Studentský matematicko-fyzikální časopis

M&M

Ročník XIX / Číslo 3

Úvodník – str. 2 • Zadání úloh třetí série – str. 2 a 25
Téma 2: Měření rychlostí – str. 4 • Téma 3: Konečné automaty – str. 7
Řešení úloh první série – str. 8
Karel Ullwer: O vzorci pro řešení kvadratických rovnic – str. 16
Elektronické podpisy – str. 20

Časopis M&M a stejnojmenný korespondenční seminář je určen pro studenty středních škol, kteří se zajímají o matematiku, fyziku či informatiku. Během školního roku dostávají řešitelé zdarma čísla se zadáním úloh a témat k přemýšlení. Svá řešení odesílají k nám do redakce. My jejich příspěvky opravíme, obodujeme a pošleme zpět. Nejzajímavější řešení otiskujeme.

Milí řešitelé,

pomalu se blíží Vánoce a poslední dny kalendářního roku. Školní rok ale zdaleka nekončí, a tak vám můžeme nabídnout další číslo našeho časopisu.

Najdete v něm tradičně zadání čtyř úloh a příspěvky k tématům. Můžete se také podívat, jak se měly řešit úlohy z prvního čísla a jak jste v jejich řešení obstáli v porovnání s jinými řešiteli. Navíc pro vás máme hned dva články. Jeden je organizátorský a pojednává o tom, jak funguje elektronický podpis. Za druhý děkujeme Karlu Ullwerovi, který se zabýval různými odvozeními vzorce pro výpočet řešení kvadratické rovnice.

Na jaře budeme pro přibližně 20 nejlepších řešitelů pořádat jako obvykle soustředění. Tentokrát se bude konat 18.–26. května na Vysočině. Pokud byste se chtěli zúčastnit, rezervujte si volné místo v kalendáři. Hlavně ale pilně řešte, ať jste mezi vybranými.

Pěkné prožití vánočních svátků přejí

organizátoři

Zadání úloh

Termín odeslání třetí série: 14. 1. 2013

Byla jednou jedna země a v té zemi hrad. *Zdejšímu lidu moudře vládl* župan *a místní lidé se vcelku pochopitelně starali o svůj* vrt *a snažili se v rámci zdejší společnosti mít co možná největší* kořist. *Na větších ulicích tu běžně měřívají jejich* chytrost *a zajímavý je také zdejší způsob bydlení, neboť obyvatelé zde povětšinou* stanují *v* chýších.

Úloha 3.1 – Stěhování (2b)

Osm lidí se chce přestěhovat tak, že si cyklicky vymění své byty – tj. první člověk se přestěhuje do bytu druhého člověka, druhý do bytu třetího a tak dále, až osmý člověk se přestěhuje do bytu prvního. Pro stěhování přitom platí tato pravidla:

(i) stěhování znamená, že si dva lidé vymění své byty,
(ii) každý se může stěhovat jen jednou denně.

Je možné, aby se všichni přestěhovali do svých vytoužených bytů za dva dny?

V této zemi mne spousta věcí zprvu poněkud zarážela. Například to, že i v jednadvacátém století mají ve většině domácností otroky. *Nebo fakt, že lidé tu běžně* kadí *(promiňte mi ten výraz) kdekoliv na ulici (jen na nástupištích jsou na to vyhrazené zóny) a nezřídka narazíte na ulici i na* chrup. *Také k zesnulým se chovají poměrně neuctivě, je tu totiž zvykem všechny nebožtíky řádně* pokopat.

Jinak se jedná o lid poměrně vzdělaný. K těmto účelům se scházívají na schodech, *kde po několika* besedách *člověk často pochopí i jednu větu. Mají také ve zvyku* brát *si knihy.*

Úloha 3.2 – Úloha pro vzdělaný lid (3b)

Pro navzájem různé parametry $a, b, c \in \mathbb{R}$ je dána funkce

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

Zjednodušte její zápis. Pro jaké hodnoty parametrů a, b, c existuje x, pro které $f(x) > 1$?

První člověk, s nímž jsem se zde seznámila, slul Igor Kokot. Řekl mi o sobě, že je vodník *a* vábil *mne na prohlídku* jámy*, neb jsou tam prý zajímavé* viry*. Nepochopil sice, proč se ho ptám, zda se nebojí onemocnění, ale vysvětlil mi, že je natolik* odporný*, že se mu i rýma vyhne obloukem. Pak mi nabídl, že mne může dnes* chránit*, a vzápětí mi nabídl* jed*. Nevěděla jsem si s tímto milým, ale záhadným člověkem příliš rady, ale nakonec nás dal dohromady jeho domácí* sok*.*

Dalším mým známým se stal Stanko Konečník. Ten měl dokonce skutečné povolání, pracoval jako dělník, ale se svou prací nebyl zdá se příliš spokojen. Musel prý pořád něco hradit *a pořád mluvil o* záporech*. Když jsme se loučili, naléhavě mne prosil, ať hlavně* zapřu vrata*. Není mi však jasné proč, neboť jsem u něj žádná neviděla.*

Úloha 3.3 – Dráty na stavbě (3b)

Dělník natahuje ve vysokém domě elektrické vedení a z přízemí si natáhl do nejvyššího patra 27 nerozlišitelných drátů. Teď neví, který je který. Chtěl by to zjistit a přitom se co nejméně nachodit po schodech (v budově totiž ještě nefunguje výtah). Na kolik cest se mu to může podařit? Nahoře i dole může dráty libovolně spojovat (i více dohromady) a z druhého konce pomocí multimetru testovat libovolné dvojice, zda jsou spojené.

Nejvíce mne v této zemi však zaujaly krásy přírody. Ve vysokých horách tu potkáte ku příkladu sněhové plazy*. Ačkoli celé vaše putování bude doprovázeno* potem*, pohled na svěží* dřevo *z* lesa *vám to vynahradí. Navíc tu po celý rok mají* léto*! V řece zde teče zelenožlutá kapalina, kde uprostřed spatříte podivně vyhlížející* otok*. Uklidnilo mne však zjištění, že v ní opravdu teče voda, takže nakonec jsem se i vykoupala v moři.*

Úloha 3.4 – Hustoměr (5b)

K ověření, zda nějaká kapalina je vodou (lihem, olejem, ...), slouží hustoměr. Je to dlouhý, úzký válec, který se do kapaliny částečně ponoří. Ze stupnice na jeho povrchu pak v místě, kde se jí dotýká hladina, odečteme hustotu kapaliny. Vyrobíme si takový z dutého skleněného válce o tloušťce stěny d, poloměru r a délce l a jako zátěž použijeme malé olověné kuličky. Jakého maximálního rozsahu měřených hodnot hustoty kapaliny dokážeme docílit v závislosti na

délce hustoměru l a množství olova m na dně válce? Jaké hodnoty parametrů odpovídají danému případu? Jak zvolit parametry, aby pomocí hustoměru šlo něco rozumného naměřit? (Například rozsah $15000\,\mathrm{kg}\cdot\mathrm{m}^{-3}$ v oblasti 15000–$30000\,\mathrm{kg}\cdot\mathrm{m}^{-3}$ nám příliš užitku nepřinese.)

Slovinsko-český slovníček:

g – h (čte se [g], ale etymologicky se jedná o naše h)
h – [ch]
di, ti, ni – [dy, ty, ny]
grad – město
župan – starosta
vrt – zahrada
korist – prospěch
hitrost – rychlost
stanovati – bydlet
hiša – dům
otrok – dítě
kadit – kouřit
hrup – hluk
pokopat – pohřbít
shod – shromáždění
beseda – slovo
brati – číst
vodnik – průvodce
vabiti – zvát
jama – jeskyně
vir – pramen
odporny – odolný
chraniti – krmit
jed – jídlo
sok – džus
graditi – stavět
zapor – vězení
zapreti – zavřít
vrata – dveře
plaz – lavina
pot – cesta
drevo – strom
les – dřevo
leto – rok
otok – ostrov

Řešení témat

Téma 2 – Meření rychlosti

K tématu nám přišla tři řešení, která obsahovala spoustu různých návrhů, jak měřit rychlost. Bohužel to byl ve všech případech spíše povrchní výčet. Autoři se nad jednotlivými postupy hlouběji nezamýšleli. Tím jim zaprvé mnohokrát uniklo, že by navrhovaný postup ve skutečnosti nefungoval, a za druhé, právě detaily jsou na fyzice a technice většinou to nejzajímavější a největší výzva, tak proč se jim vyhýbat.

Pokuste se nám raději poslat příspěvek, který rozebírá byť i jednu jedinou metodu do detailu.

Zamyslete se nad její proveditelností ve skutečném světě (ke skutečnému světu patří spousta rušivých vlivů, které mohou teoreticky dokonalý postup změnit na nepoužitelný).

Uvažujte nad dosažitelnou přesností. Jaká je přesnost vašeho navrhovaného postupu za reálných podmínek? Čím bude ovlivněna nejvíce? Dá se situace nějak zlepšit změnou měřícího postupu nebo použitého vybavení?

