující rovnici

$$(f(x) + f(y))(f(u) + f(v)) = f(xu - yv) + f(xv + yu);\ x, y, u, v \in \mathbb{R}.$$

ad 1. Funkcionální rovnice (1) nám říká: „najděte všechny funkce, které splňují rovnici $f(x+y) = f(x) + f(y)$ pro všechny hodnoty racionálních čísel x a y“. Dodat bychom ještě měli: „ … a ověřte, že vámi nalezené funkce vyhovují.“ Pro představu prozradím, že například funkce $f(x) = 2x$ této rovnici vyhovuje, protože $f(x+y) = 2(x+y)$ a $f(x) + f(y) = 2x + 2y = 2(x+y)$, takže je rovnice $f(x+y) = f(x) + f(y)$ splněna pro všechna požadovaná $x, y \in \mathbb{Q}$. Funkce $f(x) = x+1$ naopak nevyhovuje, protože $f(x+y) = x + y + 1 \neq x + 1 + y + 1 = f(x) + f(y)$.

ad 2. Funkcionální rovnice (2) má stejný tvar, ale se dvěma změnami. První je, že je definovaná na celém $\mathbb{R}$ a funkční hodnoty mohou nabývat na rozdíl od těch v (1) také reálných hodnot. Druhou je, že máme dodanou pomocnou podmínku, že je funkce spojitá. Bez této podmínky lze rovnici v $\mathbb{R}$ také vyřešit, ale řešení

je ošklivější než nechutné. Důležité je si tu uvědomit, že řešení nalezená v (1) by mohla bez větších obtíží fungovat i v (2) (při správném rozšíření z $\mathbb{Q}$ na $\mathbb{R}$).

ad 3. Tato rovnice je příkladem těch, kde nám vedlejší výrazy „vylézají“ na povrch. Kromě funkčních výrazů typu $f(něco)$ se v ní totiž objevují i výrazy typu x^2, xy, atd. Rovnice tohoto typu jsou většinou jednodušší, protože řešení v hodně případech přímo „vypadne“ nějakým speciálním dosazením za x nebo y, viz tzv. *substituční* metoda řešení.

ad 4. Toto je jedna z nejtěžších funkcionálních rovnic, s jakou jsem se setkal. Je v ní důležité mít přehled o většině triků, které se v tomto příspěvku naučíte. Na přednášce si ji vyřešíme, těšte se!

Základní metody řešení

Základními metodami řešení funkcionálních rovnic jsou *substituční* metoda a *Cauchyho* metoda.

Substituční metoda

Substituční metoda spočívá, řečeno co nejobecněji, v následujícím postupu: Předpokládáme, že už máme řešení funkcionální rovnice a vhodným dosazením za proměnné se snažíme ukázat, co by mělo toho řešení splňovat. Někdy nám vyjde užitečná vlastnost funkce ($f(x)$ je sudá, prostá, ...), jindy přímo tvar, jak musí vypadat. Pokud dostaneme tvar funkce (nebo si ho odvodíme z nalezených vlastností), je nutné ho dosadit do zadání a zkouškou ověřit, že je skutečně řešením. Osvětlíme si to na úloze (3):

Úloha. Najděte všechny funkce definované na celé reálné ose splňující funkcionální rovnici

$$f(x+y)+2f(x-y)-4f(x)+xf(y)=3y^2-x^2-2xy+xy^2.$$

Řešení. Předpokládejme, že nějaká $f(x)$ je řešením a označme $f(0)=c$. Funkcionální rovnice je splněna pro všechny dvojice čísel x, y, je tedy splněna i pro dvojici čísel[13] $x=x$, $y=0$, dosazením za tuto dvojici dostaneme:

$$-f(x)+cx=-x^2$$

neboli

$$f(x)=x^2+cx.$$

Dosadíme-li v získaném vztahu $x=0$, dostaneme navíc $f(0)=0$, tedy $c=0$ a jediným tvarem, jaký může mít naše funkce $f(x)$, zůstal $f(x)=x^2$. Z předpokladu,

[13] dosazujeme speciální hodnoty za proměnné, abychom dostali nějakou vlastnost funkce, nebo konkrétní tvar

že funkce $f(x)$ řeší naši rovnici jsme odvodili, že nutně musí platit vztah $f(x) = x^2$. Teď už stačí jen získaný vztah dosadit do zadané rovnice a ověřit, že funkce $f(x) = x^2$ je řešením naší rovnice.

Vztah, který by určoval, jak musí nutně vypadat funkce splňující zadanou rovnici, nemusí jít z funkcionální rovnice přímo získat. Proto je tu *Cauchyova* metoda.

Cauchyho metoda

Cauchyho metoda se zakládá na postupném odvození chování funkce pro přirozená čísla, poté pro celá, posléze pro racionální a s trochou štěstí (pokud to zadání požaduje) nakonec pro všechna reálná čísla.

Cauchyho metodu ozřejmíme na úloze (2).

Úloha. Najděte všechny spojité funkce $f : \mathbb{R} \to \mathbb{R}$ vyhovující rovnici

$$f(x + y) = f(x) + f(y);\ x, y \in \mathbb{R}.$$

Řešení. Předpokládejme, že máme jedno takové řešení[14] $f(x)$. Dosazením $x = 0$ a $y = 0$ zjistíme, že nutně[15] platí $f(0) = 0$. Dosazením[16] $y = -x$ dostáváme $f(-x) = -f(x)$. Matematickou indukcí snadno[17] dokážeme vztah $f(x_1 + x_2 + \cdots + x_n) = f(x_1) + f(x_2) + \cdots + f(x_n)$, speciálně pak pro $x_1 = x_2 = \cdots = x_n = x$ vztah $f(nx) = nf(x)$ pro každé reálné číslo x a přirozené(!) číslo n. Označme si $f(1) = c$. Pak $f(n) = nf(1) = cn$ pro každé přirozené číslo n. Volbou $x = m/n$ ve vztahu $nf(x) = f(nx)$ dostáváme $nf(m/n) = f(n \cdot m/n) = f(m) = cm$, neboli $f(m/n) = c \cdot m/n$. Vztah $f(x) = cx$ tedy platí pro každé kladné(!) racionální číslo x. Díky vztahu $f(0) = 0$ a $f(-x) = -f(x)$ máme platnost vztahu $f(x) = cx$ pro každé(!) racionální číslo x. Protože je množina racionálních čísel $\mathbb{Q}$ *hustá*[18] v $\mathbb{R}$ a protože je funkce $f(x)$ spojitá, musí $f(x)$ splňovat vzorec $f(x) = cx$ na všech reálných číslech.

Zkouškou[19] provedenou dosazením do rovnice v zadání úlohy snadno ověříme, že funkce $f(x) = cx$, kde $c \in \mathbb{R}$, je opravdu řešením.

Ne vždy je ale řešení takto přímočaré a v jistém smyslu jednoduché. Mnohdy je potřeba postupně, navzájem na sebe navazujícími kroky, odvodit celou řadu skutečností (vlastností), z nichž konečně poskládáme, jak může funkce vypadat.

[14] Vůbec nemusíme vědět jaké řešení. Důležité je si říci: „Kdybychom řešení měli, tak by pro něj platily následující věci . . . “

[15] funkcionální rovnice má být pro funkci $f(x)$ splněna pro všechny dvojice $x, y \in \mathbb{R}$, proto musí být splněna i pro konkrétní dvojici hodnot $x = 0, y = 0$.

[16] rovnice je splněna pro všechny dvojice x, y, takže musí platit i pro speciální volbu $y = -x$

[17] na začátku dáváme $f((x_1 + x_2) + x_3) = f(x_1 + x_2) + f(x_3) = f(x_1) + f(x_2) + f(x_3)$, atd.

[18] že $\mathbb{Q}$ je *hustá* v $\mathbb{R}$ znamená, že libovolně blízko kteréhokoli reálného čísla najdeme nějaké racionální číslo

[19] Aspoň se zmínit o zkoušce je velice potřebné, protože jsme zjistili, co by musela funkce splňovat, kdyby existovala, ale nevíme ještě, jestli když funkce splňuje $f(x) = cx$, tak vyhovuje. Může se stát, že bude vyhovovat jen pro určitá c nebo pro žádné.

Základní vlastnosti funkcí

Funkce mohou mít tyto vlastnosti důvěrně známé ze střední školy:

(a) *sudá, resp. lichá*: platí $f(x) = f(-x)$, resp. $f(x) = -f(-x)$ pro všechna $x \in \mathbb{R}$

(b) *rostoucí, resp. klesající*: pro libovolná $x < y$ je $f(x) < f(y)$, resp. $f(x) > f(y)$

(c) *nezáporná* (nebo *kladná*): $f(x) \geq 0$ (nebo $f(x) > 0$)

(d) *prostá*: funkce nenabývá žádné hodnoty víc než jednou ($x \neq y \Rightarrow f(x) \neq \neq f(y)$)

(e) *na*: funkce nabývá všech hodnot aspoň jednou

(f) *bijekce*: funkce nabývá všech hodnot právě jednou (každému x z definičního oboru náleží právě jedno $f(x)$ z oboru hodnot)

(g) *spojitá*: zjednodušeně řečeno ji jde nakreslit jedním tahem

Tyto vlastnosti ve složitějších úlohách velmi pomáhají, nebo jsou dokonce nutným krokem k řešení. Rozeberme postupně jejich užitečnost.

ad (a). Sudost nebo lichost ulehčuje práci na polovinu, pokud je potřeba řešit rovnici zvlášť pro kladná a záporná čísla. Pomáhá též, pokud nám různým dosazováním vyjde soustava rovnic – je další pomocnou rovnicí.

ad (b). Je velice důležitá, protože může v úlohách řešených pomocí *Cauchyovy* metody nahradit *spojitost*. Také z ní plyne, že je funkce *prostá*. Významná je i její slabší varianta $x < y \Rightarrow f(x) \leq f(y)$, resp. $f(x) \geq f(y)$, která taktéž může nahrazovat *spojitost*, ale už neříká, že je funkce *prostá*.

ad (c). Tato vlastnost se zkrátka může hodit :)

ad (d). Velice důležitá vlastnost, která dává $f(a) = f(b) \Rightarrow a = b$, přičemž a a b můžou být i výrazy. Pokud je funkce zároveň *na*[20], dostáváme, že je *bijekcí*.

ad (e). V naprosté většině případů zajišťuje, že pro každé x existuje y takové, že $f(y) = x$. Pokud je funkce zároveň *prostá*, je to *bijekce*.

ad (f). Shrnuje v sobě vlastnosti funkce *prosté* a *na* a zároveň dodává silnou implikaci jestliže $f(x) = y$, tak $f(y) = x$.

ad (g). Jak bylo vidět v příkladu (2), řešeném pomocí *Cauchyovy* metody, hodí se spojitost při rozšíření z nějaké *husté* číselné množiny na $\mathbb{R}$. Touto hustou číselnou množinou mohou být všechna racionální čísla, všechna iracionální čísla, zlomky ve tvaru $a/2^b$, kde $a \in \mathbb{Z}$, $b \in \mathbb{N}$, atd.

