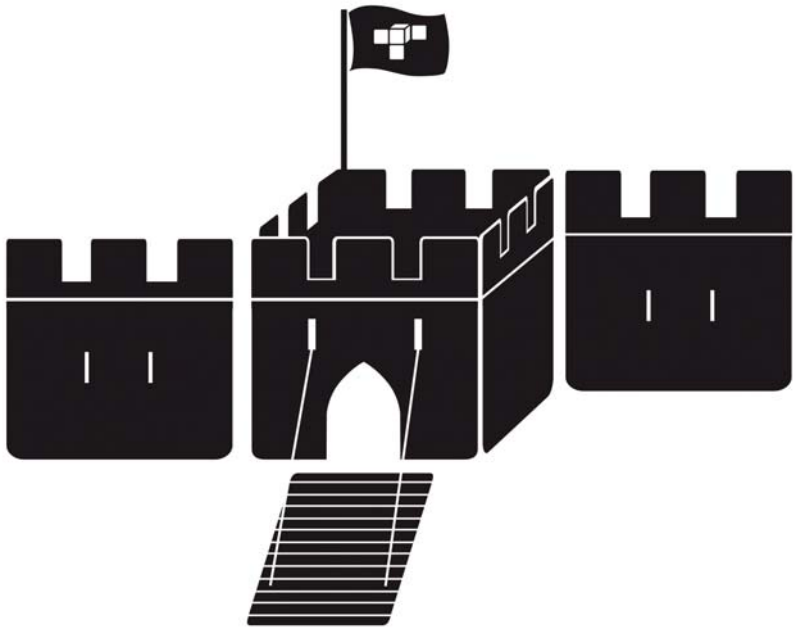


Sborník přednášek

soustředění Pikomatu MFF UK
16.–22. 4. 2016, Kunžak

Vývoj počítání

Tereza Ptáčková

Velmi zajímavou součástí historie je i vývoj matematického počítání. Začneme s Egyptem a s Mezopotámií, kde se matematika rozvíjela před spoustou a spoustou let. Potom se podíváme do antiky, do Řecka a Říma, kde se zrodila matematika, jak ji známe dnes – logická výstavba pomocí axiomů a odvozování. Povíme si, jakými krizemi si matematika prošla. Pak se podíváme do středověku, kde si zkusíme počítat pomocí algoritmů, které se tehdy učili studenti vysokých škol.

Prozradíme si pár zajímavostí, třeba odkdy se píší čísla na složenku slovy, nebo proč je 0 jedno z nejkontroverznějších čísel matematiky, nebo proč jsou hodiny na následujícím obrázku zvláštní.

Zdroj: http://www.bellarose.cz/dekorace/nastenne-hodiny-antik-cream-41-cm/

Teorie informace

František Steinhauser

Na přednášce si řekneme, co je bit, jak ho používat, a proč je toto použití nejefektivnější.

Příklad. *Kolik bitů (otázek) je nutných k rozlišení osmi různých možností?*

Někdy mají různé možnosti různé pravděpodobnosti a nás zajímá průměrný počet otázek (bitů), který chceme co nejmenší. K tomu použijeme tzv. Huffmanovo kódování.

Pokud vyjde čas, zopakujeme si základní operace s bity a rozšíříme jejich další používání.

Příklad. *Jak prohodit dvě osmice bitů bez použití další paměti?*

Sylvestrův problém

Jan Hamáček

V potravinovém řetězci prodávají kuřecí kousky. Malé menu obsahuje 6 kuřecích kousků. Střední menu jich obsahuje 9. Velké menu obsahuje 20 kuřecích kousků. Žádné jiné množství kousků objednat nejde. Kdybych si chtěl koupit 71 kousků, koupil bych například sedmkrát malé menu, jednou střední menu a jednou velké menu.