A samozřejmě experimentujte. Zkuste vaše nápady ověřit. Fungují tak, jak jste si mysleli? Podělte se s ostatními nejen o teorii, ale i o (zpracované) výsledky svých měření. Nezapomeňte, že není ani nutné, ani žádoucí „vylepšovat" výsledky tak, aby odpovídaly údajům z jiných zdrojů. Naopak, zamyslete se, proč z měření vyšlo něco jiného a hledejte příčiny.[1]

Připomínáme, že pokud vás napadne zajímavý (a rozumně proveditelný) experiment, ke kterému ale nemáte prostředky, můžete poslat organizátorům jeho popis a my se vám pokusíme zpět poslat naměřená data. Samozřejmě máte také možnost zaslat popis experimentu jako příspěvek k otištění v čísle, a nechat měření na komkoliv z ostatních řešitelů, kdo se do něj bude chtít pustit.

Abyste měli nějakou inspiraci k dalším pokusům, shrneme tu zajímavé náměty z došlých řešení.

Doba potřebná k ujetí známé vzdálenosti

Je to přímočará metoda, která napadne asi každého. Výsledkem podílu vzdálenosti a potřebného času bude průměrná rychlost. Rychlost průměrovaná přes krátký úsek ale může být i dobrým odhadem okamžité (každé vozidlo má nějaké maximální zrychlení se kterým může měnit svou rychlost)[2]. Základním problémem je, co použít jako referenční vzdálenost pro měření času.

Pro větší vzdálenosti můžeme odečítat z mapy nebo využít směrovníků u silnic udávajících vzdálenost, jak navrhuje Bc.ᴹᴹAnna Kufová. Dr.ᴹᴹJan Kadlec navrhuje použít kilometrovníky na dálnici, případně „patníky" (směrové sloupky) na obyčejných silnicích. Pro využití patníků na obyčejných silnicích nám poslal tabulku udávající jejich vzdálenost dle normy (je jiná v přímých úsecích a v zatáčkách). Vzdálenost v závislosti na poloměru zakřivení oblouku silnice (přímý úsek má poloměr oblouku nekonečný) je:

oblouk	**vzdálenost**	**oblouk**	**vzdálenost**
$\geq 1\,250$ m:	50 m	≥ 250 m:	20 m
≥ 850 m:	40 m	≥ 50 m:	10 m
≥ 450 m:	30 m	< 50 m:	5 m

[1] Kdyby ve fyzice každý zahodil výsledek, který vyjde jinak, než se čeká, nikdy by se nic nového neobjevilo. Podivná měření jsou kolikrát ta nejzajímavější, protože vám mohou ukázat, že situace je komplikovanější, než jste čekali. Samozřejmě je ale potřeba nad původem odchylky přemýšlet a hledat jej. Nejčastěji to bude nějaký kývající se kabel, zapomenutá jednička v počítačovém programu a podobné nudné věci, ale ten, kdo nemá trpělivost odhalovat nudné chyby, nikdy nenajde jiné zajímavé věci.

[2] Externí prostředky, jako třeba pevnou zeď ve směru jízdy, můžeme řešit jako zvláštní případ. Konečným výsledkem pak bude pravděpodobně nulová rychlost.

Dále Honza zmiňuje možnost využít v delším dopravním prostředku (například vlaku) dvou pozorovatelů stojících kus od sebe: „Oba se budou dívat kolmo ke směru jízdy a první zahlásí nějaký statický objekt ve chvíli, kdy ho bude mít přímo proti sobě. V tu chvíli druhý zmáčkne stopky a zastaví je, až tento objekt bude přímo proti němu. Pak změří vzdálenost mezi sebou, a mají dráhu i čas.“

Zkuste se zamyslet nad tím, jaká je vhodná délka úseku pro měření, abyste získali co nejpřesnější okamžitou rychlost. Uvažujte nepřesnost určení okamžiku míjení, měření času a případně další vlivy. Na druhou stranu uvažte typické nebo maximální zrychlení dopravního prostředku. Zkuste provést experiment a podělte se o získané výsledky a jejich přesnost.

Chůze

Dr.MMJan Kadlec zmiňuje použití krokoměru. Krokoměr je krabička, která pomocí kyvadélka (nebo jeho elektronické analogie) počítá, kolik kroků jste celkem udělali. Pro určení rychlosti potřebujeme znát čas, což většinou není problém, ale také převod počtu kroků na metry.

Zkuste experimentovat. Jak moc je přesné měření vzdálenosti na základě počtu kroků? Jak dlouhý je váš krok. Jak se takhle délka mění v závislosti na okolnostech (sklon cesty, batoh na zádech, povrch, po kterém jdete apod.). Nakolik je délka vašeho kroku během chůze stabilní? Jak byste nejlépe určili rychlost vaší chůze pomocí stopek a počítání kroků? Jak přesný výsledek můžete získat?

Houkající vlak

Bc.MMAnna Kufová zmínila využití Dopplerova efektu. Tedy skutečnosti, že zvuk přicházející z přibližujícího se vozidla nám zní vyšší, než skutečně je, a že zvuk ze vzdalujícího se vozidla je naopak nižší. Změna frekvence je úměrná vzájemné rychlosti zdroje zvuku a pozorovatele.

Změnu frekvence (výšky tónu) můžete pozorovat nejen u houkajícího vlaku, ale třeba i u projíždějícího auta (zvuk motoru). Zkuste navrhnout a zrealizovat měření rychlosti s využitím Dopplerova jevu. Co budete potřebovat za vybavení? Některým by možná mohly stačit vlastní uši. Pokud to není váš případ, zkuste si zvuk třeba nahrát a následně analyzovat na počítači. Jaké přesnosti bude schopni dosáhnout s dostupnými prostředky?

Bc.MMVáclav Skála navrhl jiný zajímavý způsob využití zvuku: „Pokud jede vlak do tunelu, obvykle dvakrát zahouká. Stačí změřit dobu od zahoukání do okamžiku, kdy se vrátí ozvěna, a toto měření porovnat s druhým.“ Bohužel se mu už nepodařilo postup dále správně dokončit.

Zkuste tuto metodu hlouběji prozkoumat. Jak určit rychlost vlaku? Na čem je postup založený? Za jakých podmínek bude fungovat. A co přesnost?

Laser

Pojďme si zastřílet z laserové pistole. Tedy, my možná ne, ale někteří policisté tak měří rychlost aut, jak připomněla Bc.MMAnna Kufová. Zařízení se jmenuje

LIDAR a princip je založený na měření doby letu světelného paprsku k měřenému předmětu a zpět. Policejní LIDAR asi po ruce nemáte, ale na stejném principu (měření doby letu) pracují běžně sehnatelné laserové měřáky vzdálenosti (nějaký takový bude pravděpodobně k vidění skoro v každém železářství nebo obchodě se stavebním materiálem). Právě využití laserového dálkoměru navrhl Bc.MMVáclav Skála. Uděláme několik měření vzdálenosti předmětu ke kterému se blížíme (který se blíží k nám) s určitým časovým rozestupem a rozdíl změřených vzdáleností podělíme časem.

Bude takový postup s využitím laserového dálkoměru fungovat? Jak přesně? Na čem může funkčnost a přesnost záviset? Pokud máte možnost, udělejte experiment a pošlete nám výsledky.

Loď

Bc.MMAnna Kufová v krátkosti zmínila i další situace. Žádnou z nich ale detailněji a správně nerozebrala, takže je tu spousta příležitostí pro další příspěvky.

Rychlost lodi se za dávných časů měřila poměrně jednoduchým zařízením, kterému se říká *log*. Námořníci hodí do vody prkno přivázané na provázku a pak měří, jak rychle se provaz odmotává. Ono prkno by mělo být vyrobené tak, aby se ve vodě ustálilo svisle, a tedy co nejúčinněji vůči vodě zabrzdilo. Pro jednoduché určení délky odmotaného provázku na něm byly uvázány uzlíky (odtud název rychlostní jednotky *uzel*) každých 14,4 metru a měřil se počet uzlíků odmotaných za 28 sekund.

Zkuste odhadnout přesnost této metody. Co je jejím limitem? Pomohlo by mít na provázku uzlíky hustěji? Představte si, že jako kapitán plachetnice plující přes Atlantik pravidelně zaznamenáváte takovéto měření rychlosti a počítáte, jak daleko jste už dopluli. Jak přesně dokážete určit vzdálenost do Ameriky? Co bude mít největší vliv na chybu výsledku?

Letadlo

Další naznačenou situací od Anny bylo pozorování letadla přičemž pozorovatel stojí na zemi. Umíte vymyslet postup, jak zjistit rychlost přelétávajícího letadla? A co třeba rychlost družice na oběžné dráze? Zkuste vymyslet vhodný postup. Nejlépe přiměřeně přesnou metoda, která ale nepotřebuje žádné speciální vybavení a informace. Uměli byste naopak pohledem z okýnka letícího letadla odhadnout jeho rychlost? Jak?

Téma 3 – Konečné automaty

K tomuto tématu jsme se zatím nedočkali žádných řešení. Pokud tě to alespoň trochu láká, zkus se na něj podívat a něco nám napsat. Třeba i pozorování, která se ti zdají úplně jasná a jednoduchá.