[20] *na* obor hodnot

Cvičení na vlastnosti funkcí

Nyní následuje několik cvičení na předchozí užitečné vlastnosti.

Cvičení. Ukažte, že

(i) z $f(x+y) = f(x) + f(y)$, $x, y \in \mathbb{R}$ vyplývá, že je $f(x)$ lichá.

(ii) z $(f(x) + f(y))(f(u) + f(v)) = f(xu - yv) + f(xv + yu)$ pro $x, y, u, v \in \mathbb{R}$, plyne, že $f(x)$ je sudá. Nápověda k (ii): $x = 0, u = 1, v = 1$

Cvičení. Ukažte, že z každého z následujících bodů plyne, že je funkce $f(x)$ rostoucí, a tedy prostá (u (iii) jen neklesající):

(i) $\mathbb{R}^+ \to \mathbb{R}^+ : f(xf(y)) = f(xy) + x$.

(ii) $\mathbb{Q}^+ \to \mathbb{Q}^+ : f(x + f(x)y) = f(x)f(y)$ a $f(x) > 1$

(iii) $\mathbb{R}^+ \to \mathbb{R} : f(x^2 + y^2) = f(x^2) + f^2(y)$

Cvičení. Ukažte, že z každého z následujících bodů plyne, že je funkce $f(x)$ prostá, u (ii) a (iii) že je bijekcí:

(i) $\mathbb{R}^+ \to \mathbb{R} : f(x^2 + y^2) = f(x^2) + f^2(y)$

(ii) $\mathbb{R} \to \mathbb{R} : f(x^2 + f(y)) = y + (f(x))^2$

(iii) $\mathbb{Q}^+ \to \mathbb{Q}^+ : f(xf(y)) = f(x)/y$

Cvičení. Vyřešte na $\mathbb{R}$ funkcionální rovnici $f(x + y) = f(x) + f(y)$, když víte, že:

(i) $f(x)$ je neklesající

(ii) $f(x)$ je omezená na nějakém intervalu (a, b)

Cvičení. Vyřešte na $\mathbb{R}$ funkcionální rovnici $f(x + y) = f(x)f(y)$, když víte, že:

(i) $f(x)$ je neklesající

(ii) $f(x)$ je spojitá na nějakém intervalu (a, b)

Další tipy a triky

Tip č.1: Nenechte se vázat tím, že jsou x a y reálné proměnné. Například $f(x)$ je hodnota funkce v čísle x, takže je to také číslo, a můžete ho bez problému za x nebo y dosadit.

Tip č.2: Pokuste se na některé straně vhodným dosazením dostat symetrický výraz[21]. Symetrický výraz Vám pomůže následovně: v příkladu s funkcí$f : \mathbb{R}^+ \to \mathbb{R}^+$ a rovnicí $f(xf(y)) = f(xy) + x$ vezměme $x = f(t)$ a dostaneme

$$f(f(t)f(y)) = f(f(t)y) + f(t) = f(ty) + y + f(t); \;\; t, y \in \mathbb{R}.$$

[21]symetrický je takový výraz, že v něm můžeme prohodit názvy proměnných, aniž by se výraz změnil. Příkladem jsou $f(x) + f(y)$ nebo $f(f(x)f(y))$.

Výraz na levé straně je symetrický, proto lze proměnné prohodit i na pravé straně:

$$f(ty) + y + f(t) = f(yt) + t + f(y).$$

Odtud už snadno dostaneme $f(t) - t = f(y) - y$, výraz $f(t) - t$ nezávisí na t a proto musí platit $f(t) = t + const$.

Těžké příklady

V následujících příkladech hledejte všechna řešení funkcionálních rovnic na zadaných oborech. Rovnice jsou splněny pro všechny hodnoty z oboru, není-li řečeno jinak.

Příklad. $\mathbb{R}^+ \to \mathbb{R}^+ : x^2(f(x) + f(y)) = (x + y)f(f(x)y)$. (Celostátní kolo MO 2004)

Příklad. $\mathbb{R}^+ \to \mathbb{R}^+ : f(xf(y)) = f(xy) + x$. (Celostátní kolo MO 2002)

Příklad. $\mathbb{Q}^+ \to \mathbb{Q}^+ : f(xf(y)) = f(x)/y$. (IMO 1990)

Příklad. $\mathbb{Q}^+ \to \mathbb{Q}^+ : f(x + f(x)y) = f(x)f(y)$ (Golab-Schinzelova rovnice)

Příklad. $\mathbb{R} \to \mathbb{R} : f(x^2 + f(y)) = y + (f(x))^2$. (IMO 1992)

Příklad. $\mathbb{R} \to \mathbb{R} : (f(x) + f(y))(f(u) + f(v)) = f(xu - yv) + f(xv + yu)$. (IMO 2002)

Příklad. $\mathbb{R} \to \mathbb{R} : f(x - f(y)) = f(f(y)) + xf(y) + f(x) - 1$. (IMO 1999)

Literatura

K příspěvku byly použity znalosti z textu *Pavla Podbrdského*, který najdete na `http://mks.mff.cuni.cz/library/funkcionalni_rovnice2/funkcionalni_rovnice2.ps`

Dále jsem použil informace ze stránek *Johna Scholese*, kde najdete nespočetné množství olympijských příkladů všech typů. (Je jich tam kolem 4000, z nich asi polovina s řešením) Nachází se na adrese `http://www.kalva.demon.co.uk/`

Posledním zdrojem byla knížečka Školy Mladých Matematiků *Funkcionální rovnice*.

Těžké příklady na zobrazení

Franta Konopecký

Úvod

Toto bude doplňková přednáška k tomu, co se nestihlo na minulém soustředění. Bude náročná a budou se na ní dělat brutality. Pochopitelné, ale brutality. Je doporučeno před ní shlédnout přednášku z minulého soustředění.

Nelehké příklady

Příklad 1. Obrazy středu S kružnice opsané trojúhelníku ABC v osových souměrnostech podle přímek BC, AC, AB jsou vrcholy trojúhelníku $A_1B_1C_1$. Dokažte, že je tento trojúhelník shodný s trojúhelníkem ABC.

Příklad 2. Jsou dány dva různé body A, B a kružnice $k(S, r)$. Sestrojte všechny kružnice, které procházejí body A, B a vytínají na kružnici k tětivu délky $|AB|$. Bonbónek: Jak by to bylo s obecnou tětivou?

Příklad 3. Sestrojte na stranách AC, CB daného trojúhelníku ABC po řadě body X, Y tak, aby úsečky AX, XY a YB byly shodné.

Příklad 4. Na přímce h jsou dány body A, C, E v tomto pořadí. Ve stejné polorovině vyťaté přímkou h jsou pak rovnostranné trojúhelníky ABC a CDE. Střed úsečky AD označme S_{AD}, střed BE označme S_{BE}. Dokažte, že je trojúhelník $CS_{AD}S_{BE}$ rovnostranný.

Příklad 5. Kružnici k je vepsán rovnostranný trojúhelník ABC. Dokažte, že pro libovolný bod X kružnice platí: Největší ze vzdáleností bodu X od vrcholů trojúhelníku ABC je rovna součtu jeho vzdáleností od zbývajících dvou vrcholů.

Příklad 6. Je dán obecný trojúhelník ABC, který má ke svým stranám připsány rovnostranné trojúhelníky BCX, ACY, ABZ. Dokažte, že se přímky AX, BY a CZ protínají v jednom bodě a že dále platí $|AX| = |BY| = |CZ|$.

Příklad 7. V rovině je dán trojúhelník PQX, kde $|PQ| = 3$cm, $|PX| = 2,6$ cm, $|QX| = 3,8$ cm. Sestrojte pravoúhlý trojúhelník ABC tak, aby se jemu vepsaná kružnice dotýkala přepony AB v bodě P, odvěsny BC v bodě Q a aby bod X ležel na přímce AC.

Obtížnější příklady

Příklad 8. Je dán pravoúhlý rovnoramenný trojúhelník ABC s pravým úhlem při vrcholu C a bod X uvnitř tohoto trojúhelníku. Dokažte, že délky $|AX|$, $|BX|$ a $\sqrt{2}|XC|$ jsou délkami stran trojúhelníku.

Příklad 9. Kružnice k_1 a k_2 mají vnější dotyk v bodě A a současně se obě dotýkají zevnitř kružnice k v bodech A_1 a A_2. Bod P je jeden z vnějších průsečíků společné vnitřní tečny kružnic k_1 a k_2 s kružnicí k. Nakonec, body B_i jsou druhé průsečíky přímek PA_i s kružnicí k_i $(i = 1, 2)$. Dokažte, že se přímka B_1B_2 dotýká obou kružnic k_1, k_2.

Příklad 10. Nechť $ABCD$ je tětivový čtyřúhelník. Označme postupně P, Q a R paty kolmic z bodu D na přímky BC, CA a AB. Dokažte, že $|PQ| = |QR|$ právě tehdy, když se osy úhlů ABC a ADC protínají na přímce AC.

Slíbené brutality

Příklad 11. Nechť $ABCD$ je daný konvexní čtyřúhelník s různoběžnými stranami BC a AD. Body E, F leží po řadě uvnitř stran BC a AD tak, že $\frac{|BE|}{|CE|} = \frac{|DF|}{|AF|}$. Přímky AC a BD se protínají v bodě P, přímky BD a EF v bode Q, přímky EF a AC v bodě R. Uvažujme všechny trojúhelníky PQR pro různé polohy bodů E a F. Ukažte, že kružnice opsané těmto trojúhelníkům mají společný bod různý od P.

Příklad 12. V rovině je dán trojúhelník KLM a bod A ležící na polopřímce opačné k polopřímce KL. Sestrojte pravoúhelník $ABCD$, jehož vrcholy B, C a D leží po řadě na přímkách KM, KL a LM. (Calábek ...)

Zdroj

Minulý příspěvek do sborníčku s názvem *Geometrická zobrazení*. Najdete ho na stránkách Prasátka (`http://mks.mff.cuni.cz`) v Knihovně.

Konstrukce pomocí koulítka a rovinítka

Anša Lauschmannová

Na přednášce si ukážeme řešení následujících úloh, v nichž máš k dispozici pouze koulítko a rovinítko (případně jen koulítko). Koulítko funguje tak, že ho zabodneš do nějakého bodu trojrozměrného prostoru, nastavíš poloměr a opíšeš tomuto bodu sféru (podobně jako kružítkem opíšeš kružnici). Rovinítko umožňuje narýsovat rovinu určenou danými třemi body (podobně jako pravítkem narýsuješ přímku procházející dvěma body).

Příklad 1. Sestrojte kouli opsanou danému čtyřstěnu.

Příklad 2. Sestrojte rovinu, která prochází daným bodem a je rovnoběžná k dané rovině.

Příklad 3. Sestrojte čtyřstěn, jsou-li zadána těžiště jeho stěn.

Příklad 4. Sestrojte kouli vepsanou danému čtyřstěnu.

