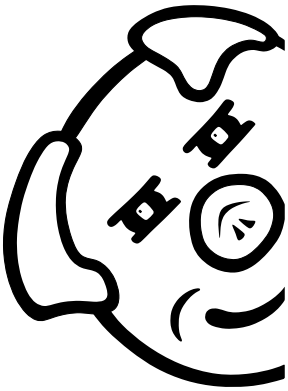
Matematický korespondenční seminář

Milý příteli !



Máme za sebou první sérii 33. ročníku Matematického korespondenčního semináře, jejíž řešení nám poslalo neuvěřitelných 185 řešitelů. V čele výsledkové listiny se kromě známých jmen objevili i úplní nováčci a je patrné, že letos půjde o vskutku tuhý matematický boj. Ve hře je účast na jarním soustředění a jiné zajímavé ceny!

Za organizátory zdraví

Alexander „Olin“ Slávik

Co je dále v komentářích?

- Jak řešit úlohy korespondenčního semináře?
- Poznámky k bodování a výsledkovým listinám
- Povídání ke třetí podzimní sérii
- Povídání ke čtvrté podzimní sérii
- Vzorové řešení 1. podzimní série
- Seriál – Teorie čísel I
- Výsledková listina 1. podzimní série
- Příloha: Zadání 3. a 4. podzimní série a 1. seriálové série

Řešení úloh

Kromě komentářů si nezapomeň pročíst i svá opravená řešení a porovnat je se vzorovými. Pokud jsi v nich napáchal chyby, máš teď jedinečnou příležitost se z nich poučit.

Pro snazší pochopení jsme pro Tebe navíc připravili krátký text **Jak řešit úlohy korespondenčního semináře**. Vřele Ti doporučujeme jeho přečtení, zvláště pak v případě, že řešit začínáš a nemáš ještě s matematickými úlohami mnoho zkušeností. Věříme, že Ti pomůže lépe porozumět zadáním a usnadní Ti sepisování řešení.

Anglická série

V podzimní části semináře se 4. série od ostatních odlišuje. Její zvláštnost tkví v tom, že je zadána výhradně v anglickém jazyce. Stejně tak **řešení přijímáme sepsaná pouze v anglickém jazyce**. Řešení napsaná česky nebo slovensky nebudou obodována. Možná Ti překlad a vlastní sepisování zabere více času než obyčejně, ale věz, že angličtina je jazyk, ve kterém se „dělá“ většina matematiky, a cizojazyčná série je tak příležitost, jak se něčemu přiučit.

Také úvodní text k této sérii je napsán anglicky, takže pokud jsi doposud s matematickou angličtinou nepřišel do styku, můžeš z něj odpozorovat používané konstrukce a fráze.

Korespondenční seminář
KAM MFF UK
Malostranské náměstí 25
118 00 Praha 1

TR*i*KS

Za touto zkratkou se skrývá Trénink v rychlosti semináře *i*KS,[1] což je nová online soutěž v rychlém řešení matematických úloh. Primárně je určena jako trénink pro středoškoláky na Matematickou olympiádu, ale účastnit se může kdokoliv. Vše potřebné nalezneš na adrese *iksko.org/triks*.

Den otevřených dveří

Rádi bychom Tě pozvali na Den otevřených dveří na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze, který se koná ve čtvrtek **28. listopadu 2013**. Další podrobnosti najdeš na fakultních stránkách *www.mff.cuni.cz*.

Na této akci se dozvíš spoustu informací o studiu na MFF UK v Praze, prohlédneš si budovy a pracoviště fakulty a budeš mít možnost navštívit zajímavé přednášky. Můžeš se také seznámit s dalšími aktivitami pořádanými fakultou pro středoškoláky. V neposlední řadě se zde setkáš s organizátory MKS a jiných seminářů či táborů.

Noví organizátoři MKS

Jak se již stalo tradicí, každým rokem se řady organizátorů rozšiřují o nové členy. Letos byla obzvláště bohatá úroda – zavítala mezi nás nová PraSátka Michal Buráň, Ondřej Cífka, Martin Čech, Anička Doležalová, David Hruška, Bára Kociánová, Marta Kossaczká, Lucka Magurová, Pepa Svoboda, Martin „E. T.“ Sýkora a Štěpán Šimsa, která společně s těmi staršími opravila Tvé vyřešené úlohy.

[1] *i*KS je korespondenční seminář, na jehož organizaci spolupracují organizátoři MKS a slovenského Korešpondenčného matematického seminára. Další informace najdeš na stránkách *www.iksko.org*.

Jak řešit úlohy korespondenčního semináře?

Tento text je primárně určen méně zkušeným řešitelům. Jeho cílem je v krátkosti popsat způsob uvažování a vyjadřování, bez kterého se při řešení matematických úloh nelze obejít.