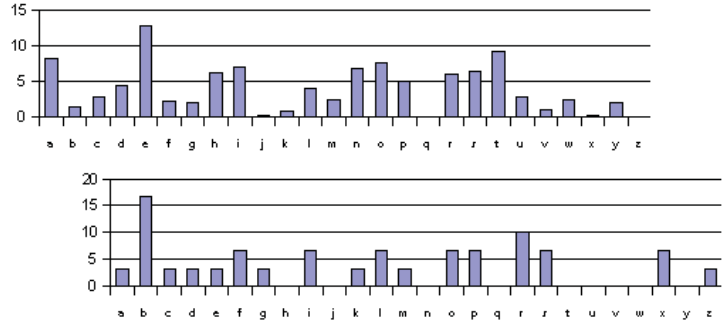
Kdybych byl vybíravý zákazník a chtěl za každou cenu koupit třeba 22 kousků, neuspěl bych. Dokázali byste popsat počty kousků, které si nemůžeme koupit? Jaký počet je největší? Mohli bychom hledat řešení tak, že si vypíšeme všechny možnosti. Takový způsob by byl hodně pracný a nezajímavý. Co kdyby navíc potravinový řetězec změnil počty kousků v nabídce?

Podíváme se proto na přednášce na obecný způsob, jak takové problémy řešit. Při hledání se dotkneme hned několika oblastí matematiky. Potkáme kousky kombinatoriky, pár grafů a možná i trochu dělitelnosti. Nebudu ale na přednášce předpokládat, že byste tyto části matematiky předem znali. Všechno, co budeme používat, pečlivě vysvětlím.

Historické šifry

František Steinhauser

Na přednášce projdeme historické šifry, konkrétně Caesarovu, Vigenerovu a obecnou substituční. U každé vysvětlíme, jak funguje a jak by se na ni útočilo. Potom popíšeme útoky pomocí frekvenční analýzy. Pokud to stihneme, projdeme i šifry založené na změnách pořadí písmen.



Zdroj: http://jaybee.cz/software/caesaruv-koder/

Příklad. *Kolik možností hesla má Ceasarova šifra?*

Příklad. *Kolik možností hesla má Vigenerova šifra s heslem délky 5?*

Gravitační vlny

Vít Strádal

První přímé pozorování gravitačních vln proběhlo 14. září 2015 v detektoru LIGO označované jako GW150914. Co to gravitační vlna je, jak se projevuje a co se vlastně pozorovalo, se dozvíte na přednášce.

Tětivové čtyřúhelníky

Václav Steinhauser

Tato přednáška je pokračováním přednášky o úhlení, a ukážeme si, že pomocí tětivových čtyřúhelníků jde vyřešit skoro každá středoškolská geometrická úloha. Jestli o nich někdo nikdy neslyšel, doporučuji napřed absolvovat přednášku o úhlení.

Úhlení

Václav Steinhauser

Na přednášce si ukážeme, že taková zbytečně vypadající věc jako jsou úhly je ve skutečnosti nejsilnější geometrická technika vůbec. Na téhle přednášce nechci probírat nic těžkého, ale raději ukázat, jak se k úloze stavět a něco si pomocí úhlů dopočítat. Přednáška je vhodná pro někoho, kdo se s úhlením nikdy pořádně nesetkal, a někdo, kdo chápe obě následující tvrzení se tady bude hodně nudit a bavit ho bude až navazující přednáška o tětivových čtyřúhelnících.

Tvrzení. (charakteristika tětivových čtyřúhelníků)
Nechť $ABCD$ je konvexní čtyřúhelník. Pak následující tvrzení jsou ekvivalentní:
(i) $ABCD$ je tětivový (jde mu opsat kružnice).
(ii) $|\sphericalangle ACB| = |\sphericalangle ADB|$.
(iii) $|\sphericalangle ABC| + |\sphericalangle ADC| = 180^\circ$.

Tvrzení. (úsekový úhel)
Nechť $ABCD$ je čtyřúhelník vepsaný do kružnice k a p přímka procházející bodem A. Na přímce p zvolme bod X tak, aby úhel XAB byl ostrý. Pak platí, že p je tečna kružnice k, právě když $|\sphericalangle XAB| = |\sphericalangle ACB|$.