Příklad 5. Nechť jsou dány body $S, S_{AB}, S_{BD}, S_{CD}$, které neleží v jedné rovině. Sestrojte čtyřstěn $ABCD$ takový, že S je střed koule jemu opsané a S_{AB}, S_{BD}, S_{CD} jsou po řadě středy hran AB, BD, CD.

Příklad 6. Sestrojte kouli, která prochází danými dvěma body a dotýká se daných dvou koulí.

Příklad 7. Nechť jsou dány nekolineární[22] body T_A, V_A, T_C, přímka p mimoběžná s přímkou T_AV_A a úsečka délky d. Sestrojte čtyřstěn $ABCD$ takový, že T_A, resp. T_C je těžiště stěny BCD, resp. ABD, V_A je pata výšky spuštěné z vrcholu A na stěnu BCD, bod B leží na přímce p a vzdálenost $|CV_A|$ je rovna d.

Příklad 8. Sestrojte krychli **pouze koulítkem**, jsou-li dány délky stěnové a tělesové úhlopříčky.

Poznámka na závěr

Všech osm úloh je převzato ze 6. série 19. ročníku našeho semináře, takže pokud si řešení raději přečteš v klidu domova, než vyslechneš na přednášce, na přednášku určitě nechoď.

[22] Tedy takové, že neleží na společné přímce.

Úvod do kryptológie

Rasťo Oľhava

Úvod

Ľudia sa už od nepamäti snažili uchovať svoje tajomstvá. Problémy však nastávajú ak sa chceme s niekým so svojími tajomstvami podeliť, ale tak aby sa o nich ostatné nežiadúce osoby nedozvedeli. Tento problém sprevádza ľudstvo už mnohé stáročia a dokonca podmienil vznik novej vedy *kryptológie*. Počas tejto prednášky si objasníme základne pojmy z tohto oboru a vyskúšame si spôsoby riešenia na konkrétnych príkladoch.

Základné pojmy

otvorený text. pôvodný text, ktorý ideme zašifrovať

šifrový text. zašifrovaný otvorený text

kryptografia. veda zaoberajúca sa šifrovaním t.j. zmenou vzhľadu textu tak aby bol obsah textu skrytý

kryptoanalýza. veda zaobeajúca sa dešifrovaním t.j. odhalením obsahu šifrového textu

kryptológia. vedná disciplína skladajúca sa z kryptoanalýzy a kryptografie

monogram. jedno písmeno

bigram, trigram, ... , polygram. skupina susediacich písmen v používanej abecede, napr. pentagram PRASE

šifrový systém (alebo algoritmus). akýkoľvek systém, ktorý vieme použiť na zašifrovanie otvoreného textu

Poznámka. Zistilo sa, že utajovanie šifrového systému je vo viacerých prípadoch nemožné, a preto je vo väčšine prípadov kryptoanalytikom šifrový systém známi. Ako je teda možné, že ak poznajú spôsob utajenia, nie je ich úloha už vyriešená? Odpoveďou je veľkosť množiny kľúčov. Aj pri použití rovnakého šifrového systému sa zmenou *kľúča dostáva* pred codebreakra (z ang. kryptoanalytik) úplne nová úloha. A teda čím väčšia je množina kľúčov, tým ťažšie je „odskúšať všetky možnosti(kľúče)“. Teda jedným zo znakov dobrej šifry je aby veľkosť množiny kľúčov presiahla možnosti výpočetnej kapacity aj tých najrýchlejších počítačov.

Klasické šifry

Najstaršie, a teda aj najjednoduchšie šifry delíme na dve základne typy: *substitučné* a *transpozičné*. Princípom substitučných šifier je nahradenie znaku z otvoreného textu iným (nie nutne iným) znakom, podľa určitého pravidla. Pričom pri transpozičných šifrách zameníme len poradie znakov v texte.

Modulárna aritmetika

Ešte pred uvedením jednotlivých šifier by sme mali vedieť čo je modulárna aritmetika. Zjednodušene je to aritmetika v ktorej počítame len na obmedzenej množine čísel napr. my budeme počítať na množine $0, 1, \ldots, 25$, pretože budeme používať anglickú abecedu, ktorá obsahuje 26 písmen. V praxi to bude vyzerať tak, že ak posunieme napr. písmeno Y ($A = 1$, $B = 2$, ...) o písmeno E, získame písmeno D, pretože $Y = 25$, $E = 5$ a $25 + 5 = 30$, lenže počítame len na množine zvyškov po delení 26, kde sa číslo 30 nenachádza. A tak číslo 30 reprezentuje také písmeno aké reprezentuje jeho zvyšok po delení 26, čo je $4 = D$.

Prehľad šifier

Caesarova šifra. Šifrový text vznikne z otvoreného posunutím každého znaku o k znakov. Číslo k je v tomto prípade rovnaké vo všetkých prípadoch. Nevýhodou je, že počet možných kľúčov (hodnôt čísla k) je obmedzený počtom znakov, ktoré používame (označím si ho ako n), a teda nie je problémov ich všetky odskúšať.

Jednoduchá zámena. Každý znak je nahradený nie nutne, ale väčšinou iným znakom z abecedy, ktorú používame. Takže kľúčom je konkrétna permutácia znakov abecedy, ktorú používame. Veľkosť množiny kľúčov sa nám teda rapídne zvýšila $(n!)$.

Vigenerova šifra. Je podobná ako Caesarova šifra s tým rozdielom, že počet znakov o koľko posúvam abecedu nie je rovnaký pre všetky znaky v otvorenom texte, ale len pre každý s-tý znak. To znamená, že kľúčom je reťazec znakov odĺžky s, v ktorom každý jeho znak reprezentuje príslušný posun.

Vernamova šifra. Zatiaľ jediná dokazateľne absolútne bezpečná šifra. S otvoreným textom sčítame náhodný reťazec - kľúč. Nevýhodou je potreba predania kľúča adresátovi. Na to môžeme použiť len cesty aké máme a tie nie sú bezpečné, pretože by sme nimi potom mohli posielať priamo otvorený text bez nutnosti zašifrovať ho.

Transpozičné šifry. Ako je už vyššie uvedené ich princípom je zmena poradia písmen v otvorenom texte. Ich použitie vieme ľahko rospoznať podľa toho, že v šifrovom texte je rovnaký výskyt znakov ako v bežnom jazyku.

Príklad 1. Vieme, že nasledujúci text bol vytvorený jednoduchou zámenou z anglického textu, a ďalej vieme, že medzery v pôvodnom texte boli pred zašifrovaním nahradené písmenom Z. Nájdite otvorený text.

MJZYB LGESE CNCMQ YGXYS PYZDZ PMYGI IRLLC PAYCK YKGWZ MCWZK YFRCM ZYVCX XZLZP MYXLG WYMJS MYGPZ YWCAJ MYCWS ACPZY XGLYZ HSWBN ZYXZT YTGRN VYMJC POYMJ SMYCX YMJZL ZYSLZ YMTZP MQYMJ LZZYB ZGBNZ YCPYS YLGGW YMJZP YMJZL ZYCKY SPYZD ZPKYI JSPIZ YMJSM YMJZL ZYSLZ YMTGY GXYMJ ZWYTC MJYMJ ZYKSW ZYECL MJVSQ YERMY MJCKY CKYKG

Príklad 2. Nasledujúci šifrový text vznikol z anglického textu, v ktorom boli medzery nahradené písmenom Z, pomocou Vigenerovej šifry. Zistite dĺžku kľúča, kľúč a pôvodný otvorený text.
HQEOT FNMKP ELTEL UEZSI KTFYG STNME GNDGL PUJCH QWFEX FEEPR PGKZY EHHQV PSRGN YGYSL EDBRX LWKPE ZMYPU EWLFG LESVR PGJLY QJGNY GYSLE XVWYP SRGFY KECVF XGFMV ZEGKT LQOZE LUIKS FYLXK HQWGI LF

Záver

Týmto chcem poďakovať Martinovi Dunglovi, ktorého príspevok o šifrách mi poskytol značnú inšpiráciu a niektoré úseky jeho príspevku sú až na poslovenčenie priamo použité v mojom.

Zdroje

`http://www.karlin.mff.cuni.cz/~tuma/nciphers.html`

RSA a teorie čísel

Jakub „šnEk“ Opršal

Definice. *Buď n přirozené číslo. Řekneme, že čísla $a, b \in \mathbb{N}$ jsou kongruentní modulo n pokud $n \mid (a-b)$. Ekvivalentně pokud a a b dávají stejný zbytek po dělení n. Zapisujeme $a \equiv b \pmod{n}$*

Věta. (Fermat) *Nechť $a \in \mathbb{N}$ a p je prvočíslo, navíc platí $p \nmid a$ pak platí:*

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

Důkaz. Uvažme množinu čísel $\{a, 2a, \ldots, (p-1)a\}$. Tyto čísla dávají po dvou různý zbytek po dělení p, neboť kdyby ne, tj. $ka \equiv la \pmod{p}$) pro nějaká $k, l \in 1, 2, \ldots p-1$ a $k > l$, pak dostáváme $p \mid (ka - la) = (k-l)a$. Tedy p dělí buď a, což je ve sporu s předpokladem věty, nebo $k - l$, což je číslo menší než p, každopádně dostáváme spor. Z toho lze také vidět, že všechna dávají nenulový zbytek po dělení p. Tedy nabývají všech zbytků, proto platí:

$$(p-1)! = 1 \cdot 2 \cdots 3 \equiv a \cdot 2a \cdots (p-1)a = (p-1)! \cdot a^{p-1} \pmod{p}$$

Protože $(p-1)!$ je nesoudělné s p mohu tuto kongruenci pokrátit a dostanu tvrzení věty. □

Věta. (Euler) *Nechť $a, n \in \mathbb{N}$ jsou dvě nesoudělná čísla a $\varphi(n)$ je počet čísel menších nebo rovných n, která jsou s n nesoudělná, pak platí:*

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

Lemma. (Výpočet Eulerovy funkce) *Nechť $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ je prvočíselný rozklad čísla n (tedy p_i jsou po dvou různá prvočísla a α_i jsou přirozená). Pak platí:*

$$\begin{aligned}\varphi(n) =& (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1} = \\ =& n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\end{aligned}$$

Definice. *Nechť n je přirozené a p prvočíslo, pak řádem čísla n modulo p nazveme nejmenší takové přirozené číslo k, že $n^k \equiv 1 \pmod{p}$.*

Lemma. *Nechť p je prvočíslo a n je přirozené číslo nesoudělné s p a k jeho řád. Čísla a a b jsou libovolná nezáporná celá. Pak platí:*

(i) $n^{ka} \equiv 1 \pmod{p}$
(ii) $n^a \equiv n^b \pmod{p} \iff a \equiv b \pmod{k}$
(iii) $k \mid (p-1)$

Definice. *Nechť n je přirozené číslo. Přirozené číslo a nazveme primitivním prvkem modulo n, pokud je řádu $\varphi(n)$. Ekvivalentně pokud $a, a^1, \ldots, a^{\varphi(n)}$ dávají všechny zbytky modulo n, které jsou s n nesoudělné.*

Lemma. *Je-li p liché prvočíslo, pak existuje primitivní prvek modulo p.*

Věta. *Nechť p je prvočíslo, pak platí:*

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Věta. (Rabin-Millerův test prvočíselnosti) *Pokud n je přirozené číslo, pak platí implikace:*

$$n \text{ je prvočíslo} \Longrightarrow \forall a \in \{1, 2, \ldots, n-1\} : a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$$

Definice. *Přirozené číslo n nazveme Carmichealovým pokud pro něj platí:*

$$\forall a \in \mathbb{N} : a^n \equiv a \pmod{n}$$

Carmichaelova čísla mají význam v tom, že co se týče prvočíselných testů jsou velmi těžko rozeznatelná oproti prvočíslům (díky tomu se jim říká pseudoprvočísla). Nejmenší Carmichaelova čísla jsou $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$ a $1729 = 7 \cdot 13 \cdot 19$.