Pokud se rozhodneš řešit úlohy korespondenčního semináře, nestačí je pouze vypočítat. Body získáš jen v případě, že svůj postup nějak rozumně dostaneš na papír. Je tedy dobré si uvědomit, co se vlastně s řešením děje poté, co jej odešleš. Dostane ho do ruky nedůvěřivý opravovatel, jehož snahou je jej pochopit a nechat se přesvědčit o jeho správnosti. Není to tedy jako opravování kvízových otázek, u nichž se dá rychle ověřit, zda byly zodpovězeny správně. Zkus si proto svá řešení přečíst očima někoho, kdo zadanou úlohu vidí poprvé v životě.

Co po Tobě úloha chce?

Úloha často vybízí *„Dokažte!“*, *„Ukažte!“*, *„Zdůvodněte!“*. To znamená, že chceme, abyste ze zadání vyvodili dokazované tvrzení pomocí logických kroků podložených pádnými argumenty. Nestačí tedy nakreslit obrázek, v němž úhel ze zadání vyjde pravý, či ověřit platnost nerovnosti na kalkulačce nebo na počítači pro 150 různých hodnot. Je totiž potřeba ukázat, že tvrzení platí pro všechny možné konstelace, kterých je obvykle nekonečně mnoho.

Jiné úlohy na řešitele apelují *„Rozhodněte!“*, například *„rozhodněte, zda platí“*, *„rozhodněte, kdo má vyhrávající strategii“* nebo *„rozhodněte, které z čísel je větší“*. Samotné rozhodnutí nestačí, je třeba jej zdůvodnit. To znamená tvrzení dokázat, případně najít protipříklad.

Často se setkáš s úlohami typu *„Najděte!“*, *„Najděte všechny . . . !“*. V prvním případě stačí, když najdeš nějaké vyhovující řešení. Je potřeba ukázat, že odpovídá požadavkům v zadání, ale už není potřeba se zabývat dalšími řešeními. Druhý případ je složitější, neboť tehdy je potřeba najít všechna vyhovující řešení, a navíc dokázat, že žádné jiné už neexistuje. Obměnou může být například *„Najděte nejmenší . . . !“*, kde je potřeba najít řešení a ukázat, že menší neexistuje.

Co nemáme rádi?

Do řešení piš jasná tvrzení a zdůvodňuj je. Zadání opisovat nemusíš. Pokud tvrdíš něco, co není pravda, pak je to ideální příležitost pro opravovatele strhnout Ti body. Navíc to, co z nepravdivého tvrzení vyvodíš, nejspíš také neplatí. Máš-li hypotézu, kterou neumíš dokázat, přiznej, že je to hypotéza. Sice pravděpodobně nedostaneš plný počet bodů, ale opravovatel bude rád, že nemusí ve Tvém řešení zbytečně hledat vysvětlení.

Dej si pozor na následující formulace:

• *„je zřejmé“*, *„je vidět“* – Tyto obraty lze v řešení použít. Řešitelé je ale často používají v případech, kdy daná věc není vůbec zřejmá, ba dokonce, když neplatí.

• *„provedeme analogicky“* – Tuto formulaci můžeš použít pouze v případě, že stačí v předchozích argumentech lehká změna značení. Analogie rozhodně neznamená zobecnění, například z důkazu pro 3 nelze takto vyrobit důkaz pro 50, či dokonce pro obecné n.

• *„z obrázku je patrné“* – Obrázky jsou velmi dobré k tomu, aby se opravovatel lépe orientoval v řešení a mohl jej snáze pochopit. Postup by však měl být srozumitelný i bez něj, nikdy se na něho neodkazuj jako na nedílnou součást řešení. Pokud v obrázku zavedeš nějaké značení, měl bys ho vysvětlit v textu, ne ho jen začít používat.

• *„stačí prozkoumat nejhorší variantu“* – Sice by to mohlo stačit, ale dokud neprozkoumáme všechny varianty, nelze říct, že tato konkrétní je nejhorší. Můžeme si to myslet, ale musíme to dokázat. Stejný problém nastává i u dalších formulací (*„nejlepší bude, když“* a podobně).

Pokud tedy některou z těchto frází používáš, rozmysli si, zda se nejedná o jeden z výše uvedených nešvarů.

Co a jak dokazovat?

V této sekci se nejprve podíváme, jak správně interpretovat zadání, a poté uvedeme některé základní důkazové techniky, které můžeš ve svých řešeních použít.

Důkaz by měl vycházet z předpokladů a postupovat k závěrům úlohy. Dej si pozor, abys během řešení nepoužil něco, co nevyplývá z předpokladů nebo předchozích úvah, zejména ne dokazované tvrzení!

• *„jestliže, pak“, „pokud, pak“, „Dokažte, že pokud platí A, pak platí B.“* – Kdykoliv se v zadání vyskytne věta tohoto typu, znamená to, že A je předpoklad (to, z čeho vycházíme a co můžeme při řešení používat), zatímco B je závěr (to, co chceme dokázat).