I některé zdánlivě jednoduché úkoly ale mohou být těžší, než se na první pohled zdá. Jaká slova přijímá automat č. 2 uveřejněný v prvním čísle?

Kuba

Řešení úloh

Úloha 1.1 – Tisíc (1+3b)

Zadání:

(i) Součet několika (nejméně dvou) po sobě jdoucích přirozených čísel je 1000. Jaké největší číslo mezi nimi může být?

(ii) Která všechna celá čísla lze zapsat jako součet dvou a nebo více po sobě jdoucích přirozených čísel?

Řešení:

(i) Aby největší ze sčítanců byl co největší, tak budeme chtít, aby sčítanců bylo co nejméně.

Součet n po sobě jdoucích čísel lze zapsat jako:

$$a + (a+1) + \ldots + (a-n-1) = na + \frac{n(n-1)}{2},$$

kde a je nejmenší číslo ze sčítaných čísel.

Aby se tento výraz rovnal 1000, tak musí platit, že

$$na = 1000 - \frac{n(n-1)}{2}.$$

Protože a má být přirozené číslo, tak musí platit:

$$n \mid 1000 - \frac{n(n-1)}{2}.$$

Nyní již jednoduchým dosazením do tohoto vztahu za n postupně 2, 3 a 4 zjistíme, že 1000 nelze zapsat jako součet méně než pěti po sobě jdoucích čísel. Jelikož $1000 = 198 + 199 + 200 + 201 + 202$, tak největší číslo v součtu bude 202.

(ii) Ukážeme, že jako součet několika po sobě jdoucích přirozených čísel jdou zapsat všechna čísla kromě mocnin dvou.

Součet lichého počtu čísel můžeme zapsat jako

$$(a-n) + (a-n+1) + \ldots + (a+n) = \frac{1}{2}(2n+1)a.$$

Aby šlo o součet přirozených čísel, tak musí platit $a > n$. Součet sudého počtu čísel lze zapsat jako

$$(n) + (n+1) + \ldots + (n+2k+1).$$

To si ovšem můžeme trikově přepsat na součet celých čísel ve tvaru

$$(-n+1) + (-n+2) + \ldots + (n+2k+1) = \frac{1}{2}(2k+2)(2k+3).$$

Ať už tedy sčítáme libovolný počet po sobě jdoucích čísel, v prvočíselném rozkladu jejich součtu bude nějaké liché číslo. Z toho plyne, že žádnou mocninu dvou nemůžeme zapsat jako součet po sobě jdoucích přirozených čísel.

Nyní už jen stačí provést pro zbylá čísla konstrukci sčítanců:

Pokud je číslo liché (a různé od jedničky, která je mocninou dvou: $2^0 = 1$), můžeme jej zapsat ve tvaru $2k + 1$, kde $k \in \mathbb{N}$. Pak toto číslo můžeme napsat jako součet dvou přirozených čísel k a $k + 1$.

Pokud je číslo sudé, ale není mocninou dvojky, pak jde zapsat jako součin lichého čísla $2k+1$ a přirozeného čísla n. Toto číslo zapíšeme jako součet po sobě jdoucích celých čísel od $n - k$ do $n + k$. Nesmíme zapomenout ošetřit, že pokud $n - k$ je liché, tak z tohoto součinu vynecháme čísla od $n - k$ do $|n - k|$. Tím se celkový součet nezmění a zbylá čísla budou určitě kladná, a tedy i přirozená. Protože $k \geq 1$, tak součet od $|n - k| + 1$ do $n + k$ bude obsahovat alespoň dvě čísla.

Martin

Úloha 1.2 – Kulatý stůl (4b)

Zadání:
Mějme les, definovaný jako množina bodů v rovině (zadaný bod je středem stromu) a jejich poloměrů (poloměr může být u různých stromů různý). Uprostřed lesa stojí kulatý stůl krále Artuše (stejně jako stromy je zadán svým středem a poloměrem). Zajímá nás, jak dostat tento stůl z lesa ven, aniž bychom přitom museli pokácet nějaké stromy. Stůl není možné naklánět, aby se nepřevrhl Svatý grál postavený uprostřed. Navrhněte proto algoritmus, který ze zadaného lesa a stolu určí cestu, kudy dokážeme stůl z lesa vymanipulovat. Pokud to také bude cesta nejkratší, odměna navíc vás nemine.

Řešení:
Nejdříve si úlohu mírně zjednodušíme. Všimněme si, že když poloměry všech stromů v lese zvětšíme o poloměr stolu a stůl samotný zmenšíme na 1 bod, řešení úlohy se nám nezmění. Pokud stůl mohl projít mezi dvěma stromy v původním zadání, projde i teď. Naopak, pokud projít nemohl, budou se stromy po „nafouknutí“ překrývat, a tedy neprojde ani jako bod.

Zkusíme si úlohu trochu zformalizovat a popsat ji prostředky moderní informatiky. Stromy v nafouknutém lese nám vytvoří tzv. triangulaci. Nataháme mezi středy stromů myšlené úsečky tak, aby se žádné dvě neprotínaly, a aby všechny vnitřní stěny vzniklého grafu byly trojúhelníky (pokud by nám vznikla mýtina složená z více stromů než tří, můžeme v ní jednoduše natahat další úsečky a rozdělit ji na trojúhelníky).

Nyní zkonstruujeme graf G, kde vrcholy tohoto grafu jsou jednotlivé trojúhelníky v triangulaci a hrana vede mezi dvěma vrcholy právě tehdy, když bylo možno projít se stolem z jednoho trojúhelníku do druhého (což je právě tehdy, když se nafouknuté stromy vymezující danou úsečku neprotínaly). Graf G je diskrétní reprezentací Artušovského lesa. Hrana v něm vede právě mezi místy, mezi kterými jsme mohli projít s kulatým stolem z původního zadání.

Nyní už můžeme na graf G pustit vyhledávací algoritmus, který nám najde cestu ven z lesa. Většina z vás navrhovala postupovat následovně:

Zkusíme se vydat po nějaké hraně. Pokud jsme se dostali do slepé uličky, nebo do místa, kde už jsme byli, vrátíme se o jeden krok zpátky a hranu, po které jsme se vrátili, si označíme a už po ní znovu nepůjdeme.

Tento algoritmus se nazývá DFS (depth-first search), česky prohledávání do hloubky. Pokud je les konečně velký, určitě najde nějakou cestu ven, nezaručí nám však, že to bude cesta nejkratší. Abychom to zaručili, museli bychom tímto algoritmem prohledat celý graf, což může být časově náročné.

Oproti tomu uvažte následující algoritmus:

Začneme ve vrcholu v. Nejdříve zkusíme všechny vrcholy ve vzdálenosti 1 od v. Pokud jsme na kraji lesa, skončíme, pokud ne, tak vezmeme všechny vrcholy ve vzdálenosti 2 od v (tedy sousedy vrcholů ve vzdálenosti 1). A tak dále, postupně prozkoumáváme vzdálenější sousedy, dokud nenajdeme cestu z lesa. Výhodou je, že první cesta z lesa, kterou najdeme, je ona vytoužená nejkratší cesta.

Výše popsaný algoritmus se nazývá BFS (breadth-first search), česky prohledávání do šířky. V nejhorším případě (tj. když jsou všechny vrcholy G vzdáleny od v nejvýše k, což je zároveň délka nejkratší cesty z lesa) projdeme celý graf, stejně jako u DFS. V průměrném případě na tom ale budeme lépe.

Počkat, počkat! Vždyť vzdálenosti mezi vrcholy G nejsou vždy stejné – stromy jsou od sebe přece různě daleko! Naštěstí úprava algoritmu, aby zohledňoval vzdálenosti, není složitá. Vezmeme si v každém trojúhelníku triangulace nějaký význačný bod, který vždy leží uvnitř – např. těžiště. Na hrany grafu G pak napíšeme čísla odpovídající vzdálenosti težišť dvou sousedících trojúhelníků.

Při prohledávání do šířky pak budeme brát vrcholy popořadě podle jejich vzdálenosti od v (která bude dána součtem čísel na hranách vedoucích z v do daného vrcholu).

Formálně: pro každý vrchol x si zapamatujeme hodnotu $d(x)$, která bude značit délku nejkratší cesty z v do x. Na začátku nastavíme $d(x) = \infty$ pro všechny vrcholy $x \neq v$ a $d(v) = 0$.

Vezmeme ještě nenavštívený vrchol x s nejnižší hodnotou $d(x)$ a podíváme se na jeho souseda y. Pokud vzdálenost $d(x)+e(x,y) < d(y)$[3], přiřadíme $d(y) = = d(x) + e(x,y)$. Tím jsme snížili délku nejkratší cesty do y (a víme, že tato cesta vede přes vrchol x). Toto provedeme pro všechny sousedy x a vrchol x uzavřeme. Jeho nejkratší vzdálenost od v už se nikdy nezmenší, kdyby ano, musel bych se do něj nejdříve dostat přes některého z jeho sousedů, ale všichni jeho sousedi jsou už uzavření, nebo jsou dále od v než x.