RSA

Šifrovací algoritmus RSA patří mezi asymetrické šifry, tedy pro zašifrování a odšifrování jsou použity dva různé (tedy relativně různé) algoritmy. Kvůli tomuto se musí vygenerovat dva klíče a to soukromý a veřejný. Klíče se generují následovně:

(i) Vybereme dost velká a dostatečně náhodná prvočísla p a q.
(ii) Spočítáme $n = pq$ a hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$. n bude použito jako část obou klíčů, bude se používat jako modul pro veškeré operace.
(iii) Zvolíme náhodné e takové, že $1 < e < \varphi(n)$ a e je nesoudělné s $\varphi(n)$, toto e bude součástí veřejného klíče.
(iv) Ze znalosti $\varphi(n)$ spočteme d tak, že $de \equiv 1 \pmod{\varphi(n)}$, d bude použito jako součást soukromého klíč.

Tedy máme veřejný klíč a to dvojici čísel (n, d) a soukromý klíč, dvojici (n, e).

Algoritmy na zašifrování a odšifrování jsou jednoduché. Tajnou zprávu, kterou převedeme do nějakého rozumného číselného formátu, zašifrujeme tak, že ji umocníme na e modulo n. Odšifrujeme tak, že šifrový text umocníme na d opět modulo n.

Uveďme ještě jeden nereálný, zato o to čitelnější, příklad použití RSA. Nejdříve si vymyslíme dvě prvočísla, třeba $p = 17$ a $q = 29$, spočítáme $n = 17 \cdot 29 = 493$ a $\varphi(n) = 448$ Zvolme si nějaký rozumný veřejný klíč $e = 33$ (e musí být nesoudělné s $\varphi(n) = 448$) a spočítáme k němu soukromý $ed + k\varphi(n) = 1$, použijeme Euklidův algoritmus na čísla $e = 33$ a $\varphi(n) = 448$ a vyjde nám $d = 353$ a jako balast $k = -26$.

A nyní si vyzkoušejme naše klíče s tajnou zprávou $m = 42$. Nejdříve zašifrujeme:

$$s = m^e \bmod n = 42^{33} \bmod 493 = 93,$$

a pak odšifrujeme:

$$m = s^d \bmod n = 93^{353} \bmod 493 = 42.$$

Takže to funguje ;-) (Proč, to už určitě tušíte.)

Kvadratické zbytky

Jakub „šnEk“ Opršal

Definice. *Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$. Řekneme, že a je kvadratickým zbytkem modulo n pokud existuje $c \in \mathbb{N}$ takové, že $c^2 \equiv a \pmod{n}$. V opačném případě řekneme, že a je kvadratickým nezbytkem.*

Definice. *Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak definujeme Legendreův symbol $\left(\frac{a}{p}\right)$ následovně:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{pro } p|a \\ +1 & \text{pokud } a \text{ je kvadratickým zbytkem a } p \nmid a \\ -1 & \text{pokud } a \text{ neni kvadratickym zbytkem} \end{cases}$$

Lemma. (Počet kvadratických zbytků) *Nechť p je liché prvočíslo, pak mezi čísly $1, 2, \ldots, p-1$ je právě $\frac{p-1}{2}$ kvadratických zbytků modulo p a stejně tolik kvadratických nezbytků.*

Věta. (Eulerovo kritérium) *Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak platí:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Důkaz. Případ $p|a$ je jednoduchý, zaměříme se tedy na případ $p \nmid a$. Podle malé Fermatovy věty platí:

$$a^{p-1} \equiv 1 \pmod{p}$$
$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p}$$

Tedy $a^{\frac{p-1}{2}} \equiv \pm 1$ (Protože p je prvočíslo.)

Je-li a kvadratický zbytek pak platí, že existuje $c \in \mathbb{Z}$ takové, že $c^2 \equiv a$ tedy $a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1$ (opět podle malé Fermatovy věty), tedy pro kvadratický zbytek věta platí. Navíc žádné jiné číslo kromě $\frac{p-1}{2}$ nenulových kvadratických zbytků modulo p nemůže splňovat $a^{\frac{p-1}{2}} - 1 \equiv 0$, protože levá strana této kongruence je mnohočlen stupně $\frac{p-1}{2}$ a proto má tato rovnice nejvýše $\frac{p-1}{2}$ kořenů modulo p. Tedy pro kvadratické nezbytky platí: $a^{\frac{p-1}{2}} \equiv -1$. □

Uvažme dvě reprezentace zbytků po dělení nějakým lichým prvočíslem p a to množiny:

$$M = \{-\tfrac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \tfrac{p-1}{2}\}$$
$$N = \{0, 1, \ldots, p-1\}$$

Dále pro nějaké celé číslo a $(p \nmid a)$ uvažme posloupnosti délky $p-1$:

$$M(a) = \left\langle m_k \in M : k \in \{1, 2, \ldots, \tfrac{p-1}{2}\}, ka \equiv m_k \pmod p \right\rangle$$
$$N(a) = \left\langle n_k \in N : k \in \{1, 2, \ldots, \tfrac{p-1}{2}\}, ka \equiv n_k \pmod p \right\rangle$$

Označme $m(a)$ počet záporných členů $M(a)$ a obdobně $n(a)$ počet členů $N(a)$ větších než $\frac{p-1}{2}$. Uvědomme si, že záporné členy $M(a)$ dostaneme z členů $N(a)$, které jsou větší než $\frac{p-1}{2}$ tak, že od nich odečteme p, tedy speciálně dostáváme $n(a) = m(a)$.

Zamyslíme-li se hlouběji snadno přijdeme na to, že pokud v posloupnosti $N(a)$ změníme znaménka všech členů na kladná (označme takovou posloupnost $N^+(a)$) dostaneme všechny zbytky od 1 do $\frac{p-1}{2}$, neboť kdybychom uvážili posloupnost

$$M_-(a) = \left\{ < m_{-k} \in M : k \in \{1, 2, \ldots, \tfrac{p-1}{2}\}, -ka \equiv m_{-k} \pmod p \right\}$$

Tak tato posloupnost má právě členy opačných znamének, než $M(a)$ a obě posloupnosti dohromady mají za členy všechny nenulové zbytky modulo p.

Věta. (Gaussovo lemma) *Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo, navíc $p \nmid a$, pak platí:*

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

Důkaz. Protože $m(a) = n(a)$ stačí nám dokázat první rovnost. Platí:

$$\left(\frac{p-1}{2}\right)! = \prod_{m \in M^+(a)} \equiv (-1)^{m(a)} \prod_{k=1}^{\frac{p-1}{2}} ka = (-1)^{m(a)} a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

Pokrácením $\left(\frac{p-1}{2}\right)!$ (což je jistě nesoudělné s p) na obou stranách a použitím Eulerova kritéria dostaneme kongruenci $1 \equiv (-1)^{m(a)} \left(\frac{a}{p}\right)$, což lze snadno upravit do požadovaného tvaru vynásobením $(-1)^{m(a)}$. □

Věta. (Zákon kvadratické reciprocity) *Nechť p, q jsou dvě lichá prvočísla, pak platí:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$
$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

Lemma. (Nutnost čtyř čtverců) *Nechť $k, m \in \mathbb{N} \cup \{0\}$. Číslo $4^m(8k+7)$ nelze zapsat jako součet nejvýše tří čtverců přirozených čísel.*

Věta. (Lagrange) *Každé přirozené číslo lze zapsat jako součet nejvýše čtyř čtverců přirozených čísel.*

Matematická heuristika

Pavel Paták

Úvod

Pokud nás řešení příkladu nenapadá na první pohled, musíme systematicky vyzkoušet množství možností. Matematická heuristika se zabývá tím, jak nejrychleji nalézt tu správnou. Ukazuje se, že existuje pár postupů, které vedou k cíli téměř vždy. Ty nejpoužívanější si vysvětlíme a ukážeme na příkladech.

Důkazy existence

Chceme-li dokázat, že nějaký objekt existuje, téměř jistě využijeme jedno z následujících tvrzení.

Tvrzení. (Nutná existence) Jde-li daný objekt zkonstruovat, pak existuje.

Příklad. Nechť $a \in \mathbb{N}$. Dokažte, že rovnice $x^2 - y^2 = a^3$ má celočíselné řešení.

Tvrzení. (Dirichletův princip)

(1) Je-li $n+1$ perel rozděleno do n šuplíků, pak existuje alespoň jeden šuplík, ve kterém jsou alespoň 2 perly.
(2) Vlétlo-li alespoň $kn+1$ holubů do k děr holubníku, pak existuje alespoň jedna díra, do které vlétlo více než n holubů.
(3) Je-li nekonečně mnoho molů v konečně mnoha skříních, aspoň v jedné z nich jich musí být nekonečně.

Cvičení.

(1) Kolik osob je minimálně zapotřebí, abychom mohli tvrdit, že existují 3 osoby mající narozeniny ve stejný den?
(2) Ve čtverci o straně délky 7 je 51 bodů. Dokažte, že vždy existují tři body, které leží v kruhu o poloměru 1.
(3) Střelecký terč ve tvaru rovnostranného trojúhelníka byl 17-krát trefen. Co můžeme říct o minimu vzdáleností mezi jednotlivými trefami?
(4) Každý bod prostoru je obarven červeně nebo modře. Ukažte, že existuje kvádr, jehož vrcholy mají všechny stejnou barvu.
(5) Každý bod prostoru je obarven modře, červeně či zeleně. Označme M, Č, Z množiny všech čísel r takových, že existuje úsečka délky r, jejíž oba koncové body jsou modré (červené, zelené). Dokažte, že alespoň jedna z těchto množin obsahuje všechna kladná reálná čísla.
(6) Body s celočíselnými souřadnicemi nazýváme mřížové body. V prostoru

vybereme libovolných 9 mřížových bodů $B_1, B_2, ...B_9$. Dokažte, že střed jedné z úseček B_iB_j $(1 \leq i < j \leq 9)$ je mřížovým bodem.

(7) V obdélníku 10x17 je 74 bodů. Dokažte, že existují dva, jejichž vzdálenost je maximálně 2.

(8) Nechť p je prvočíslo větší než 3 a n přirozené číslo takové, že p^n má v desítkovém zápisu 20 cifer. Dokažte, že alespoň jedna z cifer se objevuje více než dvakrát.