Předpoklad a závěr nesmíš za žádných okolností zaměnit! Srovnej následující tvrzení:

> Jestliže je číslo dělitelné čtyřmi, pak je sudé. (platí)
> Jestliže je číslo sudé, pak je dělitelné čtyřmi. (neplatí, např. pro 2)

• *„právě když“, „právě tehdy, když“, „tehdy a jen tehdy, když“, „Dokažte, že A platí právě tehdy, když platí B.“* – V tomto případě se vlastně jedná o dvě úlohy. Je totiž potřeba dokázat následující dvě tvrzení:

(i) Pokud platí A, pak platí B.
(ii) Pokud platí B, pak platí A.

Platnost tvrzení se nezmění, když A a B prohodíme, viz následující příklad.

> Dané číslo je dělitelné deseti, právě když jeho poslední cifrou je nula.
> Poslední cifrou daného čísla je nula, právě když je dělitelné deseti.

Důkazových technik je mnoho a my si zde ukážeme dvě základní – přímý důkaz a důkaz sporem.

V přímém důkazu postupujeme od předpokladů, z nichž logickými úvahami vyvozujeme dílčí závěry, až dospějeme ke kýženému výsledku. Naproti tomu v důkazu sporem si na začátku představíme, co by se stalo, kdyby tvrzení neplatilo, a z tohoto předpokladu pak odvodíme evidentně neplatné tvrzení (spor). Použití této techniky si ukážeme na příkladu:

Příklad. Dokažte, že každé prvočíslo větší než 2 je liché.

Řešení. Pro spor předpokládejme, že jsme našli sudé prvočíslo p větší než 2. Dvojka je jeho dělitel, který není roven ani jedné, ani p. To je spor s předpokladem, že p je prvočíslo. Dokazované tvrzení tedy platí.

Význam výrazů

Když matematik napíše vzoreček, nepředstavuje si pod ním nic jiného než běžné tvrzení. Pro úpravy výrazů, rovnic apod. tedy platí stejná pravidla jako pro obyčejné dokazování.

Definuj všechny proměnné, které ve vzorečcích používáš a nejsou v zadání. Opravovatel jinak těžko pozná, co jsi jimi chtěl říct. Se značením to však není třeba přehánět, a proto si označ vždy jen to, co v řešení budeš potřebovat. Příliš mnoho písmenek přehlednosti neprospívá.

Dále připomínáme, že je v důkazu třeba vycházet z předpokladů, ne z dokazovaného tvrzení. To ukážeme na příkladu:

Příklad. Dokažte, že pro libovolná kladná čísla a, b platí $\sqrt{ab} \leq (a+b)/2$.

Správné řešení může vypadat takto:

Řešení. Kdykoli umocníme reálné číslo na druhou, získáme nezáporné číslo. Tedy

$$\begin{aligned} 0 &\leq (\sqrt{a}-\sqrt{b})^2 = a - 2\sqrt{ab} + b, \\ 2\sqrt{ab} &\leq a + b, \\ \sqrt{ab} &\leq \frac{a+b}{2}, \end{aligned}$$

což jsme chtěli dokázat.

Jiná možnost je tato:

Řešení. Pro spor předpokládejme, že máme dvojici čísel a, b, pro která tvrzení neplatí, tedy $\sqrt{ab} > (a+b)/2$. Pak ovšem

$$\begin{aligned} ab &> \frac{(a+b)^2}{4}, \\ 4ab &> (a+b)^2 = a^2 + 2ab + b^2, \\ 0 &> a^2 - 2ab + b^2 = (a-b)^2. \end{aligned}$$

To je spor, neboť umocněním reálného čísla nemůžeme dostat záporné číslo. Dokazované tvrzení tedy platí.

Oba tyto postupy byly v pořádku. První (přímý) důkaz vycházel pouze ze známých faktů a dobral se kýženého výsledku, druhý důkaz (sporem) předpokládal neplatnost tvrzení a došel k něčemu, co neplatí.

K řešení ale není možné přistupovat zcela přímočaře, tedy jen upravovat dokazovaný vzoreček. To proto, že jakmile do řešení napíšeš $\sqrt{ab} \leq (a+b)/2$, znamená to, že již předpokládáš, že daná nerovnost platí. Jenže to nemůžeš předpokládat, neboť Tvým cílem je to teprve dokázat.

Uveďme ještě jeden příklad, na kterém si ukážeme dvě různá použití proměnných.

Příklad. V závislosti na parametrech a, b, c vyřešte kvadratickou rovnici $ax^2 + bx + c = 0$.

Zadání říká, že pro libovolná, ale pevně zvolená čísla a, b, c hledáme všechna x, která vyhovují zadané rovnici. Proměnné a, b, c označují v celém příkladu stále tatáž tři (ne nutně různá) reálná čísla. Každá konkrétní volba parametrů vlastně určuje jinou úlohu, ale přitom chceme vyřešit všechny tyto úlohy naráz, obecně. Proměnná x hraje zcela odlišnou roli – její hodnota je neznámá a naším cílem je ji určit.