Dobré rady při řešení geometrických úloh:
(i) Určete, které úhly jsou v úloze důležité.
(ii) Rozmyslete si, jaké další úhly lze pomocí těchto úhlů vyjádřit.
(iii) Postupujte odpředu („Vím, že …“) i odzadu („Stačilo by mi …“).
(iv) Velký obrázek (fakt je to na něm lépe vidět).

Zajímavé matematické úlohy

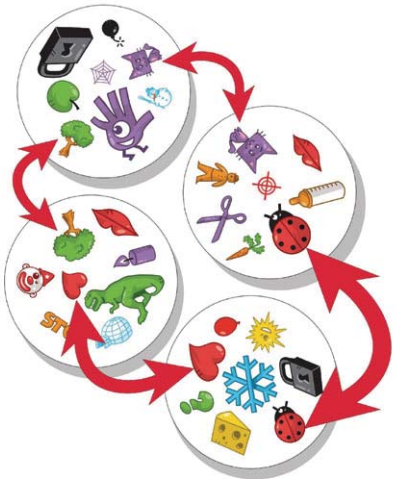
Barbora Šmídová

Vydáme se na ostrov, kde všichni mluví vždy pravdu, nebo vždy lžou, zachráníme pár odsouzených před smrtí, necháme se překvapit rozdělováním výdělku za práci a na závěr si trochu zacestujeme. A to vše díky matematickým problémům, ke kterým nepotřebujeme kalkulačku ani znalost náročných matematických operací, použijeme pouze logické uvažování, tužku a papír.

Dobble – proč a jak to funguje?

Zbyněk Pawlas

Dobble je oblíbená karetní hra, ve které každá dvojice karet obsahuje právě jeden společný symbol, který je potřeba co nejrychleji najít. Jak autoři dosáhli toho, že to skutečně funguje? To znamená, že se nenajde dvojice karet, která by neměla žádný nebo měla více než jeden společný symbol. Funkční balíček karet má zajímavou matematickou strukturu. Můžeme si ho sami sestrojit pomocí tzv. konečné projektivní roviny. Základy pro studium tohoto objektu sahají k renesančním malířům, kteří se snažili vyvinout techniky pro zachycení perspektivy.



Zdroj: http://dobble.cz/images/

Analytická geometrie I a II

Petra Zahajská

Napadlo vás někdy, že geometrie nemusí být jen o pravítku a kružítku, ostře ořezané tužce a rýsování? Je to tak! Máme přeci ještě analytickou geometrii, která pracuje s geometrickými objekty v kartézské souřadné soustavě. Vše, co se nám do soustavy vejde, můžeme spočítat, popsat pomocí rovnic, vektorů, bodů a dokonce to nemusíme ani malovat. Stačí nám jen souřadnice bodů na to, abychom odhalili, zda body tvoří trojúhelník, a když se všechno tohle naučíme, můžeme popisovat rovnicí nejen přímku, ale i elipsu, parabolu, hyperbolu nebo kružnici. Můžeme na nich hledat body, dělat tečny, sečny a další psí kusy.

Příklad. *Body* $A[1;3], B[4;1]$ *určují vektor* u*, tj.* $u = B - A$.

1. *Vypočítejte souřadnice vektoru* u.
2. *V soustavě souřadnic znázorněte body* A, B*, potom nakreslete alespoň tři orientované úsečky, které jsou umístěním vektoru* u.
3. *Vypočítejte souřadnice bodu* X *tak, aby orientovaná úsečka* CX*, kde je* $C[-3;-2]$*, též určovala vektor* u.
4. *Vektor* u_1 *je opačný vektor k vektoru* u*. Vypočítejte souřadnice vektoru* u_1*. Nakreslete orientované úsečky* OU, OU_1*, které jsou umístěním vektorů* u *a* u_1 *s počátečním bodem* $O[0;0]$.

Příklad. *Dokažte, že dané vektory* u, v *jsou kolmé:* $u = (2;4), v = (-3;\frac{3}{2})$.

Příklad. *Vypočítejte velikost daného vektoru* $u = (-4;2)$.