(9) Nechť P je množina n prvočísel. M buď množina více než n přirozených čísel, z nichž žádné nemá prvočinitele, který by neležel v P. Dokažte, že existuje $T \subseteq M$ taková, že součin všech čísel z T je čtverec.

Dirichletův princip je speciální případ následující hrůzostrašně vypadající věty:

Věta. (Ramsey) *Pro každé n a pro každou t-tici čísel $k_1, k_2, \ldots, k_n$ existuje číslo $r(k_1, k_2, \ldots, k_t; n)$ takové, že pro každou množinu A, která má alespoň r prvků platí: Rozdělíme-li všechny n-prvkové podmnožiny A do t přihrádek $T_1, T_2, \ldots, T_t$, pak existují $F \subseteq A$ a i takové, že F má velikost aspoň k_i a každá n-prvková podmnožina F náleží do T_i. Nejmenší takové číslo r se nazývá Ramseyovo číslo.*

Triviální případy jsou:

$$r(k_1, \ldots, k_t; 1) = 1 + \sum_{i=1}^{t} (k_i - 1)$$
$$r(k_i, r; r) = r(r, k_1; r) = k_1$$

Je-li některé k_i je menší než n, platí navíc $r(k_1, \ldots, k_t; n) = k_i$.

Ostatní Ramseyova čísla se nazývají netriviální. Je jich známo 12. Pro zbylá čísla máme jen hrubé odhady. Např.

$$k_1, k_2 \leq r(k_1, k_2; n) \leq \binom{k_1 + k_2 - 2}{k_1 - 1}.$$

Příklad. Mezi šesti lidmi vždy existují 3 lidé, kteří se navzájem neznají nebo tři lidé, kteří se navzájem znají. Pro 5 lidí to již neplatí.

Nevíme-li, jak v existenčním důkazu začít, zkusíme využít následující jednoduché tvrzení:

Tvrzení. (Existence maxima a minima) Každá konečná množina čísel obsahuje maximální a minimální prvek.

Prostě si vybereme nějaký objekt, který je svým způsobem výjimečný.

Cvičení.

(1) Dokažte, že každý konvexní mnohostěn obsahuje dvě stěny se stejným počtem hran.

(2) V rovině je n studní a n domů. Dokažte, že domy jdou spojit se studnami tak, že žádné dvě cesty se nebudou křížit.
(3) V rovině je dán konečný počet bodů, které nejsou všechny kolineární. Dokažte, že existuje přímka, která prochází právě přes dva z nich.

Důkazy neexistence

Máme-li dokázat, že něco neexistuje, buď najdeme nějaký vhodný invariant, či zvolíme důkaz sporem.

Cvičení.

(1) Na každé pole šachovnice 7x7 postavíme jezdce, je možné potáhnout všemi jezdci naráz dle šachových pravidel?
(2) Může pro přirozená čísla a, b, c platit $(2^a - 1)(2^b - 1) = 2^{2^c} + 1$?

Využití symetrie

Ačkoli se symetrie nejčastěji využívá v geometrii, můžeme ji uplatnit téměř kdekoli. Je-li problém symetrický, ušetří nám to spoustu času a práce. Máme-li důvod se domnívat, že je symetrické i řešení, rovnou odvrhneme všechny nesymetrické nápady. Speciálním případem je tzv. princip nedostatečného důvodu, tj. tvrzení, že kde není důvod na rozlišení, tam nemůže být rozdíl.

Příklad. Roznásobte $(a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$

Řešení. Vzhledem k symetrii víme, že výsledek je tvaru $A(a^3+b^3+c^3)+B(a^2b+ +a^2c+b^2a+b^2c+c^2a+c^2b)+C(abc)$. A okamžitě vidíme, že $A = 1, B = 0, C = -3$.

Příklad. Zjednodušte $\frac{(d-b)(d-c)}{(a-b)(a-c)} + \frac{(d-a)(d-c)}{(b-a)(b-c)} + \frac{(d-a)(d-b)}{(c-a)(c-b)}$

Řešení. Nejprve si všimneme, že výraz je symetrický vzhledem k a, b, c. Aby měl výraz smysl, musí platit $a \neq b$. Ze symetrie tedy $a \neq b \neq c \neq a$

Daný výraz je vlastně polynom $P(d)$ (nejvýše druhého stupně). Dosazení $d = a$ a symetrie dává, že $P(a) = P(b) = P(c) = 1$. Jedná se tedy o konstantní polynom a výraz je vždy roven jedné.

Příklad. Najděte maximum výrazu xy za podmínek $x + y = 1, x > 0, y > 0$.

Řešení. Vztahy jsou symetrické, můžeme tedy očekávat, že maximum nastane pro $x = y = \frac{1}{2}$. Nemá důvod nastávat jinde. Ověříme to: Buď $x = \frac{1}{2} + e$, $y = \frac{1}{2} - e$. Pak $xy = \frac{1}{4} - e^2$, tedy maximum skutečně nastává pro $e = 0$

Cvičení.

(1) Dva hráči pokládají mince na obdélníkový stůl tak, aby se nepřekrývaly.

Kdo již nemůže položit minci na stůl prohrál. Má některý z hráčů vyhrávající strategii? Jestli ano, kdo a jakou?

(2) Dokažte pro $a, b, c > 0$ nerovnost $\frac{bc}{a} + \frac{ca}{b} + \frac{ab}{c} \geq a + b + c$.

(3) Najdete minimum výrazu $x_1^2 + x_2^2 + \ldots + x_n^2$ za podmínek $0 < x_i < 1$ a $x_1 + x_2 + \ldots x_n = 1$.

(4) V libovolném trojúhelníku platí $\frac{1}{3} \leq \frac{a^2+b^2+c^2}{(a+b+c)^2} \leq \frac{1}{2}$. Přitom odhad $\frac{1}{2}$ nejde zlepšit.

Hledání zákonitostí

Když už nás nenapadá nic jiného, zkusíme si napsat pár jednoduchých příkladů, vyřešit problém pro malá čísla apod. Postupujeme přitom systematicky, abychom se vyhnuli zbytečné práci. Třeba nás časem něco napadne.

Cvičení.

(1) Buď S_1 posloupnost 1,2,3,4, ... všech přirozených čísel. Nechť S_{n+1} vznikne z S_n tak, že čísla z S_n, která jsou dělitelná n zvětšíme o jedničku. S_2 je tedy posloupnost 2,3,4,5,6,7, ... a S_3 posloupnost 3,3,5,5,7,7, ... Najděte všechna přirozená čísla, pro která platí, že prvních $n-1$ členů S_n má stejnou hodnotu.

(2) Definujme rekurentně zadanou posloupnost $a_1 = 1, a_2 = 1, a_3 = 2$,

$$a_{n+3} = \frac{a_{n+1}a_{n+2} + 7}{a_n}$$

pro $n > 0$. Dokažte, že všechna členy jsou přirozená čísla.

Ostatní postupy

Metod jak řešit matematické úlohy existuje pochopitelně celá řada, uvedu jen letmý výčet dalších metod: kreslení obrázků, přeformulování zadání, modifikace problému (dokážeme silnější tvrzení), výběr vhodného označení, rozdělí problému na speciální případy, zpětný postup, nepřímý postup, zevšeobecnění.

Při řešení každého příkladu se vždy snažme svůj postup reflektovat. Naše schopnosti řešit cokoli se velice rychle zvýší, pokud si uvědomíme, že ke každému příkladu se hodí jiná metoda a dovedeme co nejrychleji vybrat tu správnou. Ale pokud nic nevíme, tak je nám i sebelepší heuristika na nic.

Geometria

Zuzka Pôbišová

Na prednáške si zopakujeme vety o obvodových a stredových uhloch a mocnosti bodu ku kružnici a budeme riešiť príklady v ktorých sa využívajú. Na záver si dokážeme niekoľko jednoduchých vlastností trojuholníka na ktoré sa často zabúda a môžu sa hodiť.

Veta. (Obvodové a stredové uhly) *Majme kružnicu k so stredom S, jej tetivu AB a ľubovoľný bod $M \in k$ na väčšom (menšom) oblúku AB. Potom menší (väčší) z uhlov ASB nazývame stredový uhol príslušný k tetive AB a uhol AMB obvodový a platí $2|\sphericalangle AMB| = |\sphericalangle ASB|$.*

Veta. (Úsekový uhol) *Majme kružnicu k so stredom S, jej tetivu AB a dotyčnicu AX ku kružnici v bode A. Uhol BAX nazývame úsekový uhol a má rovnakú veľkosť ako obvodový uhol príslušný k tomu oblúku AB, ktorý leží v opačnej polrovine určenej priamkou AB ako uhol BAX.*

Veta. (Mocnosť) *Majme kružnicu k a bod P. Bodom P vedieme ľubovoľnú sečnicu kružnice k, ktorá ju pretne v bodoch A, B. Mocnosť bodu P ku kružnici k definujeme ako $\mu(P,k) = |PA| \cdot |PB|$ a je rovnaká pre všetky sečnice kružnice k prechádzajúce bodom P. Ak t je dotyčnica ku kružnici k z bodu P, tak $A = B$ a $\mu(P,k) = |PA|^2$.*

Príklad. Nech k_1, k_2 sú kružnice pretínajúce sa v dvoch bodoch A, B. Priamky p, q také, že $A \in p$, $B \in q$ pretínajú k_1 a k_2 v ďalších štyroch bodoch, C, $D \in k_1$, E, $F \in k_2$. Dokáž, že CD a EF sú rovnobežné.

Príklad. Nech k_1, k_2 sú kružnice pretínajúce sa v dvoch bodoch A, K. Potom zostrojíme ΔKLM taký, že $A \in LM$, $L \in k_1$ a $M \in k_2$. Kedy bude mať ΔKLM najväčší obsah?

Príklad. Dve kružnice k_1 a k_2 sa pretínajú v dvoch bodoch A, B. Na k_1 sú ďalej dané 2 rôzne body C, D. Sečnica BC vytína na k_2 bod E, podobne BD bod F. Dokáž, že ak $|DF| = |CE|$, tak bod A je rovnako vzdialený od priamok BC a BF.

Príklad. Majme 3 zhodné kružnice pretínajúce sa v jednom bode O. Ostatné priesečníky označme A, B, C. Dokáž, že O je ortocentrum ΔABC.

Príklad. Vnútri strany AC trojuholníka ABC leží bod D taký, že $|AB| = |CD|$ a uhly ACB a ABD majú rovnakú veľkosť. Os uhla CAB pretína stranu BC v bode E. Dokáž, že priamky AB a DE sú rovnobežné.

Veta. *V trojuholníku ABC nech os uhla ACB pretína stranu AB v bode X.*

Potom

$$\frac{|AC|}{|BC|} = \frac{|AX|}{|BX|}.$$

Tj., os uhla v trojuholníku rozdeľuje protiľahlú stranu v pomere priľahlých.