Používání známých tvrzení

Může se stát, že v literatuře nebo na internetu narazíš na tvrzení, které Ti usnadní řešení úlohy. Pokud je to nějaká věta, která má jméno (například Cevova věta), nezapomeň její název do řešení uvést. Pravděpodobně ji budeme znát, a když ne, dovedeme ji alespoň najít. Důkaz přitom opisovat nemusíš. V případě, že se jedná o nepojmenované tvrzení, napiš nám zdroj, kde jsi ho našel.

Vzorová řešení

V neposlední řadě bychom Tě chtěli povzbudit k řešení našich úloh. Pokud náš seminář vidíš poprvé, nedej se odradit případnými počátečními neúspěchy. Prostuduj si svá opravená řešení a nezapomeň se podívat také na vzoráky. Vzorové řešení Ti má často co nabídnout i tehdy, když jsi úlohu vyřešil správně. Můžeš v něm najít různé zajímavé přístupy či myšlenky, a něco nového se tak naučit. V poznámkách opravovatele si pak můžeš přečíst, jak se s řešením potýkali ostatní.

Věříme, že Ti tento text usnadní řešení úloh v semináři i jinde a pomůže Ti osvojit si základy matematického uvažování. To, co se naučíš, není jen schopnost řešit matematické úlohy, ale také schopnost samostatně hlouběji přemýšlet. To se Ti určitě bude někdy hodit, a to i tehdy, když se matematikou dále zabývat nebudeš.

Přejeme Ti mnoho radosti při objevování tajů matematiky!

Poznámky k bodování a výsledkovým listinám

Nejprve se zaměříme na jednu zvláštnost našeho semináře. Protože opravování úloh je komplexní záležitost, jsou komplexní i body, které obdržíte od opravovatelů. Každé řešení ohodnotíme číslem tvaru $x + yi$, kde x představuje reálné body a y jsou body imaginární. Jaký je mezi nimi rozdíl? Reálné body jsou „solidní“; jsou to body za správnost řešení, které obvykle dostáváte ve škole, na olympiádách a podobně. Jde o nezáporné celé číslo. Za naprosto správné řešení jich dostanete tolik, kolik činí bodové ohodnocení dané úlohy.

Imaginární body představují druhou, nezávislou stupnici. Vyjadřují míru elegance daného řešení. Hodnota y je celé číslo od -2 do 2. Kladné imaginární body značí řešení, které je radost číst: obsahuje šikovné triky a originální myšlenky nebo nachází souvislosti mezi zdánlivě vzdálenými pojmy. Naopak záporné imaginární body vyjadřují, že jsi někde použil zbytečně složité formulace, několikrát dokazoval totéž, všechno řešil hrubou silou nebo třeba napsal jednoduchý důkaz na pět stránek.

Od komplexních bodů k výslednému hodnocení

Každou úlohu tedy hodnotíme komplexním číslem ve tvaru $x + yi$. Do výsledků celé série pak započítáme hodnocení pěti úloh, které jsi vyřešil nejlépe (měl jsi z nich nejvíce reálných bodů, v případě rovnosti rozhoduje počet imaginárních bodů). Hodnocení těchto příkladů sečteme a tím dostaneme komplexní číslo, které označíme b.

S číslem b se dále pracuje následovně: Nejprve vypočteme *hrubý bodový zisk* – to je reálné číslo, se kterým ve výpočtu všude dále pracujeme namísto komplexního čísla, kterým byly Tvé úlohy ohodnoceny opravovateli. Při zisku b bodů za sérii je výchozí hodnota hrubého bodového zisku dána vztahem[2]

$$\tilde{h} = \Re(b) + \left(2 - \sqrt{3}\right) \Im(b).$$

Jelikož by toto číslo mohlo být teoreticky záporné nebo větší, než je maximální počet bodů za sérii (označíme ho s, obvykle je $s = 25$), „ořízneme“ výchozí hodnotu do tohoto intervalu:

$$h = \begin{cases} s & \text{pokud } \tilde{h} \geq s, \\ 0 & \text{pokud } \tilde{h} \leq 0, \\ \tilde{h} & \text{jinak.} \end{cases}$$

Aby byli při bodování úloh mírně zvýhodněni mladší a začínající řešitelé, určuje se u každého řešitele tzv. *koeficient*. Jeho výchozí hodnota se vypočte následovně:

$$\tilde{\kappa} = (r - 1) + \frac{2z}{450},$$

kde r je ročník[3] (přepočítaný tak, aby odpovídal čtyřletému gymnáziu, studenti a žáci plnící povinnou školní docházku mají $\frac{1}{2}$) a z je počet počet bodů, které řešitel získal během předchozích ročníků.[4] Jelikož výsledný koeficient $\tilde{\kappa}$ je vždy číslo z intervalu $\langle -\frac{1}{2}, 6\rangle$, položíme $\kappa = \min(\tilde{\kappa}, 6)$.