Takto budeme postupovat, dokud nenajdeme cestu na kraj lesa. Když si navíc u každého vrcholu poznamenáme, odkud jsme do něj museli po nejkratší trase přijít (poslední vrchol, který snížil $d(x)$), dostaneme nejen délku nejkratší cesty, ale rovnou i její trasu.

Tento propočet je pro nás již dostatečně dobrou aproximací reálné situace. Kdybychom chtěli být ještě preciznější, museli bychom uvažovat to, že budeme

[3] $e(x,y)$ značí délku hrany mezi vrcholy x a y

se stolem rotovat okolo stromů a přecházet od jednoho stromu ke druhému pouze po společných tečnách. Způsob, jak tento způsob manipulace popsat pomocí grafů, ponecháme čtenáři jako jednoduché myšlenkové cvičení :-).

Honza

Úloha 1.3 – Jablko nepadá daleko od stromu (3b)

Zadání:

Jak nejdál může dopadnout jablko, které spadne ze stromu o výšce 3 m? Strom se nachází na rovném trávníku, tedy ani na kopci, ani v dolíku. Předpokládejte, že při odrazu jablka od země se na deformace spotřebuje 1/4 kinetické energie jablka. Nebojte se zavést nějaká vlastní zjednodušení, pokud to budete považovat za nutné (ale nezapomeňte je v řešení popsat), máte přece počítat ideální případ...

Řešení:

Vaším úkolem bylo zjistit (spočítat, kvalifikovaně odhadnout) jak nejdál může jablko dopadnout od stromu. Měli jste tedy hledat podmínky nějakým způsobem ideální, které by umožňovaly jablku dostat se co nejdál. Chtělo to trochu fantazie, a většina z vás ji měla. Našlo se jen pár výjimek, kteří suše konstatovali, že za ideálních (ale jiným způsobem ideálních, tím nešikovným) podmínek spadne jablko přímo pod místo, kde na stromě rostlo, a šmitec. Někteří se snažili započítat vliv větru, který by měl jablko unášet směrem od stromu. Ve výsledku sice hrál jistou roli, ale my ho zanedbáme. Stejně tak zanedbáme délku větve a za bod nula budeme považovat bod, kde se jablko poprvé dotklo země. Zanedbáme i odpor vzduchu (bez něj nám ten vítr ani nebude nic unášet :-). Povrch trávníku považujeme za potenciálně hrbolatý, protože jsme v sadu, a ne na golfovém hřišti.

Prvním trikem je představit si v místě dopadu jablka vhodný hrbol, který nám jablko odrazí směrem, který chceme.

Směr, který chtěla většina z vás, byl pryč od stromu pod úhlem 45°. Šikmý vrh pod tímto úhlem má, jak známo, nejdelší dolet. Pokud by vám nestačil argument, že je to všeobecně známo, můžete si vztah pro dolet šikmého vrhu odvodit

$$x = v_0 t \cos\alpha \quad \text{pro} \quad y = v_0 t \sin\alpha - \frac{1}{2} g t^2 = 0\,.$$

Jablko padá z výšky $h = 3\,\mathrm{m}$ a získá tím kinetickou energii $E_0 = mgh$. Odrazí se rychlostí

$$v_1 = \sqrt{\frac{3}{2} gh}\,,$$

což odpovídá o čtvrtinu menší energii

$$E_1 = \frac{3}{4} mgh\,.$$

Odrazí se tedy rychlostí

$$v_1 = \sqrt{\frac{3}{2} gh}\,.$$

Podle výše uvedených vztahů pro šikmý vrh uletí vzdálenost

$$x_1 = v_1 \cos\alpha \frac{2v_1 \sin\alpha}{g} = \frac{v_1^2 \sin 2\alpha}{g}\,.$$

Dále dosadíme za v_1 ze vztahu původní potenciální energie a kinetické energie po odrazu

$$x_1 = \frac{3}{2}h \sin 2\alpha = \frac{3}{2}h\,.$$

Dalším odrazem ztratí další čtvrtinu energie a uletí vzdálenost (x závisí na v^2, tedy lineárně na energii)

$$x_2 = \frac{3}{2}\frac{3}{4}h\,.$$

Každý další skok bude tři čtvrtiny předchozího. Celkovou vdálenost, do jaké se jablko dostane, si můžeme zapsat jako součet nekonečné řady

$$x = h\sum_{i=1}^{\infty} \frac{3}{2}\left(\frac{3}{4}\right)^i = h\frac{3}{2}\sum_{i=1}^{\infty}\left(\frac{3}{4}\right)^i\,,$$

což je řada geometrická. Platí

$$\sum_{i=1}^{\infty} q^i = \frac{1}{1-q}\,,$$

pro $q \in (0,1)$. Součet naší řady je tedy

$$x = h\frac{3}{2}\cdot\frac{1}{1-3/4} = 18\,\mathrm{m}\,.$$

Překvapilo mě, kolik z vás mělo problém se součtem geometrické řady. Štěpánka Titlová využila k řešení program, který našla na internetu. Na jejím příkladě je krásně vidět, že dokážete vyřešit lecjaký úkol, pokud se k němu postavíte čelem a zeptáte se na správných místech (na googlu). Pro řešení hádanek, které zadáváme občas jako čtvrtou úlohu, tahle metoda ale není úplně fér.

Další možný směr, kterého byste mohli chtít docílit, je vodorovný. Jablko se tedy bude po odrazu kutálet po povrchu, bude ale nutné odhadnout některé další parametry.

Pokud se tedy jablko kutálí, překonává valivý odpor

$$F_\mathrm{o} = \xi\frac{F_\mathrm{n}}{r}\,,$$

kde ξ je rameno valivého odporu, je definováno vždy pro dvojici materiálů a uvedeno v tabulkách, pro dvojici jablko–tráva ale, obávám se, nikde nenajdete, a bude třeba jej odhadnout. Pro obvyklé dvojice materiálů je v řádu tisícin až desetitisícin metru, pro jablko a trávu tedy tipneme např. $0,05\,\mathrm{m}$, to je o dva řády víc, takže by to mělo dostatečně zohlednit, jak blbě se valí po hrbolatém

trávníku. F_n je přítlačná síla kolmá na povrch. Náš povrch je vodorovný, takže je rovna tíhové síle působící na jablko. Druhým parametrem je poloměr jablka. Řekněme tak 3 cm. Tato síla působí směrem proti pohybu jablka a koná tak práci

$$W = F_\mathrm{o} \cdot s\,.$$

Kde s je dráha. Síla působí tak dlouho, dokud se jablko nezastaví. Musí tedy vykonat práci, která eliminuje energii jablka.

$$W = F_\mathrm{o} \cdot s = \frac{\xi m g}{r} s = E_1 = \frac{3}{4} m g h\,.$$

s je tedy naše hledané x.

$$x = \frac{3}{4} \cdot \frac{rh}{\xi} = 1{,}3\,\mathrm{m}\,.$$

To je poněkud méně, než pro skákání pod úhlem 45°. Musím ale upozornit, že ztráta jenom čtvrtiny energie při odrazu není reálná, rozumnější by bylo předpokládat, že jablku místo tří čtvrtin zůstane jen desetina původní energie. Někteří z vás si toho všimli a budiž pochváleni před nastoupenou jednotkou. Jsou to Bc.ᴹᴹ Michal Buráň a Mgr.ᴹᴹ Lubomír Grund. Na to, zda byla chyba v zadání důsledkem nedbalosti, nebo úmyslný quest, si udělejte názor sami. Pokud bychom uvažovali reálnější koeficient zachování energie při odrazu 0,1, dostaneme pro skákání vzdálenost

$$x = h\frac{3}{2} \cdot \frac{1}{1-0{,}1} = 5\,\mathrm{m}\,.$$

A pro kutálení

$$x = 0{,}1\frac{rh}{\xi} = 0{,}45\,\mathrm{m}\,.$$

Zuzka

Úloha 1.4 – Ruleta (1+1b)

Zadání:

Riki vymyslel strategii, jak vyhrávat v ruletě. Na začátku vsadí určitou částku na červenou barvu. Pokud vyhraje, vrátí se mu její dvojnásobek, pokud nevyhraje, v dalším kole její dvojnásobek vsadí opět na červenou. A tak dále. Pravděpodobnost, že by ani jednou nepadla červená je nulová. Po nějaké době tedy zákonitě musí vyhrát. Když sečte své vklady a výhry, tak zjistí, že vyhrál více než vložil. Tento postup může neustále opakovat.

(i) Bude tato strategie opravdu fungovat?

(ii) Riki má 100 Kč a chce hrát pomocí své strategie tak dlouho dokud nezíská 200 Kč nebo vše neprohraje. Poraďte mu, kolik má postupně do hry vsázet, aby měl co nejvyšší pravděpodobnost výhry. Do rulety lze vsázet pouze celé koruny.

Řešení:

(i) Většina z vás odvodila, že dokud má Riki dost peněz na vsázení, tak bez ohledu na počet po sobě jdoucích proher vyhraje při první výhře svůj původní vklad. Pokud by tedy měl Riki nekonečně mnoho peněz a kasíno by povolovalo neomezeně velké sázky, jeho strategie by fungovala. Nekonečně mnoho peněz ale z principu nemůže existovat, protože pak by měla libovolná částka v té měně nulovou hodnotu. (Představte si to třeba tak, že by si Riki koupil při vstupu do kasina nekonečně žetonů. Pak musí mít každý jeden žeton reálně nulovou cenu a výhra 1 žetonu není žádnou výhrou.) Tudíž strategie nebude fungovat nikdy.