Veta. *V trojuholníku ABC nech p je os uhla ACB, q nech je os strany AB a k nech je kružnica opísaná trojuholníku ABC. Potom p, q, k sa pretínajú v jednom bode. Tj., os uhla a os protiľahlej strany sa pretínajú na opísanej kružnici.*

Veta. *V trojuholníku ABC nech O je ortocentrum a výška na stranu AB nech sa pretína so stranou AB v bode Y a s opísanou kružnicou v bode X. Potom $|OY| = |YX|$. Tj., výška pretína opísanú kružnicu v bode súmerne združenom s ortocentrom podľa strany trojuholníka.*

Veta. *V trojuholníku ABC nech X je päta výšky na stranu AB a Y nech je priesečník osi uhla ACB so stranou AB. Potom*

$$|\sphericalangle XCY| = \left| \frac{|\sphericalangle ABC| - |\sphericalangle BAC|}{2} \right|.$$

Tj., uhol medzi osou uhla a výškou prislúchajúcou k jednému vrcholu sa rovná polovici rozdielu zvyšných dvoch uhlov v trojuholníku.

Nerovnosti

Michal Rušin a Martin Tancer

Úvod

V tomto příspěvku najdeš některé známé nerovnosti. Nerovnosti jsou oblíbeným tématem úloh matematických soutěží, například matematické olympiády. Existuje velké množství přístupů, jak nerovnosti řešit. Na přednášce si řekneme jak nějaké základní obraty, tak nějaké trikovější. Obsah přednášek lze přizpůsobit podle zájmu. Předběžně se budeme věnovat použití AG-nerovnosti a vážené AG-nerovnosti, Cauchyho nerovnosti, různým substitucím, používání (méně známé) Schurovy nerovnosti, některým trikům (například umocnění nerovnosti) a pravděpodobnostní interpretaci nerovností.

Známé nerovnosti

Značení. Výraz $[n]$ bude značit množinu $\{1, 2, \ldots, n\}$.

Definice.

(i) Aritmetickým průměrem *reálných čísel* x_1, x_2, …, x_n *nazveme výraz*

$$\frac{x_1 + x_2 + \cdots + x_n}{n}.$$

(ii) Geometrickým průměrem *kladných reálných čísel* x_1, x_2, …, x_n *nazveme výraz*

$$\sqrt[n]{x_1 \cdot x_2 \cdots x_n}.$$

Věta. (AG-nerovnost; nejdůležitější ze všech) *Aritmetický průměr kladných reálných čísel je větší roven geometrickému, rovnost nastává, právě když jsou všechna průměrovaná čísla stejná. Jinými (méně) slovy: Pro libovolná* x_1, x_2, …, $x_n > 0$ *platí:*

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdot x_2 \cdots x_n}.$$

Rovnost nastává, právě když $x_1 = x_2 = \cdots = x_n$.

Věta. (mincová nerovnost; Čebyševova nerovnost) *Nechť* $x_1 \geq x_2 \geq \cdots \geq x_n$ *jsou reálná čísla a nechť* y_1, y_2, …, y_n *je nějaké pořadí pevně daných reálných čísel* z_1, z_2, …, z_n. *Potom je výraz* $x_1y_1 + x_2y_2 + \cdots + x_ny_n$ *maximální, právě když je* $y_1 \geq y_2 \geq \cdots \geq y_n$, *a je minimální, právě když je* $y_1 \leq y_2 \leq \cdots \leq y_n$.

Věta. (Cauchyho nerovnost) *Nechť* x_1, x_2, … , x_n, y_1, y_2, … , y_n *jsou reálná čísla. Potom* $(x_1y_1 + x_2y_2 + \cdots + x_ny_n)^2 \leq (x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2)$.

Rovnost nastává právě tehdy, když jsou buď všechna x_i nulová, nebo existuje nějaké reálné r takové, že $y_i = r \cdot x_i$ pro každé $i \in [n]$.

Definice. *Reálná čísla $w_1, w_2, \ldots, w_n$ nazveme* váhami, *právě když jsou všechna kladná a jejich součet je roven jedné.*

Věta. (vážená AG-nerovnost) *Nechť $w_1, w_2, \ldots, w_n$ jsou váhy, nechť $a_1, a_2, \ldots, a_n$ jsou kladná reálná čísla. Potom platí nerovnost*

$$w_1a_1 + w_2a_2 + \cdots + w_na_n \geq a_1^{w_1}a_2^{w_2}\cdots a_n^{w_n}.$$

Definice. *Nechť $w_1, w_2, \ldots, w_n$ jsou váhy, nechť $a_1, a_2, \ldots, a_n$ jsou kladná reálná čísla a nechť $p \in (-\infty; 0) \cup (0; \infty)$.* Váženým mocninným průměrem řádu q čísel $a_1, a_2, \ldots, a_n$ (s vahami $w_1, w_2, \ldots, w_n$) *nazveme výraz*

$$p_q^{w_1,w_2,\ldots,w_n}(a_1, a_2, \ldots, a_n) = (w_1a_1^q + w_2a_2^q + \cdots + w_na_n^q)^{\frac{1}{q}}.$$

V případě, že budou váhy známé, nebudeme je do horního indexu psát. Dále lze definici ještě rozšířit (limitami) na

$$p_0(a_1, a_2, \ldots, a_n) = a_1^{w_1}a_2^{w_2}\cdots a_n^{w_n},$$

$$p_{-\infty} = \min_{i\in[n]} a_i \text{ a } p_\infty = \max_{i\in[n]} a_i.$$

Věta. (nerovnost mezi mocninnými průměry) *Nechť $q, r \in \langle -\infty; \infty\rangle, q < r$, potom pro mocninné průměry z předchozí definice platí nerovnost*

$$p_q(a_1, a_2, \ldots, a_n) \leq p_r(a_1, a_2, \ldots, a_n),$$

rovnost nastává, právě když je $a_1 = a_2 = \cdots = a_n$.

Poznámka. Průměry p_0 a p_1 už známe (geometrický a aritmetický). Průměru p_{-1} se obvykle říká harmonický, průměru p_2 se říká kvadratický. Nerovnostem $p_{-1} < p_0$, $p_0 < p_1$, $p_1 < p_2$ se pak často (po řadě) říká (vážená) HG-nerovnost, AG-nerovnost, AQ-nerovnost.

Věta. (Schurova nerovnost) *Nechť x, y, z jsou kladná čísla a α je reálné číslo. Potom*

$$x^\alpha(x-y)(x-z) + y^\alpha(y-x)(y-z) + z^\alpha(z-x)(z-y) \geq 0.$$

Věta. (Jensenova nerovnost) *Nechť f je ryze konvexní funkce na intervalu $I = \langle a; b\rangle$ (I může být i otevřený či polouzavřený). Nechť $w_1, w_2, \ldots, w_n$ jsou váhy a nechť $x_1, x_2, \ldots, x_n \in I$. Potom platí nerovnost*

$$f(w_1x_1 + w_2x_2 + \cdots + w_nx_n) \leq w_1f(x_1) + w_2f(x_2) + \cdots + w_nf(x_n).$$

Rovnost nastává, právě když $x_1 = x_2 = \cdots = x_n$.

Užitečné postupy

Když máte nerovnost zadanou pro všechna reálná čísla, zkuste se zamyslet, jestli ji nestačí řešit jenom kladná čísla.

U nerovností, ve kterých je n proměnných, zkuste, jestli nejdou dokazovat indukcí.

Zkuste nějaké substituce, například zkuste substituovat jmenovatele zlomku či výraz pod odmocninou.

Občas se hodí vědět, že čísla a, b, c jsou stranami trojúhelníku, právě když existují kladná x, y, z taková, že $a = x + y$, $b = x + z$ a $c = y + z$. Čísla x, y a z lze pomocí a, b, c vyjádřit jako $2x = a + b - c$, $2y = a - b + c$ a $2z = -a + b + c$.

Nerovnost se nazývá homogenní, pokud se po vynásobení kladným reálným číslem nezmění. Například nerovnost $a^2 + b^2 + c^2 \geq ab + ac + bc$ je homogenní. U homogenních nerovností se občas vyplatí předpokládat nějakou podmínku typu $abc = 1$, $a + b + c = 1$ apod. Někdy se naopak vyplatí, pokud je nerovnost zadána s podmínkou $abc = 1$, $a + b + c = 1$ apod. dosadit tuto podmínku vhodně tak, aby vzniklá nerovnost byla homogenní.

Je-li zadána nerovnost v proměnných x_1, x_2, $\ldots$ x_n. Pokud se nerovnost nezmění prohozením libovolných dvou proměnných x_i a x_j, potom lze bez újmy na obecnosti předpokládat, že $x_1 \geq x_2 \geq \cdots \geq x_n$. Pokud se nerovnost změní po prohození některých dvou proměnných, ale nezmění se, když se změní x_i na x_{i+1} (a x_n na x_1), pak lze předpokládat, že x_1 je větší rovno všem ostatním prvkům.

Pokud je nerovnost zadána pro čísla z intervalu $\langle 0, 1\rangle$, potom se může hodit nějaká goniometrická substituce, popř. pravděpodobnostní interpretace.

Příklady

Příklad 1. Dokažte, že pro libovolná x, y, $xy > x + y$ platí

$$\frac{(x-1)(y-1)}{\sqrt{xy - x - y}} \geq 2.$$

Příklad 2. Dokažte, že pro délky a, b, c stran libovolného trojúhelníku platí

$$\frac{(a^2+b^2)c^2 - (a^2-b^2)^2}{abc^2} \leq 2.$$

Příklad 3. Nechť n je přirozené. Dokažte že

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1.$$

Příklad 4. Pro libovolná a, b kladná reálná dokažte nerovnost

$$\left(1+\frac{1}{a}\right)\left(1+\frac{1}{b}\right) \geq \frac{8}{1+ab}.$$

Příklad 5. Nechť x, y, z jsou kladná reálná čísla splňující $x^2+y^2+z^2=1$. Nalezněte minimální možnou hodnotu výrazu

$$\frac{xy}{z}+\frac{yz}{x}+\frac{zx}{y}.$$

Příklad 6. Nechť a, b, c, d jsou kladná reálná čísla, dokažte nerovnost

$$\frac{a}{b+2c+3d}+\frac{b}{c+2d+3a}+\frac{c}{d+2a+3b}+\frac{d}{a+2b+3c} \geq \frac{2}{3}.$$