Předpokládejme dále, že $\kappa < 3$. Pro další výpočet bude podstatné číslo t definované jako

$$t = \frac{s}{2}\left(1 + \sqrt{3}\,\mathrm{tg}\,\frac{\kappa\pi}{6}\right).$$

[2] Symboly $\Re(w), \Im(w)$ značí reálnou a imaginární část komplexního čísla w.

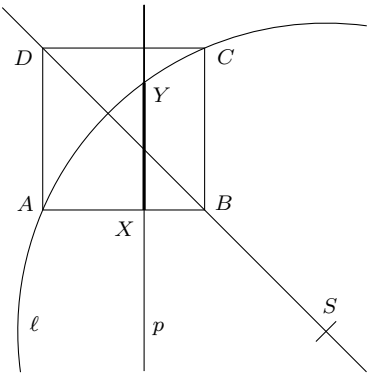
[3] Pokud máš ve výsledkové listině uvedený čtvrtý (maturitní) ročník, a přitom jsi mladší, je to nejspíše proto, že nám nedošla informace o Tvém ročníku. Napravit to můžeš buď mailem na *mks@mff.cuni.cz*, nebo přiložením svých údajů k řešením další série.

[4] V minulých letech se při výpočtu koeficientu zohledňovalo i zaměření třídy řešitele. Počínaje loňským ročníkem se již tento údaj nezapočítává.

Hledaný *výsledný bodový zisk* za sérii (což už je číslo, které se udává ve výsledkové listině) pak dostaneme podle vztahu

$$v = \sqrt{t^2 + (s+t)^2 - (s+t-h)^2} - t.$$

Jak toto číslo interpretovat geometricky? Uvažujme v rovině čtverec $ABCD$ o straně s. Na přímku BD vyneseme bod S ve vzdálenosti $\sqrt{2}\,t$ od bodu B, přičemž celá úsečka BS je vně čtverce. Dále nechť je dána kružnice ℓ o středu S procházející body A a C. Na úsečce AB najdeme bod X takový, že $|AX| = h$, a povedeme jím kolmici p ($p \perp AB$). Kružnice ℓ a přímka p se protnou ve dvou bodech, ten uvnitř čtverce označíme Y. Výsledný bodový zisk za sérii je $v = |XY|$.



V případě, že $\kappa > 3$, postupujeme takto: číslo t se nyní zvolí jako

$$t = \frac{s}{2}\left(1 + \sqrt{3}\,\mathrm{tg}\,\frac{(6-\kappa)\pi}{6}\right)$$

a výsledný bodový zisk je

$$v = s - \left(\sqrt{t^2 + (s+t)^2 - (t+h)^2} - t\right).$$

Tento vzorec lze interpretovat tak, že kružnice ℓ je obrazem kružnice získané dle postupu uvedeného výše pro koeficient $6-\kappa$ v osové souměrnosti podle osy AC, jinak zůstává postup stejný.

Nakonec zbývá případ $\kappa = 3$ – tehdy je prostě $v = h$. Lze si to představit tak, že střed S je „v nekonečnu“, tudíž se kružnice změnila na přímku AC.

Další detaily a statistiky úloh

Kromě výsledného bodového zisku lze ve výsledkové listině najít i další údaje. Je v ní po řadě uvedeno jméno, příjmení, třída, zkratka školy, reálné body za jednotlivé příklady a celkové body za sérii.

Do závěrečného hodnocení se počítají všechny série, takže se vyplatí poslat z každé série byť jen jedinou úlohu. Co se naopak nevyplatí, je poslat řešení pozdě: jak ses mohl již v minulých letech přesvědčit, netolerujeme žádné zpoždění! Tedy pokud pošleš své řešení pozdě, sice Ti ho opravíme, ale body za něj nečekej.

Jak řešili úlohu ostatní, se můžeš dozvědět z výsledkové listiny. Abychom Ti však usnadnili toto zjišťování, uvádíme u řešení úloh statistická čísílka o došlých řešeních. Je to čtveřice čísel,

z nichž první říká, kolik lidí řešilo tuto úlohu, druhé, kolik lidí získalo alespoň dva body, třetí průměr udělených reálných bodů a čtvrté pak jejich medián (ten dostaneme tak, že seřadíme počty bodů za jednotlivá řešení podle velikosti a vezmeme číslo na prostřední pozici[5]).

[5] Pokud je čísel sudý počet, vezmeme aritmetický průměr dvou prostředních čísel.

Povídání k třetí podzimní sérii

Třetí podzimní série prověří Tvoji zdatnost v práci s funkcemi. Tento text by Ti měl pomoci zorientovat se v zadáních úloh a osvětlit některé důležité pojmy. Pokud však zadáním rozumíš už teď, není třeba jej číst příliš podrobně.

Co je funkce?