Catalanova čísla

Tereza Ptáčková

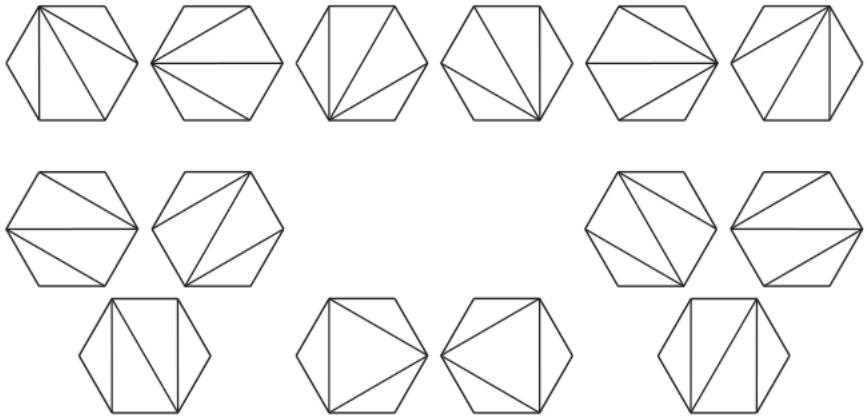
Catalanova čísla jsou velmi zajímavá čísla, která jsou známá hlavně díky svým aplikacím v kombinatorických úlohách. Vychází z nich plno zajímavých úloh, které si přiblížíme na přednášce. Catalanova čísla nám například udávají počet správných uzávorkování výrazu, nebo různých triangulací konvexního n-úhelníka.

Příklad. *Před pokladnou, kde se prodávají vstupenky za* 5 *Kč, stojí fronta tvořená* $m + n$ *osobami. Přesně* n *z nich má* 5 *Kč, zbylých* m *má* 10 *Kč. Prodavačka má* a *pětikorun. Jestliže je pořadí lidí ve frontě náhodné, kolik z možných uspořádání fronty „projde“? (Fronta „projde“, pokud prodavačka může všem lidem s* 10 *Kč vrátit* 5 *Kč.)*

Příklad. *Mějme mřížku* $n \times n$*. Kolik existuje cest z bodu* $[0;0]$ *do* $[n;n]$ *takových, že cesta nikdy neprotne diagonálu, když můžeme jít pouze nahoru nebo doprava?*

Příklad. *Kolika způsoby lze za pomocí* $2n$ *závorek uzávorkovat součin* $x_0 \cdot x_1 \cdot \ldots \cdot x_n$ *tak, aby bylo pořadí násobení jednoznačně určené?*

Příklad. *Mějme pravidelný* n*-úhelník. Kolika způsoby můžeme provést triangulaci* n*-úhelníka za pomocí jeho úhlopříček tak, aby se žádné dvě úhlopříčky nekřížily?*



Diofantické rovnice

Tereza Ptáčková

Diofantické rovnice jsou rovnice s více neznámými, které se řeší v oboru celých čísel. Jinými slovy: máme rovnici a zajímají nás pouze celočíselná řešení. Takovéhle úlohy se vyskytují v různých olympiádách a matematických soutěžích, tak je pojďme společně prozkoumat. Na přednášce se naučíme takové rovnice řešit, zároveň se naučíme snadno a rychle poznávat, kdy takové rovnice řešení nemají. Ukážeme si, jak k řešení využít dělitelnost čísel, a pokud nám zbyde čas, podíváme se i na řešení diofantických rovnic za pomocí řetězových zlomků.

Příklad. *Najděte všechna celočíselná řešení rovnice* $18x + 25y = 1$.

Příklad. *Najděte všechna celočíselná řešení rovnice* $18x + 25y = 10$.

Příklad. *Najděte všechna celočíselná řešení rovnice* $18x + 24y = 10$.

Příklad. *Najděte všechna celočíselná řešení rovnice* $18x + 25y = 12$.