Příklad 7. Nechť a, b, c jsou strany trojúhelníka. Dokažte, že

$$\frac{a}{b+c-a}+\frac{b}{a+c-b}+\frac{c}{a+b-c} \geq 3.$$

Příklad 8. Nechť x, y, z reálná splňují $x^2+y^2+z^2+2xyz=1$. Dokažte, že pak

$$x^2+y^2+z^2 \geq \frac{3}{4}.$$

Příklad 9. Nechť a_i, b_i jsou pro $i \in [n]$ kladná reálná čísla. Nechť $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$, dokažte, že pak platí

$$\sum_{i=1}^{n} \frac{a_i^2}{a_i+b_i} \geq \frac{1}{2}\sum_{i=1}^{n} a_i.$$

Příklad 10. Pro libovolná reálná a, b dokažte nerovnost

$$\frac{a^4+a^2b^2+b^4}{3} \geq \frac{a^3b+b^3a}{2}.$$

Příklad 11. Dokažte, že pro libovolná čísla a, b, c z intervalu $\langle 0,1\rangle$ platí nerovnost

$$2(a^3+b^3+c^3) \leq 3+a^2b+b^2c+c^2a.$$

Příklad 12. Pro libovolná nezáporná a, b, c dokažte nerovnost

$$a^4+b^4+c^4+a^2bc+b^2ac+c^2ab \geq 2(a^2b^2+a^2c^2+b^2c^2).$$

Příklad 13. Dokažte, že pro libovolná a, b, c kladná platí nerovnost

$$\frac{a^3+b^3+c^3+abc}{2} \geq \frac{a^2b+ab^2+a^2c+ac^2+b^2c+bc^2}{3}.$$

Příklad 14. Dokažte, že pro libovolná a, b, c kladná platí nerovnost

$$a^3b^3+a^3c^3+b^3c^3+3a^2b^2c^2 \geq a^3b^2c+a^3bc^2+a^2b^3c+a^2bc^3+ab^3c^2+ab^2c^3.$$

Příklad 15. Nechť x, y, $z > -1$ a $x+y+z=3$. Dokažte, že platí

$$\frac{x}{x+1}+\frac{y}{y+1}+\frac{z}{z+1} \leq \frac{3}{2}.$$

Příklad 16. Nechť a, b, c jsou kladná reálná čísla taková, že $abc=1$. Dokažte, že platí

$$\frac{1}{1+a+b}+\frac{1}{1+b+c}+\frac{1}{1+c+a} \leq \frac{1}{2+a}+\frac{1}{2+b}+\frac{1}{2+c}.$$

Příklad 17. Nechť x a y jsou kladná reálná čísla taková, že

$$2x+y+\sqrt{8x^2+4xy+32y^2}=3+3\sqrt{2}.$$

Dokažte, že pak $x^2y \leq 1$.

Příklad 18. Nechť a, b a c jsou délky stran trojúhelníka. Dokažte, že platí:

$$\sqrt{a+b-c}+\sqrt{b+c-a}+\sqrt{c+a-b} \leq \sqrt{a}+\sqrt{b}+\sqrt{c}.$$

Příklad 19. Dokažte, že pro libovolná kladná čísla $a_1, a_2, \ldots, a_n$ platí nerovnost

$$(a_1^3+1)(a_2^3+1)\cdots(a_n^3+1) \geq (a_1^2a_2+1)(a_2^2a_3+1)\cdots(a_n^2a_1+1).$$

Příklad 20. Dokažte, že pro libovolné celé $n \geq 3$ a libovolná reálná čísla $x_1 < < x_2 < \cdots < x_n$ platí

$$\frac{n(n-1)}{2}\sum_{i<j} x_ix_j > \left(\sum_{i=1}^{n-1}(n-i)x_i\right)\left(\sum_{j=2}^{n}(j-1)x_j\right).$$

Příklad 21. Dokažte pro a, b, $c > 0$ nerovnost

$$\frac{a}{\sqrt{a^2+8bc}}+\frac{b}{\sqrt{b^2+8ca}}+\frac{c}{\sqrt{c^2+8ab}} \geq 1.$$

Příklad 22. Dokažte, že pro každé kladné reálné číslo x a přirozené n platí

$$\lfloor nx \rfloor \geq \frac{\lfloor x \rfloor}{1}+\frac{\lfloor 2x \rfloor}{2}+\cdots+\frac{\lfloor nx \rfloor}{n}.$$

Příklad 23. Nechť $r_i \in \langle 0;1 \rangle$ pro $i \in [n]$. Dokažte, že pak platí nerovnost

$$(1-(1-r_1)(1-r_2)\cdots(1-r_n))^m+(1-r_1^m)(1-r_2^m)\cdots(1-r_n^m) \geq 1.$$

Burnsideovo lemma

Zuzka Safernová

Jedná se o velice silný nástroj při počítání jistých kombinatorických úloh, které by nám bez znalosti tohoto lemmatu připadaly neřešitelné :-)

Než si povíme, co toto úžasné lemma říká, přiblížíme si pár pojmů:

Definice. Permutace *množiny X je* prosté *zobrazení množiny X* na *X (tzn. žádné dva prvky se nezobrazí na stejný prvek (prosté) a zároveň se na každý prvek něco zobrazí (na).*

Definice. Grupa permutací[23] *v podstatě znamená, že máme množinu, na ní permutace a mezi permutacemi jakožto prvky množiny binární operaci skládání (složit 2 permutace znamená provést je za sebou – POZOR záleží na pořadí – běžně se permutace skládají zprava doleva). Ke každé permutaci existuje permutace k ní inverzní (složením permutace s permutací k ní inverzní dostaneme identitu).*

Definice. (Podgrupa) *Nechť S(X) je grupa permutací na množině X. Pojmem* podgrupa *rozumíme podmnožinu grupy S(X) takovou (označme ji G), která s každou permutací obsahuje i její inverzi a navíc je uzavřená na skládání (tzn. s každými dvěma permutacemi obsahuje i jejich složení – z čehož mimo jiné vyplývá, že obsahuje i identitu).*

Orbita, pevné body

Definujme ekvivalenci[24] $\sim$ na množině X následovně: $x \sim y$, pokud existuje permutace $g \in G$ taková, že $g(x) = y$. Navíc ekvivalence vytváří rozklad množiny na disjunktní bloky ekvivalence (tedy každý prvek množiny leží právě v jednom bloku). Ekvivalence tak sdružuje k sobě prvky stejných vlastností. Není těžké ověřit, že námi definovaná relace je opravdu ekvivalence. Její bloky se nazývají *orbity.* Orbita příslušná prvku x je vlastně množina bodů, kam se můžeme z bodu x dostat pomocí permutací z G. Množinově zapsáno $O_x = \{g(x); g \in G\}$.

Bod x se nazývá **pevným bodem** permutace π, pokud $\pi(x) = x$ (tedy se jedná o body, které permutace π zachová (nepohne s nimi). Množinu všech pevných bodů permutace π budeme značit $X_g = \{x \in X; g(x) = x\}$.

A teď již slíbené lemma:

Lemma. (Burnsideovo) *Působí-li konečná grupa G na konečnou množinu X, pak je počet orbit roven*

$$\frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

[23] Tohoto pojmu netřeba se bát :-)

[24] Ekvivalence je relace na množině A splňující tyto 3 podmínky: $a \sim a$ (*reflexivita*) , $a \sim b \Rightarrow$ $\Rightarrow b \sim a$ (*symetrie*) a pokud $a \sim b, b \sim c$, pak i $a \sim c$ (*tranzitivita*

Možná interpretace: „Počet orbit je roven průměrnému počtu pevných bodů permutací v G.“

Pěkný důkaz je v příspěvku Roberta Šámala: „Burnsideovo lemma aneb kterak náhrdelníky spočítati“. Jestli si ho na přednášce povíme i my, si však ještě rozmyslím :-)

Určitě Tě zajímá, na jaké typy příkladů se dá toto lemma aplikovat. Řešením drtivé většiny úloh bude právě počet orbit při působení grupy symetrií daného objektu na množinu všech obarvení či konfigurací.

Úlohy

Příklad 1. Kolik různých náhrdelníků lze sestavit ze 3 skleněných a 5 dřevěných korálků? Korálky jsou navlečené na šňůrce, takže dva náhrdelníky lišící se jen pootočením, považujeme za shodné. Jak se výsledek změní, budeme-li moci náhrdelník i převracet?

Příklad 2. Kolik náhrdelníků lze sestavit z k skleněných a $8 - k$ dřevěných korálků?

Příklad 3. Kolika způsoby lze obarvit políčka šachovnice

(1) 3×3
(2) 4×4
(3) $n \times n$

dvěma barvami? Dvě obarvení považujeme za stejná, pokud lze dostat jedno z druhého pootočením šachovnice.

Příklad 4. Řešte předchozí úlohu za předpokladu, že je šachovnice skleněná (sklo je průhledné, šachovnice se teď dá i překlápět).

Příklad 5.

(1) Dětská šachovnice obsahuje 3 červené, 3 modré a 3 zelené čtvercové destičky. Kolika způsoby je lze sestavit do velkého čtverce 3×3?
(2) Jak se změní výsledek, pokud je možné dílky pevně spojovat?

Příklad 6. Kolika způsoby lze obarvit stěny krychle

(1) 2 barvami?
(2) k barvami? Dvě obarvení považujeme za totožná, pokud lze jedno dostat z druhého otočením krychle.

Příklad 7. Kolika způsoby lze na stěny krychle umístit čísla 1–6? Kolika způsoby to lze udělat tak, aby byl součet protilehlých čísel 7?

Příklad 8. Kolika způsoby lze obarvit stěny čtyřstěnu

(1) 2 barvami?
(2) k barvami?

Dvě obarvení považujeme za totožná, pokud lze jedno dostat z druhého otočením čtyřstěnu. Co se stane, pokud budeme uvažovat všechny symetrie čtyřstěnu?

Úlohy jsou čerpány ze sbírky „Příklady z algebry“, kterou sepsal David Stanovský.

Zdroje

Robert Šámal: Burnsideovo lemma aneb kterak náhrdelníky spočítati
David Stanovský: Příklady z algebry

Konečné součty

Pavel Šalom

V zásadě existují dva typy součtů – konečné a nekonečné. Těmi nekonečnými se zabývat nebudeme, protože je k jejich výpočtu potřeba znát a umět pracovat s limitou. Přesto se však i při jejich zkoumání uplatňují někdy podobné metody, jaké si ukážeme při výpočtech konečných součtů. Dá se říci, že i konečné součty můžeme rozdělit na dva typy, a to takové, které jsme schopni vždy standardními metodami spočítat a takové, pro něž neexistuje jednoznačný recept. Potom nezbývá, než zkoušet vše možné i nemožné, přemýšlet, bloumat, lámat tužky a někdy si raději nechat poradit :)

Mezi první typ součtu patří například dobře známá aritmetická či geometrická posloupnost. Dále k nim patří součty $S_k = 1^k + 2^k + \cdots + n^k$. Dokonce jsme schopni vždy spočítat každou sumu, jejíž i-tý člen je vyjádřený jako polynom v proměnné i. Kromě tohoto typu součtů zde patří ještě takové, které si nazveme aritmeticko-geometrické. Mezi ně patří například součet $q + 2q^2 + 3q^3 + \cdots + nq^n$, což je jakási smíchanina aritmetické a geometrické řady. Jeden z nejobecnějších součtů, které jsme schopni vždy spočítat má tvar

$$\sum_{i=1}^{n} P(i)q^i$$

kde $q \in R$, $P(i)$ je daný polynom libovolného stupně. Další typ součtu, který ještě jsme schopni rozumně spočítat, je tvaru

$$\sum_{i=0}^{n} P(i)\binom{n}{i}$$

Existuje ještě několik dalších typů, u nichž jsme schopni obecné metody popsat, ale určitě tě samotného napadne další spousta, u nichž opravdu nejsme schopni najít žádné pěkné vyjádření, natož obecné postupy, přestože se součet samotný tváří velmi jednoduše. Například zkus $\sum_{k=1}^{n} \frac{1}{k}$ nebo $\sum_{k=1}^{n} \frac{1}{k^2}$. Jiná je situace při sčítání kombinatorických čísel, kde je sice známo mnoho identit, avšak podat obecnou metodu je téměř nemožné.