Pravděpodobně nejnázornější pohled na funkce (někdy též zvané *zobrazení*) je ten, že funkci vnímáme jako tajemnou černou krabičku. Tato krabička přijímá nějaké vstupy[6] a v závislosti na tom, jaký vstup dostane, vydá výstup. Množinu všech vstupů funkce f nazýváme *definičním oborem* a značíme zpravidla D_f nebo $D(f)$, množinu všech výstupů nazýváme *oborem hodnot* a značíme H_f nebo $H(f)$.

Formálněji můžeme říci, že funkce $f\colon X \to Y$ je přiřazení, v němž každému $x \in X$ odpovídá právě jedno $y \in Y$.[7] Tento zápis nám tedy prozrazuje, že funkce f je definována na celém X ($D(f) = X$). O tom, jestli tato funkce nabývá všech hodnot z Y, ovšem nic neříká.

Rovností funkcí $f = g$ rozumíme, že $D(f) = D(g)$ a zároveň $f(x) = g(x)$ pro všechna x z definičního oboru. Rovnost $f(x) = g(x)$ přitom znamená, že funkční hodnoty v bodě x jsou u obou funkcí stejné.

Definujeme-li funkci předpisem, musíme uvádět její definiční obor vždy, když není zřejmý z kontextu. Pokud tedy napíšeme pouze $f(x) = x^2$, nedefinujeme tím žádnou funkci, neboť o x nic nevíme. Dále je dobré si uvědomit, že funkce není totéž, co předpis funkce. Uvážíme-li například

$$f(x) = x^2 - 1,\ x \in \mathbb{R}, \qquad g(x) = (x+1)(x-1),\ x \in \mathbb{R},$$

vidíme, že ačkoliv se předpisy těchto dvou funkcí liší, platí $f = g$.

Některé funkce navíc vůbec nemusejí být dány vzorcem. Takovou funkcí může být třeba $f\colon \mathbb{R} \to \mathbb{Z}$, která každému reálnému číslu přiřadí počet sedmiček v jeho desetinném zápisu, pokud jich je konečně mnoho, a -1 v opačném případě.

Vlastnosti funkcí

U funkcí rozlišujeme různé vlastnosti, jejichž znalost nám mnohdy může značně pomoci při řešení úloh. Zde je uveden seznam těch, se kterými se shledáváme nejčastěji. Funkce $f\colon X \to Y$ je

(i) *rostoucí*, pokud pro každá dvě $x, y \in X$ taková, že $x > y$, platí $f(x) > f(y)$,
(ii) *klesající*, pokud pro každá dvě $x, y \in X$ taková, že $x > y$, platí $f(x) < f(y)$,
(iii) *neklesající*, pokud pro každá dvě $x, y \in X$ taková, že $x > y$, platí $f(x) \geq f(y)$,
(iv) *nerostoucí*, pokud pro každá dvě $x, y \in X$ taková, že $x > y$, platí $f(x) \leq f(y)$,
(v) *monotónní*, pokud je nerostoucí nebo neklesající,

[6] Těm formálněji říkáme *argumenty*.

[7] Písmena X, Y značí nějaké (libovolné) množiny. My si ale vystačíme s běžně používanými číselnými množinami, jimiž jsou například přirozená nebo reálná čísla.

(vi) *periodická*, pokud existuje kladné reálné číslo t takové, že pro všechna $x \in X$ platí $x \pm t \in X$ a zároveň $f(x) = f(x+t)$,[8]
(vii) *sudá*, pokud pro každé $x \in X$ platí $-x \in X$ a zároveň $f(x) = f(-x)$,
(viii) *lichá*, pokud pro každé $x \in X$ platí $-x \in X$ a zároveň $f(x) = -f(-x)$,
(ix) *prostá*, pokud nabývá každé hodnoty nejvýše jednou, tedy pokud pro každá dvě $x, y \in X$ taková, že $x \neq y$, platí $f(x) \neq f(y)$,
(x) *na*, pokud nabývá každé hodnoty z Y alespoň jednou, tedy pokud pro každé $z \in Y$ existuje $x \in X$ takové, že $f(x) = z$,
(xi) *bijekce*, pokud je prostá a zároveň na, tedy pokud nabývá každé hodnoty z množiny Y právě jednou.

Abychom se s výše uvedenými pojmy seznámili, vyřešíme si následující příklad.

Příklad. Dokažte, že periodická funkce nemůže být rostoucí.

Řešení. Předpokládejme, že funkce f je periodická s nějakou periodou t. Dále si zvolme libovolné x_0 z definičního oboru funkce f. Protože t je kladné číslo, platí $x_0 + t > x_0$. Zároveň ale z definice periodické funkce vyplývá, že $f(x_0 + t) = f(x_0)$. Tedy f nemůže být rostoucí.