Příklad. *Tři rybáři společně ulovili určité množství ryb a ulehli ke spánku. První se vzbudil jeden z nich a chtěl si odnést svůj podíl. Počet ryb ale nebyl dělitelný třemi, proto jednu rybu pustil zpět do vody. Vzal si třetinu zbývajícího počtu a odešel. Když se vzbudil druhý rybář, situace se opakovala. Jednu rybu pustil, vzal si třetinu a odešel. Totéž udělal třetí rybář. Kolik bylo ryb celkem?*

Kompresní algoritmy

Jan Hamáček

Na přednášce si ukážeme algoritmy používané při kompresi dat v počítači. Budeme si povídat o algoritmech bezztrátové komprese. Takové algoritmy se používají, pokud potřebujeme zkomprimovaná data rozbalit zpět do nezměněné původní podoby.

Algoritmy, o kterých budeme mluvit, se používají například při archivování formátů metodou zip, nebo při ukládání obrázků gif. I bez počítače si ale ukážeme, jak některé z algoritmů použít pro zakódování textu.

Tabulka 1: Tabulka četností znaků zbavených diakritiky v českém jazyce

a – 8,4 %	g – 0,3 %	l – 3,8 %	r – 4,9970 %	x – 0,076 %
b – 1,6 %	h – 1,8 %	m – 3,2 %	s – 5,3160 %	y – 3,0 %
c – 2,5 %	ch – 1,2 %	n – 6,6 %	t – 5,7 %	z – 3,1 %
d – 3,6 %	i – 7,6 %	o – 8,7 %	u – 3,9 %	
e – 10,7 %	j – 2,1 %	p – 3,4 %	v – 4,6 %	
f – 0,2 %	k – 3,7 %	q – 0,0013 %	w – 0,009 %	

Příklad. *Sestrojte optimální prefixový strom a zkomprimujte pomocí něj do binární abecedy (tedy pouze pomocí znaků* 0 *a* 1*) větu „Rytířova dcera běhá po zahradě bosá“. Diakritiku vynechte.*

Příklad. *Jsou dány body* $A[1;1]$, $B[2;-1]$ *a* $C[3;2]$.

1. *Dokažte, že body* A, B *a* C *jsou vrcholy trojúhelníku.*
2. *Vypočítejte délky stran trojúhelníku* ABC.
3. *Vypočítejte vzdálenost těžiště* T *trojúhelníku* ABC *od vrcholu* C.

Příklad. *Přímka* p *je dána obecnou rovnicí* $2x + 5y - 6 = 0$.

1. *Vyjádřete přímku* p *parametrickými rovnicemi.*
2. *Napište rovnici přímky* p *ve směrnicovém tvaru.*

Axiom, definice, věta, důkaz

Vít Strádal

Matematika je jediný z oborů, který je obdařen darem, že když něco tvrdí, tak je to opravdu pravda. Když je něco dokázáno v matematice, je to na 100 %.

Jenže na základě čeho je věta dokázána? Na základě dalších vět s použitím dříve uvedených definic. Ale to přeci nemůže fungovat do nekonečna!

Ano, matematici chytře zvolili systém axiomů, tedy vět, které se již nedokazují. A jak tedy vědí, že jsou pravdivé, když je nikdo nedokazuje? A v tom je právě to tajemství matematiky: to matematika nezajímá, jestli jsou axiomy pravdivé, nebo ne. Matematické věty mají v sobě skryto „Pokud platí vybrané axiomy, tak platí následující věta“. Trochu to připomíná smlouvu z pojišťovny, kde je drobným téměř nečitelným písmem poznamenáno, na co všechno se pojištění nevztahuje.

To ovšem umožňuje matematikovi zkoumat, co by se stalo, kdyby si vzal axiomy jiné, které by byly ve sporu s těmi běžnými. Pak velmi pravděpodobně dojde k rozdílným závěrům. A tak samozřejmě matematici pěstují rozbujelý les matematických teorií, kde každý strom má kořeny v jiné sadě axiomů.

Tohle všechno má ještě jednu výhodu. Pokud někdo přijde s úplně neznámou strukturou a podaří se mu jen ukázat, že splňuje nějakou známou sadu axiomů, okamžitě dostane i základní sadu vět z těchto axiomů dokazatelných.