Nyní již k samotným výpočtům. Obecně uplatnitelné metody jsou

(i) Představit si daný součet v obráceném pořadí – aritmetická řada
(ii) Vhodně daný součet vynásobit – geometrická řada.
(iii) Tušit, v jakém tvaru by výsledek mohl vyjít, případně použít metodu neurčitých koeficientů a výsledek dokázat indukcí :)
(iv) Využít extrémně chytrých identit – součty S_k.

(v) Pokusit se každý člen vyjádřit jako rozdíl dvou podobně vypadajících členů například metodou rozkladu na parciální zlomky.
(vi) Zkusit odhadnout součet integrálem a poté se zabývat chybou.
(vii) Vhodné použití derivací.

Při počítání kombinatorických součtů se často využívá jiných postupů:

(vi) Pascalův trojúhelník.
(vii) Binomická věta.
(viii) Vytvořující funkce.
(ix) Komplexní čísla a Moivreova věta – nejen pro kombinatorické součty, ale třeba i součty $\sum_{k=1}^{n} \sin(k\alpha)$, $\sum_{k=1}^{n} \cos(k\alpha)$, atd.
(x) Kombinatorická interpretace.

Metody i-v bychom si měli na přednášce ukázat a osvojit, další podle času.

Tvrzení. Pro polynomy $P(x)$, $Q(x)$ nastává rovnost $P(x) = Q(x)$ právě když se rovnají příslušné koeficienty u jednotlivých mocnin.

Tvrzení. Pro libovolná A, B reálná (i komplexní) je

$$A^n - B^n = (A - B)(A^{n-1} + A^{n-2}B + \cdots + AB^{n-2} + B^{n-1})$$

Věta. (Binomická) *Pro libovolná A, B reálná (i komplexní) je*

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

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

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Tvrzení. Buď $S_k(n) = \sum_{i=1}^{n} i^k$. Potom platí

$$S_{k+1}(n+1) - 1 = \sum_{i=0}^{k+1} \binom{k+1}{i} S_i(n)$$

Tvrzení. Buď $R_k = \sum_{i=1}^{n} i^k q^i$ pro nějaká n, $q \neq 1$ (případ $q = 1$ je obsažen v předchozím tvrzení). Potom platí

$$R_k = \frac{1}{q-1}\left[n^k q^{n+1} + \sum_{i=0}^{k-1} (-1)^{k-i} \binom{k}{i} R_i\right]$$

Věta. *Buď $P(x)$ polynom stupně m. Pak existuje polynom $Q(x)$ stupně $m+1$ takový, že pro všechna n platí*

$$\sum_{i=1}^{n} P(i) = Q(n)$$

Věta. *Buď $P(x)$ polynom stupně m, $q \neq 1$ (případ $q = 1$ je v předchozí větě). Pak existuje polynom $Q(x)$ stupně m a číslo d takové, že pro všechna n platí*

$$\sum_{i=1}^{n} P(i)q^i = d + Q(n)q^n$$

Příklady

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

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

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

Příklad 4. $S = 1\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n}$

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. $S = \binom{m}{m} + \binom{m+1}{m} + \cdots + \cdots + \binom{m+n-1}{m}$

Příklad 8. Těžké $\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}$, resp. $\binom{n}{0}\binom{m}{p} + \binom{n}{1}\binom{m}{p-1} + \cdots + \binom{n}{p}\binom{m}{0} = \binom{m+n}{p}$

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

Příklad 10. $S = 1\cdot 2\cdot\ldots\cdot k + 2\cdot 3\cdot\ldots\cdot(k+1) + \cdots + (n+1)\cdot(n+2)\cdot\ldots\cdot(n+k-1)$

Příklad 11. Určete $R_1 = 1q + 2q^2 + 3q^3 + \cdots + nq^n$

Příklad 12. Určete $R_2 = 1^2q + 2^2q^2 + 3^2q^3 + \cdots + n^2q^n$

Příklad 13. $S = \frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)}$

Příklad 14. $S = \frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \cdots + \frac{1}{n(n+1)(n+2)}$

Příklad 15. $S = \frac{1}{1\cdot 3\cdot 5} + \frac{2}{3\cdot 5\cdot 7} + \cdots + \frac{n}{(2n-1)(2n+1)(2n+3)}$

Příklad 16.

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

Příklad 17. Těžké $\binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \cdots = 2^{n-2} + (\sqrt{2})^{n-2} \sin(\frac{n\pi}{4})$

Příklad 18. Těžké $\binom{n}{0} + \binom{n}{6} + \binom{n}{12} + \cdots = \frac{1}{3}\left[2^{n-1} + \cos(\frac{n\pi}{3} + (\sqrt{3})^n \cos(\frac{n\pi}{6})\right]$

Příklad 19. Těžké

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

Příklad 20. Těžké

$$\sum_{k=0}^{n} \cos(\varphi + k\alpha) = \frac{\sin\frac{(n+1)\alpha}{2} \cos\left(\varphi + \frac{n\alpha}{2}\right)}{\sin\frac{\alpha}{2}}$$

Příklad 21. Těžké

$$\sum_{k=1}^{n} k\cos(k\alpha)$$

Příklad 22. Těžké ($x \neq 0$)

$$\sum_{k=0}^{n} ke^{kx} = \frac{e^x - (n+1)e^{(n+1)x} + ne^{(n+2)x}}{(1-e^x)^2}$$

Příklad 23. Těžké

$$\sum_{k=0}^{2n} (-1)^k \binom{2n}{k} k^n = 0$$

Kombinatorická geometrie

Martin Tancer

Na přednášce budeme řešit úlohy z kombinatorické geometrie. Nebude se jednat o přednášku, která by vykládala nějakou ucelenou teorii, spíš si ukážeme si nějaké užitečné postupy, jak úlohy z kombinatorické geometrie řešit.

Pomocné věty

Věta. (Hellyho věta – verze pro rovinu) *V rovině jsou dány konvexní množiny K_1, K_2, ... , K_n pro $n \geq 3$. Navíc platí, že každé tři z těchto množin mají neprázdný průnik. Potom už nutně všechny mají neprázdný průnik.*

Věta. (Hellyho věta – obecná verze) *V $\mathbb{R}^d$ jsou dány konvexní množiny K_1, K_2, ... , K_n pro $n \geq d+1$. Navíc platí, že každých $d+1$ z těchto množin má neprázdný průnik. Potom už nutně všechny mají neprázdný průnik.*

Příklady

Příklad 1. Uvnitř rovnostranného trojúhelníku o straně 1 je dáno deset různých bodů. Dokažte, že mezi těmito body existují dva různé body takové, že jejich vzdálenost je nejvýše $\frac{1}{3}$.

Příklad 2. Vnitřní prostory muzea tvoří (ne nutně konvexní) mnohoúhelník s n vrcholy. Dokažte, že lze do muzea umístit nejvýše $\frac{n}{3}$ hlídačů tak, že ohlídají celé muzeum.

Příklad 3. Určete, kolik nejvýše bodů lze umístit v rovině tak, aby žádné tři neležely na společné přímce a aby každý úhel tvořený trojicí těchto bodů byl nejvýše 119°.

Příklad 4. Rozhodněte, zda je možné v rovině umístit 13 bodů tak, aby žádné tři neležely na společné přímce a aby každý úhel tvořený trojicí těchto bodů byl nejvýše 150°.

Příklad 5. V rovině je dáno 100 bodů, žádné tři neleží na přímce. Uvažujme všechny trojúhelníky, jejichž vrcholy jsou některé tři z daných bodů. Dokažte, že nejvýše 70% uvažovaných trojúhelníků je ostroúhlých.

Příklad 6. Je dána konečná množina bodů v rovině taková, že každé 3 body určují tupoúhlý trojúhelník. Dokažte, že lze k této množině přidat bod, aby tato vlastnost zůstala zachována. Platí analogické tvrzení i pro nekonečné množiny?

Příklad 7. Na přímce je dáno 50 úseček, dokažte, že platí alespoň jedno z následujících tvrzení:

(i) Existuje 8 úseček se společným bodem.
(ii) Existuje 8 úseček, z nichž každé dvě jsou disjunktní.

Příklad 8. V rovině je dáno $n \geq 3$ navzájem rovnoběžných úseček. Pro každé tři existuje přímka, která je protíná. Dokažte, že existuje přímka protínající všechny tyto úsečky.

Příklad 9. Konečná množina M bodů v rovině má takovou vlastnost, že libovolné tři body z ní lze pokrýt kruhem o poloměru 1. Dokažte, že celou množinu M lze pokrýt kruhem o průměru 1.

Příklad 10. Je dáno n bodu v rovině, každé dva body mají vzdálenost nejvýše 1. Určete maximální možný počet úseček tvořených těmito body, které mají délku přesně 1.

Příklad 11. V prostoru je dána kartézská soustava souřadnic. Každý bod s celočíselnými souřadnicemi nazveme mřížovým. Obarvěme 2000 mřížových bodů modře a jiných 2000 mřížových bodů červeně tak, aby žádné dvě modročervené úsečky neměly společný vnitřní bod (modročervená úsečka je taková úsečka, že má jeden krajní bod modrý a druhý červený). Uvažujme nejmenší kvádr s hranami rovnoběžnými s osami souřadnic, který obsahuje všechny obarvené body.

(i) Dokažte, že kvádr obsahuje alespoň 500 000 mřížových bodů.
(ii) Udejte příklad popsaného zobrazení, kdy uvažovaný kvádr obsahuje nejvýše 8 000 000 bodů.

Příklad 12. V rovině je dán pravoúhlý trojúhelník ABC, označme c délku přepony ABC. V tomto trojúhelníku je dána konečná množina S. Dokažte, že je možné body množiny S uspořádat do posloupnosti $X_1, X_2, \ldots, X_n$ tak, že

$$|X_1X_2|^2 + |X_2X_3|^2 + \cdots + |X_{n-1}X_n|^2 \leq c^2.$$

Příklad 13. V rovině je daných deset různých bodů s následující vlastností: mezi každými pěti z nich lze vybrat čtyři takové, které tvoří tětivový čtyřúhelník. Kolik nejméně z těchto bodů musí ležet na jedné kružnici?

Příklad 14. Nechť $n \geq 4$ a nechť M je konečná množina n bodů v prostoru. Předpokládejme, že tyto body jsou obarveny černě či bíle tak, že každá sféra[25], která protíná M v alespoň čtyřech bodech obsahuje stejný počet černých a bílých bodů. Dokažte, že všechny body z M leží na společné sféře.

[25] Sféra je povrch koule.

Obsah