Skládání funkcí

Při práci s funkcemi se můžeme setkat s pojmem *skládání funkcí*. Abychom si tento termín vysvětlili, opět se vrátíme ke „krabičkovému modelu funkcí“. Předpokládejme, že máme dvě krabičky (funkce) takové, že výstupy jedné fungují jako vstupy té druhé, ze které vycházejí nějaké finální výstupy. Tyto dvě funkce se tedy dohromady chovají jako jedna samostatná funkce. Tomuto „zapojování funkcí za sebe“ říkáme skládání.

Poněkud formálněji se můžeme na skládání funkcí dívat takto: Mějme funkce $f\colon A \to B$, $g\colon B \to C$ a definujme funkci $g \circ f$ předpisem $(g \circ f)(x) = g(f(x))$,[9] přičemž definičním oborem této funkce je množina A. Funkci $g \circ f$ nazýváme složenou funkcí.

Povšimni si ale, že vnitřní funkce musí zobrazovat do definičního oboru vnější funkce. Kdybychom tedy chtěli složit $f \circ g$, musela by být množina C podmnožinou množiny A.

Dále je důležité si uvědomit, že $f \circ g$ není totéž jako $g \circ f$. Položme $f\colon \mathbb{R} \to \mathbb{R}; f(x) = x^2$, $g\colon \mathbb{R} \to \mathbb{R}; g(x) = x - 1$. Pak pro každé reálné x máme $(f \circ g)(x) = (x-1)^2$, zatímco $(g \circ f)(x) = x^2 - 1$. Tedy například $(f \circ g)(0) = 1 \neq -1 = (g \circ f)(0)$.

Funkcionální rovnice

Bavíme-li se o funkcionálních rovnicích, máme na mysli rovnice, v nichž jsou neznámými funkce, nikoliv čísla. Jinak řečeno, hledáme funkce (resp. jejich předpisy) takové, že pro všechna možná čísla z nějaké množiny platí zadaná rovnost. Obecný postup řešení těchto rovnic neexistuje, většinou ale postupujeme v několika základních krocích. Prvním z nich je předpoklad, že nějaká funkce f je řešením naší rovnice. Druhým je zjišťování vlastností této funkce za pomoci dané rovnice (většinou tak, že dosazujeme konkrétní hodnoty). Posledním, často opomíjeným krokem je ověření, že námi nalezená funkce je opravdu řešením dané rovnice. Pro objasnění si vyřešme dva ilustrační příklady:

Příklad. Najděte všechny funkce $f\colon \mathbb{R} \to \mathbb{R}$ splňující pro všechna reálná x, y vztah

$$f(xy) = yf(x).$$

[8] Číslo t se pak nazývá *periodou* funkce f.
[9] Právě kvůli tomuto předpisu říkáme funkci, do které vstupují x, *vnitřní* a té druhé *vnější*.

Řešení. Předpokládejme, že funkce f je řešením dané rovnice. Zadaný vztah má platit pro všechny dvojice x, y, takže musí speciálně platit pro ty dvojice, v nichž je $x = 1$, neboli

$$f(1 \cdot y) = yf(1),$$
$$f(y) = yf(1).$$

Úprava, kterou jsme právě udělali, není ekvivalentní, protože zkoumá pouze jeden konkrétní případ $x = 1$. Může tedy existovat funkce, která neřeší naši rovnici, ale tomuto konkrétnímu případu vyhovuje. Proto musíme při řešení funkcionálních rovnic vždy provádět zkoušku.

Teď, poučeni o nutnosti zkoušky, pokračujme v řešení. Protože $f(1)$ je nějaké (neměnné) reálné číslo, můžeme jej označit $c = f(1)$ a psát $f(y) = cy$. Nyní stačí zjistit, pro která c je funkce $f(y) = cy$ opravdu řešením. Dosazením do původní rovnice dostáváme:

$$f(xy) = yf(x),$$
$$c \cdot xy = y \cdot cx,$$

což platí pro všechna reálná c. Řešením jsou tedy všechny funkce tvaru $f(x) = cx$, kde c je nějaké pevné reálné číslo.

Možná Tě překvapilo, že jsme na konci řešení nedělali zkoušku. Ve skutečnosti jsme ji ale provedli, byť poněkud skrytě, v posledním kroku.

Příklad. Nalezněte všechny funkce $f\colon \mathbb{R} \to \mathbb{R}$ vyhovující pro všechna $x, y \in D(f)$ rovnici

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

Řešení. Předpokládejme, že funkce f vyhovuje zadání, a do rovnice dosaďme $y = 1$. Po úpravě získáme $f(x) = x + f(1)$. Tedy $f(x)$ je tvaru $x + c$, kde c je reálné číslo. Nyní už nám zbývá jen zjistit, pro která c je funkce $f(x) = x + c$ řešením. Víme, že pro všechna x, y má být splněn vztah $f(xy) = x + f(y)$, tedy:

$$xy + c = x + y + c,$$
$$xy = x + y.$$

Tento výraz však neplatí pro všechna reálná čísla x, y, takže námi nalezená funkce neřeší rovnici pro žádné reálné c. Zadaná rovnice tedy nemá řešení.