(ii) U první otázky nezáleželo na tom, jaká je pravděpodobnost výhry, pouze na tom, že někdy výhra nastane. U druhé otázky už nás začíná zajímat, jak taková ruleta vlastně vypadá. Běžně se objevují dva typy: francouzská ruleta, která má jednu nulu, a americká, která má nuly dvě. Nula je speciální políčko, které se nepočítá ani jako červené, ani jako černé a vnáší do hry větší nejistotu. Vezměme si třeba francouzskou ruletu a ptejme se, jaký je náš očekávaný zisk za jedno kolo hry.

Dejme tomu, že můžeme prohrát maximálně n sázek, než zbankrotujeme. Pravděpodobnost, že se tak stane, je q^n, kde q je pravděpodobnost prohry (u francouzské rulety $\frac{19}{37}$). V případě, že zbankrotujeme, prohrajeme celkem $B(2^n-1)$, kde B je základní sázka, kterou začínáme hru. Naopak, s pravděpodobností $1-q^n$ vyhrajeme základní vklad B. Jen pro příklad, pokud bychom měli na začátku 127 Kč, můžeme vsadit až šestkrát po sobě, než zbankrotujeme. Pravděpodobnost bankrotu bude $\left(\frac{19}{37}\right)^6 \approx 0{,}018$, tedy necelá dvě procenta.

Očekávaný zisk v jednom kole hry spočteme jako pravděpodobnost výhry krát hodnotu výhry mínus pravděpodobnost prohry krát hodnotu prohry:

$$(1-q^n)B - q^n(2^n-1)B = B(1-q^n-2^nq^n+q^n) = B(1-(2q)^n)$$

Vidíme, že kdykoliv je $q > 0,5$, je očekávaný zisk záporný. V každé hře, kde je pravděpodobnost prohry větší, než pravděpodobnost výhry, v průměru ztrácíme peníze. Dokonce i kdyby v ruletě nebyla zelená nula, očekávaný zisk by byl veškerý žádný.

Z uvedeného vzorce také vyplývá, že čím déle hrajeme, tím víc peněz ve výsledku ztratíme. Odpověď na otázku, jak má Riki sázet, když chce ze 100 Kč udělat 200 Kč je tedy jednoduchá – má rovnou vsadit celých 100 Kč a doufat ve štěstí.

Protože je vždy dobré ověřit si výsledky svého výpočtu v praxi, napsal jsem simulační program, který zkusil za Rikiho hrát ruletu a vsázet postupně počáteční částky mezi 1 Kč do 100 Kč. Pro každou vsazenou počáteční částku proběhla simulace stotisíckrát. Uvádíme pouze některá zajímavá čísla:

B	výher	proher	pravděpodobnost výhry
1	30767	69233	0,30767
2	31382	68618	0,31382
3	31019	68981	0,31019
4	32540	67460	0,3254
33	29277	70723	0,29277
34	26265	73735	0,26265
99	23732	76268	0,23732
100	48706	51294	0,48706

Honza

O vzorci pro řešení kvadratických rovnic

Karel Ullwer

Přinášíme vám článek našeho řešitele Karla Ullwera představující různá alternativní odvození vzorce pro výpočet řešení kvadratické rovnice. Na níže uvedených postupech lze pěkně demonstrovat, že když známe výsledek, umíme se k němu dostat i všelijakými oklikami. Zkuste si promyslet, nakolik jsou jednotlivé varianty opravdu rozdílné.

Článek zachovává původní strukturu i prezentované výsledky, stylisticky je však redakčně upraven.

Kuba

Uvažujme obecnou kvadratickou rovnici $ax^2 + bx + c = 0$, kde $a, b, c \in \mathbb{R}$ jsou parametry a x reálná proměnná. Hledáme vzorec, kterým pomocí zadaných parametrů vyjádříme neznámou x vyhovující rovnici. Cílem tohoto článku je ukázat několik zajímavých metod, jak ke vzorci dojít. Uvidíme, že zcela rozdílnými úvahami můžeme dojít ke stejnému výsledku.

Doplnění na čtverec

Klasickou školní metodou odvození vzorce je tzv. doplnění na čtverec. To dostaneme následovně:

$$\begin{aligned} ax^2 + bx + c &= 0 \qquad / \cdot 4a \quad / + b^2 - b^2 \\ 4a^2x^2 + 4abx + b^2 - b^2 + 4ac &= 0 \\ (2ax + b)^2 &= b^2 - 4ac \\ 2ax + b &= \pm\sqrt{b^2 - 4ac} \\ x_{1,2} &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

Nás budou ale zajímat především alternativní odvození.

Substituce $x = u + v$

Kvadratickou rovnici vydělíme parametrem a, dostaneme tak znormovanou rovnici $x^2 + px + q = 0$, kde $p, q \in \mathbb{R}$. Do této rovnice za x dosadíme $u + v$. Dostaneme:

$$\begin{aligned} (u+v)^2 + p(u+v) + q &= 0 \\ u^2 + 2uv + v^2 + pu + pv + q &= 0 \\ u^2 + v^2 + v(2u + p) + pu + q &= 0 \end{aligned}$$

Nyní využijeme podobnou myšlenku jako při odvození Cardanových vzorců pro řešení kubických rovnic. Dva parametry nám dávají dostatečnou volnost a

můžeme proto zvolit $2u+p=0$, neboli $u=-\frac{p}{2}$. Každé x můžeme stále vyjádřit vhodnou volbou v. Dosadíme do výše upravené rovnice:

$$\begin{aligned}\frac{p^2}{4}+v^2-\frac{p^2}{2}+q&=0\\ v^2&=\frac{p^2}{2}-\frac{p^2}{4}-q\\ v^2&=\frac{2p^2-p^2-4q}{4}=\frac{p^2-4q}{4}\\ v&=\pm\frac{\sqrt{p^2-4q}}{2}\end{aligned}$$

Zjistili jsme, že $u=-\frac{p}{2}$ a $v=\pm\frac{\sqrt{p^2-4q}}{2}$. Přitom ale

$$x=u+v=-\frac{p}{2}\pm\frac{\sqrt{p^2-4q}}{2}=\frac{-p\pm\sqrt{p^2-4q}}{2}.$$

Nyní stačí dosadit $p=\frac{b}{a}$ a $q=\frac{c}{a}$ a vyjde nám stejný vzorec jako u doplnění na čtverec.

Využití algebraického tvaru komplexního čísla

V rovnici $ax^2+bx+c=0$ substituujme $x=q+pi$, kde i je komplexní jednotka. Při tom využíváme faktu, že každé reálné číslo je zároveň i komplexní. Upravujme:

$$\begin{aligned}a(q+pi)^2+b(q+pi)+c&=0\\ aq^2+2aqpi-ap^2+bq+bpi+c&=0\end{aligned}$$

Rovnost musí platit v reálné i komplexní složce rovnice. Můžeme tedy rovnici přepsat na soustavu rovnic:

$$aq^2-ap^2+bq+c=0 \quad (1)$$
$$2aqp+bp=0 \quad (2)$$

Z rovnice (2) vyjádříme $q=-\frac{b}{2a}$ a dosadíme do rovnice (1), získáme tak vztah:

$$\begin{aligned}a\frac{b^2}{4a^2}-ap^2-\frac{b^2}{2a}+c&=0\\ \frac{b^2-2b^2+4ac}{4a}&=ap^2 \qquad /\cdot 1/a\\ \frac{-b^2+4ac}{4a^2}&=p^2\\ p&=\pm\frac{\sqrt{-b^2+4ac}}{2a}\end{aligned}$$

Celkem

$$x = q + pi = \frac{b}{2a} \pm \frac{i\sqrt{-b^2+4ac}}{2a} = -\frac{b}{2a} \pm \frac{\sqrt{b^2-4ac}}{2a},$$

což jsme chtěli.