Úvod do šifrovacích mechanismů

František Steinhauser

Rozebereme, jak se liší symetrický a asymetrický kryptosystém (šifra). Jak může vypadat bloková a jak proudová šifra a jaké základní vlastnosti by měly mít.

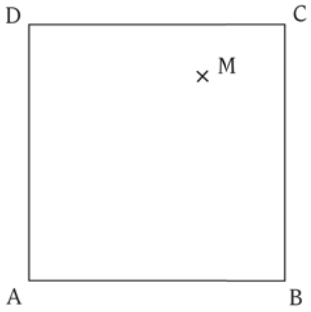
Dále popíšeme myšlenku, jak fungují asymetrické šifry, a ukážeme si jak se tato myšlenka konkretizuje na známém šifrovacím algoritmu RSA.

Rotační úlohy

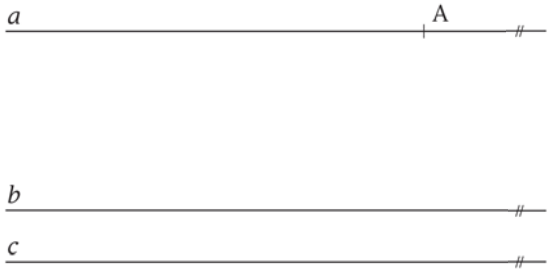
Jiří Erhart

Už jste slyšeli o rotacích? Ačkoliv se tato geometrická zobrazení ne vždy vejdou do osnov základní školy, umožňují řešit zajímavou množinu konstrukčních úloh. Úloh, které většinou zní velmi jednoduše, ale bez rotací bychom si na nich vylámali zuby. Pokud se tedy nebojíte kružítka s pravítkem, přijďte si rozšířit své geometrické obzory.

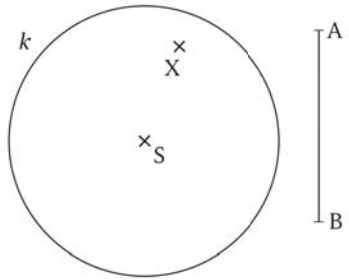
Příklad. *Dorýsujte do čtverce* ABCD *rovnostranný trojúhelník* KLM *tak, že vrcholy* K *a* L *budou ležet na obvodu čtverce.*



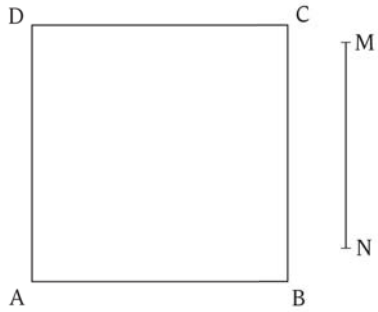
Příklad. *Dorýsujte do obrázku rovnostranný trojúhelník* ABC *tak, že bod* B *bude ležet na přímce* b *a bod* C *na přímce* c.



Příklad. *Dorýsujte do obrázku tětivu kružnice* k *délky* |AB| *procházející bodem* X.



Příklad. *Vepište čtverci* ABCD *čtverec o délce hrany* |MN|.



Množina jako základ všeho

Jan Hamáček

Na začátku této přednášky vás poprosím, abyste zapomněli všechno, co jste se doteď o matematice naučili. Intuitivně si představíme, co je to množina, ukážeme si pár jednoduchých příkladů množin a pustíme se do popisu matematického světa pouze pomocí množin.

Skutečně nepoužijeme nic jiného než množiny. Tak třeba číslo 0 bude v našem množinovém světě matematiky reprezentováno jako prázdná množina. Povídání o dalších číslech a jejich sčítání bude potřebovat hodně abstraktního přemýšlení. Třeba už číslo 1 bude množina obsahující prázdnou množinu.

Pomocí množin tak vybudujeme přirozená čísla, ukážeme si, jak je sčítat, porovnávat a jak pomocí zobrazení (funkce) poznat, že jsou dvě množiny stejně velké.