Využití komplexních čísel v goniometrickém tvaru

Do rovnice $ax^2+bx+c=0$ dosaďme tentokrát komplexní číslo v goniometrickém tvaru $x = r(\cos\varphi + i\sin\varphi)$, kde $r \in \mathbb{R}^+{}_0$ a $\varphi \in \langle 0, 2\pi)$. Následně upravíme pomocí Moivrovy věty:

$$\begin{aligned} ar^2(\cos\varphi + \subset \sin\varphi)^2 + br(\cos\varphi + i\sin\varphi) + c &= 0 \\ ar^2(\cos 2\varphi + i\sin 2\varphi) + br(\cos\varphi + i\sin\varphi) + c &= 0 \\ ar^2\cos 2\varphi + ar^2 i\sin 2\varphi + br\cos\varphi + bri\sin\varphi + c &= 0 \end{aligned}$$

Opět porovnáme zvlášť reálnou a imaginární část. Předchozí vztah si můžeme napsat jako soustavu rovnic:

$$ar^2\sin 2\varphi + br\sin\varphi = 0 \tag{3}$$
$$ar^2\cos 2\varphi + br\cos\varphi + c = 0 \tag{4}$$

Z rovnice (3) vyjádříme

$$r = \frac{-b\sin\varphi}{a\sin 2\varphi} = \frac{-b\sin\varphi}{2a\sin\varphi\cos\varphi} = \frac{-b}{2a\cos\varphi}$$

a dosadíme do rovnice (4), kterou následně upravíme. Dostaneme tak:

$$\begin{aligned} a\frac{b^2}{4a^2\cos^2\varphi}\cos 2\varphi - b\frac{b}{2a\cos\varphi} + c &= 0 \\ \frac{ab^2(\cos^2\varphi - \sin^2\varphi)}{4a^2\cos^2\varphi} + c &= \frac{b^2}{2a} \\ \frac{b^2}{4a} - \frac{b^2\sin^2\varphi}{4a\cos^2\varphi} + c &= \frac{b^2}{2a} \\ \frac{b^2}{4a} - \frac{2b^2}{4a} + c &= \frac{b^2}{4a}\sin^2\varphi\cos^2\varphi \\ \frac{-b^2+4ac}{4a} &= \frac{b^2}{4a}\sin^2\varphi\cos^2\varphi \\ \pm\sqrt{\frac{-b^2+4ac}{b^2}} &= \frac{\sin\varphi}{\cos\varphi} \\ \sin\varphi &= \pm\frac{-b^2+4ac}{b}\cos\varphi \end{aligned}$$

Celkem jsme odvodili, že $r = \dfrac{-b}{2a\cos\varphi}$ a $\sin\varphi = \pm\dfrac{-b^2+4ac}{b}\cos\varphi$. To dosadíme zpět do substituce $x = r(\cos\varphi + i\sin\varphi)$ a dopočítáme

$$\begin{aligned} x &= \frac{-b}{2a\cos\varphi}\left(\cos\varphi + i\frac{\pm\sqrt{-b^2+4ac}}{b}\cos\varphi\right) = \\ &= \frac{-b}{2a} + \frac{-bi\left(\pm\sqrt{-b^2+4ac}\right)}{2ab} = \frac{-b}{2a} - \frac{i\left(\pm\sqrt{-b^2+4ac}\right)}{2a} = \\ &= \frac{-b}{2a} \pm \frac{\sqrt{b^2-4ac}}{2a}. \end{aligned}$$

Opět máme ten samý vzorec pro výpočet řešení kvadratické rovnice.

Proti výše uvedeným postupům by bylo možné vznést námitku, že komplexní čísla jsou konstrukce mnohem mladší než kvadratické rovnice. Cílem tohoto článku bylo ale hlavě ukázat, jak různé postupy dávají stejný výsledek, a demonstrovat tak zvláštní krásu matematiky.

Elektronické podpisy

Pojem elektronický podpis už nejspíš většina z vás mnohokrát slyšela. Jedná se o snahu nějak prokázat, že určitá osoba nějaký dokument viděla a souhlasí s jeho obsahem. Částečně můžeme elektronický podpis chápat jako alternativu k podpisu klasickému. Oproti němu ale narážíme na určitá omezení, například na omezenou dobu, po kterou je podpis důvěryhodný. To je občas nepříjemné například při uzavíraní elektronických smluv.

Pokusíme se problematiku elektronického podpisu nastínit z pohledu matematika, programátora-inženýra i běžného uživatele. Při tom se nevyhneme ani některým právním poznámkám. V textu se záměrně vyskytuje mnoho zkratek, které pro pochopení nejsou podstatné, ale pomohou s orientací při případném hledání dalších informací.

Princip fungování

V podstatě každý elektronický podpis je založen na nějaké asymetrické šifře a hešovací funkci. Jako šifra se nejčastěji požívá kryptosystém RSA, hešovací funkce bývá typicky SHA-1 či nějaký její nástupce (např. SHA-256).

Hešovací funkce je technický prostředek umožňující libovolně dlouhé zprávě přiřadit jednoznačně řetězec znaků (ten bývá nazýván heš) pevné délky, například 160 bitů v případě SHA-1. Přitom chceme, abychom mohli heš považovat za jedinečný v tom smyslu, že k němu nedokážeme najít žádnou jinou zprávu se stejným hešem. Snažíme se ale vyvarovat i toho, abychom uměli najít dvě zprávy mající jakýkoli (námi zvolený) stejný heš.

Algoritmus je RSA založený na tom, že je obtížné velká čísla rozkládat na prvočísla (faktorizovat) a že neumíme efektivně odmocňovat, pokud počítáme vše modulo velké číslo (tomu se říká problém diskrétního logaritmu). Pro jeho matematický popis budeme potřebovat několik pojmů z teorie čísel.

V následujícím textu si skutečnost, že čísla a a b dávají stejný zbytek po dělení n (neboli $n|a-b$) označíme $a \equiv b \pmod{n}$ (čteme a je kongruentní s b modulo n). Platí takzvaná Malá Fermatova věta, která říká, že pro přirozené číslo a a s ním nesoudělné prvočíslo p platí $a^{p-1} \equiv 1 \pmod{p}$. Podrobněji včetně důkazů (které nejsou nijak obtížné) lze vše najít například v seriálu MKS [1].

Před samotným podepisováním pomocí RSA si nejdříve vygenerujeme dvě různá velká prvočísla p a q (např. dlouhá 2048 bitů). Spočítáme si jejich součin $n = p \cdot q$ a číslo $m = (p-1)(q-1)$. Následně zvolíme libovolné číslo e, které je menší než m a s m nesoudělné, a dopočítáme d tak, aby $e \cdot d \equiv 1 \pmod{m}$. To umíme efektivně pomocí Euklidova algoritmu. Dvojici (n, e) budeme říkat veřejný klíč a někam ji veřejně vystavíme. Ta bude sloužit k ověřování našeho podpisu. Naopak dvojici (n, d) nazývanou soukromý klíč nikomu jinému neprozradíme – pomocí ní budeme zprávy podepisovat.

Pokud budeme chtít nějakou zprávu z podepsat, spočítáme si nejdříve její heš $h(z)$, což bude číslo menší než n (potřebujeme vhodnou hešovací funkci), a

potom pro tento heš spočítáme podpis jako $s \equiv (h(z))^d \pmod{n}$. Se zprávou z pak pošleme i její podpis s. Příjemce si spočítá $Z \equiv s^e \pmod{n}$. Pokud vše proběhlo v pořádku, tak

$$Z \equiv s^e \equiv (h(z))^{de} \equiv (h(z)) \pmod{n}.$$

Poslední kongruence platí díky Malé Fermatově větě (rozmysli si). Příjemci tedy stačí pro ověření podpisu porovnat, jestli se rovnají Z a $h(z)$.

Poznamenejme, že kryptosystém RSA lze mimo podepisování použít také pro šifrování. V takovém případě odesílatel zašifruje data pomocí příjemcova veřejného klíče. A adresát je pak dešifruje pomocí svého soukromého klíče. Celá zpráva je ale obvykle příliš velká, na to, abychom ji mohli šifrovat pomocí RSA. Proto se RSA použije pouze pro šifrování klíče nějakého jiného (obvykle symetrického) kryptosystému.

Technická realizace

Nyní už umíme posílat elektronicky podepsané zprávy. Má to ale jeden háček. Kde vzít veřejný klíč pro ověření podpisu? Pokud bychom ho dostávali společně se zprávou, mohl by si útočník vygenerovat nějakou vlastní dvojici RSA klíčů a zprávu podepsat pomocí nich. Bylo by možné si klíče s druhou stranou vyměnit nějakou bezpečnou cestou před samotnou komunikací. Tak se to skutečně občas dělá, ale není to příliš praktické.

Lepší variantu představuje využití takzvaných certifikačních autorit (běžně se používá zkratka CA). To jsou instituce, kterým všichni implicitně věří. Pokud chcete poslat podepsanou zprávu, můžete se nejdřív obrátit na certifikační autoritu, která ověří, že dané podpisové klíče patří opravdu vám. K tomu stačí, když ji sdělíte svůj veřejný klíč a podepíšete nějakou zprávu pomocí soukromého klíče. Samotný soukromý klíč byste neměli svěřovat ani certifikační autoritě. Budete také pochopitelně muset nějak prokázat svou totožnost. Certifikační autorita vám pak vytvoří soubor zvaný certifikát, který obsahuje informace o vašem veřejném klíči a identifikaci vaší osoby. Platnost tohoto certifikátu potvrdí tak, že jej sama podepíše pomocí svého soukromého podpisového klíče.

Pokud chcete nyní poslat nějakou podepsanou zprávu, stačí k ní přiložit i váš certifikát. Příjemce si může ověřit pravost podpisu certifikační autority (informace o veřejných klíčích certifikačních autorit bývají standardně dostupné na každém počítači) a tedy i důvěryhodnost vašich veřejných klíčů. Pomocí nich pak ověří podpis zprávy.

Ve skutečnosti je situace ještě malinko složitější. Certifikačních autorit je hodně a samy mohou být uspořádány v hierarchické struktuře. Na počítači tedy nebývají informace o veřejných klíčích všech autorit, ale jen těch nejvyšších. Zbývající mezičlánky pro ověření podpisu je potřeba si stáhnout od jednotlivých autorit. Ale to se v případě různých softwarových produktů děje obvykle zcela automaticky. Posloupnosti všech certifikátů potřebných pro ověření podpisu se obvykle říká certifikační cesta. Navíc není pravda, že jsou všechny autority v nějaké struktuře. Občas se může stát, že při hledání vhodného veřejného

klíče pro ověření certifikátu neuspějeme. Pak je na nás, jestli se rozhodneme certifikační autoritě ověřující pravost podpisových klíčů odesílatele věřit a přidat si ji mezi důvěryhodné.

Možná vás napadla otázka, jak se šíří informace o veřejných klíčích certifikačních autorit. Překvapivě je to opět pomocí certifikátů. Jen autority na nejvyšší úrovni si certifikáty podepisují samy, nemáme tedy jak ověřit jejich pravost. Pro zájemce o hlubší proniknutí do problému ještě poznamenejme, že vnitřně má certifikát předepsanou strukturu v jazyce ASN.1 a typicky se kóduje pomocí BER nebo DER kódování. Mimo veřejných klíčů a identity odesílatele obsahuje ještě spoustu dalších technických dat, například o certifikační autoritě. Zkuste si nějaký certifikát prohlédnout.

Praktické použití

Pokud chceme elektronický podpis používat, musíme si nejdříve obstarat náš osobní certifikát. V Česku existují tři certifikační autority, které vydávají certifikáty použitelné i při komunikaci se státními úřady. Jsou to První certifikační autorita (I.CA), česká pošta (PostSignum) a eIdentity [2]. Podpisům vytvořeným pomocí certifikátů od těchto autorit se dle zákona říká zaručené. Pro získání certifikátu bývá potřeba zajít na nějaké místo a tam skutečně prokázat svou totožnost. Hlavně se ale tyto certifikáty nevydávají zadarmo.

Pokud nechceme komunikovat s úřady, můžeme si vystačit s libovolnou certifikační autoritou, na jejíž důvěryhodnosti se s druhou stranou dohodneme. Na vyzkoušení elektronického podpisu si můžeme opatřit certifikát několika způsoby. Všechny certifikační autority nabízejí možnost zdarma vystavit certifikát pro testovací účely – stačí vyplnit příslušný formulář na webu. Například pro I.CA lze nalézt tuto možnost na jejím webu [3] (vyžaduje Windows a MS Internet Explorer). Další možností je pak využít služeb certifikační autority CAcert [4]. Ta vám po bezplatné registraci umožní si vystavit téměř libovolný certifikát.

V obou případech budou podpisové klíče vygenerovány pomocí skriptu uvnitř prohlížeče. Ten si pak soukromý klíč uloží a pošle certifikační autoritě žádost o certifikát, na jejímž základě CA certifikát vystaví. Ten pak bude naimportován přímo do prohlížeče. Pokud ho budeme chtít použít pro podepsání nějakého dokumentu, musíme ho z něj nejdříve vyexportovat ve formátu PKCS#12 (soubor s příponou p12 nebo idx). Zároveň vám bude autorita nabízet ke stažení certifikát ve formátu PKCS#7 – přípony pem nebo cer, ten ale obsahuje pouze veřejnou část klíče, takže k podepisování dokumentů nestačí. Ve Firefoxu vyexportujeme certifikát následovně: Menu > Preferences > Advanced > Encryption > View Certificates > zvolte certifikát, Backup. Certifikát opatřete po vyzvání heslem proti zneužití a uložte si ho na disk. V ostatních prohlížečích bude postup podobný.

Případně si můžete klíče, žádost o certifikát i (nedůvěryhodný) certifikát vygenerovat sami na svém počítači. K tomu lze využít například nástroje z balíku OpenSSL [5]. Ty představují velmi silný nástroj umožňující téměř všechny

manipulace s klíči a certifikáty, které můžete potřebovat. Pro někoho může být nevýhodou pouze textové ovládání.

Nyní máme certifikát a můžeme podepisovat. Podepsat lze v podstatě libovolný soubor. Časté a užitečné je to například v případě PDF dokumentů nebo e-mailů. Pro podepisování PDF dokumentů lze využít například jednoduchý prográmek PortableSigner [6]. Ověřit podpis je možné pomocí Adobe Readeru.

V případě e-mailů je situace malinko složitější. Většina větších e-mailových programů (Mozilla Thunderbird, MS Outlook, ...) si s podepisováním dobře poradí. Naopak webová rozhraní freemailů (např. Gmail, Email Seznam.cz, ...) podpisy ověřovat neumí a pouze zobrazí podpis jako přílohu s příponou p7s. Ověřit podpis je ale pak značně komplikované. Podepisovat e-maily v těchto webových rozhraních není možné vůbec.

Ukážeme si nastavení Thunderbirdu. Předpokládejme, že máme nakonfigurovaný e-mailový účet. Zvolte Edit > Preferences > Advanced > Certificates > View Certificates > Your Certificates > Import a vyberte váš certifikát. Možná ještě budete potřebovat importovat kořenový certifikát certifikační autority. To uděláte ve stejném okně, jen v záložce Authorities. Nyní zbývá přiřadit certifikát k účtu. Zvolte Edit > Account Settings > položku Security u vašeho účtu > vyberte certifikát pro Digital Signing. Hotovo. Nyní při psaní zprávy můžeme nahoře kliknout na Security > Encrypt This Message a zpráva se odešle podepsaná. Zkuste si to.

Jak jsme psali výše, RSA lze využít mimo podepisování i k šifrování. Proto pokud máme něčí certifikát s veřejnými klíči (PKCS#7), můžeme data z něj použít i pro šifrování e-mailu. Příjemce pak pomocí svého soukromého klíče zprávu dešifruje. Většina e-mailových klientů to opět udělá automaticky za nás.

Zajímavostí je, že mnoho e-mailových zpráv je elektronicky podepsaných, aniž o tom odesílatel má tušení. Občas zprávy podepisuje i server, který e-mail odesílá (SMTP server), aby ověřil, že je odeslal opravdu on. To může sloužit jako ochrana proti spamu s falešnou adresou odesílatele. Tomuto druhu podpisu se říká DKIM (hledejte položku DKIM-Signature v hlavičce e-mailu) [7]. Oproti běžnému elektronickému podpisu zaručuje obvykle konzistenci celé hlavičky e-mailu. Identifikuje ale SMTP server a ne odesílatele. Takže má smysl oba podpisy kombinovat.

Alternativa: PGP

Alternativou k certifikátům určenou především pro šifrování, ale použitelnou i pro podpis, je standard PGP (resp. OpenPGP). V tomto standardu opět využíváme pro šifrování algoritmus RSA a hešovací funkce. Nejsou zde ale žádné certifikační autority. Každý si své klíče generuje sám a jsou servery, kde mohou všichni sdílet své veřejné klíče.

Pokud tedy někomu chci poslat zašifrovanou zprávu, najdu si v databázi jeho veřejný PGP klíč a použiji ho k šifrování.

Podobně bych mohl používat svůj soukromý klíč pro podpis. Není zde ale certifikační autorita, která přímo ověří, že klíč patří zrovna mně. Místo toho já mohu kohokoli majícího také PGP klíč požádat, aby mi podepsal můj veřejný klíč a potvrdil tím, že můj klíč patří opravdu mně. Pochopitelně by si to měl nejdřív pořádně ověřit. Pokud budu mít klíč podepsaný od dostatečného počtu důvěryhodných osob, může ho příjemce považovat za důvěryhodný. Bývá též zvykem vystavovat veřejné PGP klíče na webových stránkách.

Pěkný návod, jak používat PGP, sepsal Stefan Moser [8]. Návodů k instalaci na všelijakých operačních systémech i různých grafických klientů lze nalézt na webu spoustu. Existuje i rozšíření pro Thunderbird zvané Enigmail.

PGP lze používat pro šifrování (resp. podepisování) e-mailů dvěma způsoby. Buďto se šifruje celá zpráva (mimo hlaviček) podobně jako v případě použití certifikátů, nebo se šifruje jen vlastní tělo dokumentů. To znemožní například používat ve zprávách HTML tagy, ale umožní to používat PGP i třeba ve webových e-mailových rozhraních. Stačí vlastní text zkopírovat a dešifrovat (případně ověřit podpis) pomocí externího programu.

Celkově lze říct, že pro šifrování souborů je vhodnější PGP, pro podepisování spíš využití certifikátů.

Obecně se certifikáty nepoužívají pouze pro podepisování nebo šifrování jednotlivých dokumentů. Můžete se s nimi setkat i v případě šifrovaného připojení na internetu – například protokoly https, sftp nebo ssh jsou založeny na standardu SSL/TLS, který právě certifikáty využívá. Méně často se pak můžeme setkat i s tím, že se uživatel ve webovém rozhraní místo jména a hesla autentizuje pomocí certifikátu. To se občas využívá třeba u elektronického bankovnictví. V takovém případě by certifikát pro autentizaci klienta neměl být z bezpečnostních důvodů používán i pro podepisování dokumentů.

Zkuste si nějaký certifikát ve svém webovém prohlížeči prohlédnout.

Používání šifrování souborů i e-mailů je nejlepší si skutečně vyzkoušet. Pokud byste měli jakékoli otázky nebo problémy, můžete se obrátit na e-mail `jakub.topfer@matfyz.cz`. Pokud budu vědět jak, rád vám pomohu.

Zdroje dalších infromací

[1] Seriál o teorii čísel z 28. ročníku MKS
`http://mks.mff.cuni.cz/archive/28/9.pdf`

[2] Seznam akreditovaných certifikačních autorit MV ČR
`http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx`

[3] Testovací certifikáty I.CA, zvolte „Žádost o testovací certifikát“
`http://ica.cz/Testovani-kvalifikovane`

[4] Certifikační autorita CAcert, po registraci a přihlášení zvolte v menu „Klientské certifikáty“
`http://www.cacert.org/`

[5] OpenSSL – balík nástrojů pro práci s certifikáty a klíči
`http://www.openssl.org/`

[6] PortableSigner – program pro podepisování PDF dokumentů.
`http://portablesigner.sourceforge.net/`

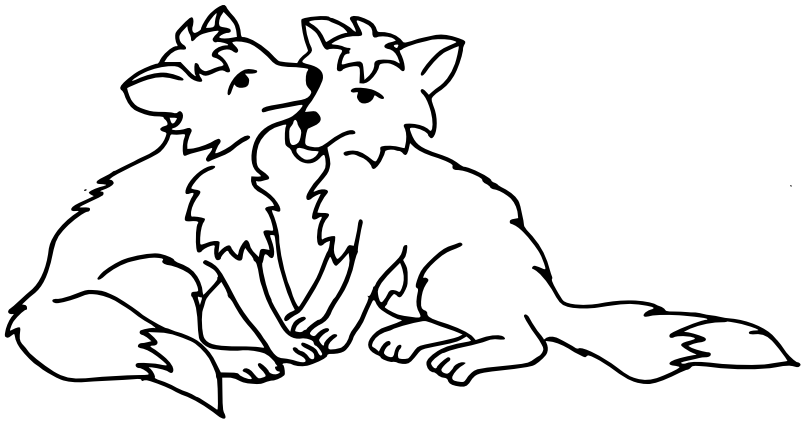
[7] DomainKeys Identified Mail (DKIM) from Wikipedia
`http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail`
[8] Návod na používání PGP nejen pod UNIXem
`http://moser.cm.nctu.edu.tw/gpg.html`

Kuba

Úloha 3.5 – Podepisujeme prakticky (až 4b)

Cílem této úlohy je vyzkoušet si prakticky práci s elektronicky podepsanými dokumenty a certifikáty. Za každou položku je jeden bod, úkoly lze plnit postupně.

- Z adresy `http://mam.mff.cuni.cz/vstupy/19_3_podepsane.pdf` si stáhněte podepsaný PDF dokument. Kdo dokument podepsal? Jaké k tomu použil algoritmy? Čí jsou další certifikáty v certifikační cestě? Pošlete nám sériová čísla všech certifikátů z certifikační cesty.
- Nechte si vygenerovat (případně vygenerujte) certifikát použitelný pro podpis a pošlete ho s řešením. Jaký veřejný klíč používá?
- Pošlete mi na `jakub.topfer@matfyz.cz` vámi elektronicky podepsaný mail.
- Pošlete mi na výše uvedený mail váš veřejný PGP klíč, dostanete zpět zašifrované heslo. Stačí když ho rozšifrujete a pošlete zpět.



Výsledková listina

Poř.	Jméno	R.	$\sum_{-1}$	Úlohy							$\sum_{0}$	$\sum_{1}$
				r1	r2	r3	r4	t1	t2	c		
1.	Bc.ᴹᴹ Filip Homza	4.	18	3	4	3	2	6			18	18
2.	Bc.ᴹᴹ Anna Kufová	1.	17	3	4		1		9		17	17
3–4.	Bc.ᴹᴹ Michal Buráň	4.	13	4	4	2	3				13	13
	Dr.ᴹᴹ Jan Kadlec	2.	61	3		1	1		8		13	13
5.	Bc.ᴹᴹ Aranka Hrušková	3.	12	4		3	2	3			12	12
6–9.	Bc.ᴹᴹ Jakub Kušnír	2.	11	3	1	2	1		4		11	11
	Bc.ᴹᴹ Marian Poljak	1.	11	2	4	3	2				11	11
	Bc.ᴹᴹ Václav Skála	2.	11	2		0	1	1	7		11	11
	Bc.ᴹᴹ Pavel Souček	1.	11	2		3	2	4			11	11
10–12.	Mgr.ᴹᴹ Lubomír Grund	4.	48	3	2	4	1				10	10
	Bc.ᴹᴹ Patrik Nácovský	2.	10	1	2	2	1	4			10	10
	Bc.ᴹᴹ Jiřina Svobodová	3.	10	1	3	2	1	3			10	10
13–16.	Bc.ᴹᴹ Matěj Bidlák	3.	12	3	2	3	1				9	9
	Sabína Fraňová	4.	9	3	2	3	1				9	9
	Mgr.ᴹᴹ Matej Lieskovský	3.	36	3		4	2				9	9
	Karel Ullwer	4.	9	0	0	1	1			7	9	9
17–18.	Zdeněk Garčic	2.	8	3	1	3	1				8	8
	Mgr.ᴹᴹ Aneta Šťastná	3.	49	3		3	2				8	8
19–20.	Mgr.ᴹᴹ Markéta Calábková	2.	26	2	3	2					7	7
	Mgr.ᴹᴹ Ondřej Mička	4.	35	4	3						7	7
21–27.	Jaroslav Cerman	1.	6	1		3	1	1			6	6
	Kristýna Ilievová	2.	6	1	3	1	1				6	6
	Bc.ᴹᴹ Linda Langerová	2.	18	3	3						6	6
	Viktor Skoupý	3.	6	2		3	1				6	6
	Valentína Straková	3.	6	3	2	1					6	6
	Jiří Štábl	2.	6	1	3	1	1				6	6
	Štěpánka Titlová	1.	6	1	1	3	1				6	6
28–30.	Marek Biroš	2.	5	3	0	1	1				5	5
	Mgr.ᴹᴹ Josef Svoboda	4.	29					5			5	5
	Mgr.ᴹᴹ Petr Vincena	2.	32	4			1				5	5

Poř.	Jméno	R.	$\sum_{-1}$	Úlohy r1	r2	r3	r4	t1	t2	c	$\sum_0$	$\sum_1$
31–39.	Eliška Bušáková	4.	7	3			1				4	4
	Mark Daniel	3.	4	3			1				4	4
	Jan Dittrich	1.	4	3			1				4	4
	Jakub Kolář	2.	4	1		2	1				4	4
	Václav Krchňák	1.	4	3			1				4	4
	Patrik Kroft	2.	4	2			2				4	4
	Mgr.ᴹᴹ Jan Mikel	4.	25	4							4	4
	Matěj Vanko	4.	4	2		1	1				4	4
	Rostislav Zlatník	1.	4	0	2	1	1				4	4
40–49.	Mgr.ᴹᴹ Jakub Dolejší	2.	21	1		2					3	3
	Lucie Draslarová	1.	3	1	2						3	3
	Jan Erhart	2.	7	3			0				3	3
	Jan Kučera	1.	3	3							3	3
	Jan Kulička	1.	3	3			0				3	3
	Dominika Macháčová	3.	3	1		1	1				3	3
	Jakub Novák	1.	3	1		0	1	1			3	3
	Dušan Stěhule	2.	3	1		2					3	3
	Kateřina Škorvánková	1.	3	2			1				3	3
	Jan Škvára	3.	3	3							3	3
50–55.	Dávid Barbora	2.	2				2				2	2
	Jitka Fürbacherová	4.	2	1		0	1				2	2
	Jan Knížek	2.	2	2							2	2
	Olga Leskovjanová	2.	2	1	0		1				2	2
	Michal Reška	1.	2	2							2	2
	Dávid Sekáč	2.	2	1	0	1	0				2	2
56–59.	Zuzana Kuchařová	1.	1	1							1	1
	Timotej Mareš	1.	1				1				1	1
	Dávid Princík	4.	1	1		0					1	1
	Michal Šafek	2.	1	1							1	1

Sloupeček $\sum_{-1}$ je součet všech bodů získaných v našem semináři, $\sum_0$ je součet bodů v aktuální sérii a Sloupeček „+“ značí bonusové body udělované podle ročníku a součtu bodů za úlohy. Tituly uvedené v předchozím textu slouží pouze pro účely M&M.

Adresa redakce:

M&M, OVVP, UK MFF
Ke Karlovu 3
121 16 Praha 2

Telefon: +420 221 911 235
E-mail: `mam@matfyz.cz`
WWW: `http://mam.mff.cuni.cz`

Časopis M&M je zastřešen Oddělením pro vnější vztahy a propagaci Univerzity Karlovy, Matematicko-fyzikální fakulty a vydáván za podpory středočeské pobočky Jednoty českých matematiků a fyziků.