Pro hlubší seznámení s tématem funkcionálních rovnic doporučujeme prostudovat nějaký z textů k sérii na téma funkcionální rovnice z minulých ročníků (ty je možné nalézt v sekci našich stránek „minulé ročníky“), nebo nějaký z příspěvků o funkcionálních rovnicích v knihovně na našich internetových stránkách.[10]

[10] *http://mks.mff.cuni.cz/library/FunkcionalniRovniceVM/FunkcionalniRovniceVM.pdf*

Minima and Maxima – Introduction

This text aims to give you a basic grasp of what a typical solution of a problem involving minima or maxima should look like and warn about common mistakes. Perhaps the most instructive way of doing so is through an example.

Problem. Find the largest number of chess knights that can be placed on an 8×8 chessboard so that no knight is attacked by another knight.

Solution. The first step in attacking such problems is usually to "guess" the desired number.[11] In this case it might consist of trying various configurations of knights, observing conditions on them etc.

We may notice that if two knights attack each other, then they are necessarily placed on squares with different colors, thus by filling all the light (or all the dark) squares with knights gives a valid configuration of 32 knights. Since this seems like a promising number, let us try to prove that it is indeed the maximum. We have to show two separate propositions:

(i) that we are really able to distribute 32 knights on the chessboard in accordance with the given condition, and

(ii) that whenever we place at least 33 knights, there will be at least two of them attacking each other.

Concerning the proposition (i), we do not have much work left: We have already described one suitable placement in the previous paragraph. However, keep in mind that the solution of any minima/maxima problem is incomplete without providing an example (or at least proving the existence) of a situation in which the extremum is attained.

The proposition (ii) is more challenging. Seeing the configuration from (i), one might try to argue that we have placed the knights in "the best possible way", and hence there is no way to place more than 32 of them. Unfortunately, showing something like that is usually very difficult and the reasoning based on "best ways" is *almost never* correct.

A better approach is to examine a situation with too many knights and derive a contradiction. Consider a division of the chessboard into eight 2×4 rectangles. Observe that when there are more than 32 knights, one of these rectangles has to contain at least five of them. But in every such rectangle, each knight attacks exactly one square, thus each "covers" two squares out of eight. We infer that every rectangle can hold at most four non-attacking knights, contradicting the observation above.

The propositions (i) and (ii) together imply that 32 is indeed the sought largest number.

We hope that reading this short introduction helps you deal with any minima/maxima problems and wish you good luck in solving the problems of the 4th autumn series!

[11] Of course, this step is omitted if the problem already says what the sought extreme value is; that would be the case if the problem above was formulated like "Prove that the largest number of chess knights (...) is 32."

Čtverečkovaný papír

1. podzimní série — Vzorové řešení

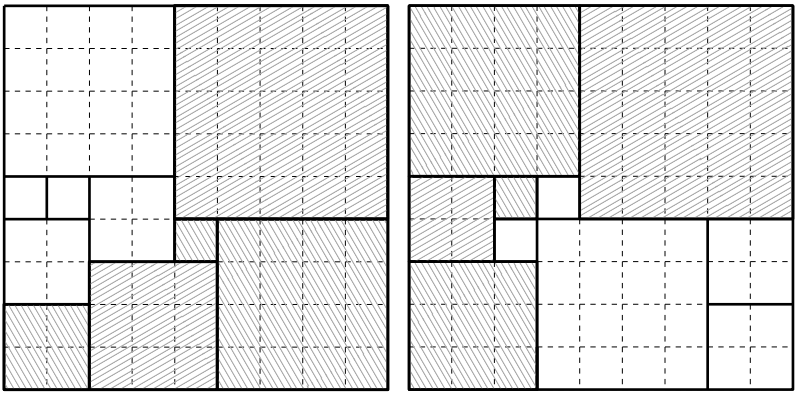
Úloha 1. (180; 168; 2,81; 3,0)

Anička našla o hodině v penálu čtverečkovaný papír 9×9, i rozhodla se ho po čarách rozstříhat na několik čtverců. Chtěla, aby jich bylo celkem deset a aby takto získala každý ze čtverců $1 \times 1, \ldots, 5 \times 5$ aspoň jednou. Mohlo se jí to podařit? *(Anička Doležalová)*

Řešení:

Původní papír má obsah 81, čtverce $1 \times 1, \ldots, 5 \times 5$ mají obsah v součtu 55. Dalších pět čtverců, které chceme vystřihnout, má tedy obsah $81 - 55 = 26$, což můžeme poskládat jako $1 \times 1 + 1 \times 1 + 2 \times 2 + 2 \times 2 + 4 \times 4$. (Tento rozklad je jediný možný, dokazovat to zde ale nebudeme, ostatně to po nás úloha ani nechce.) Celý papír tak chceme rozdělit na jeden čtverec 5×5, dva 4×4, jeden 3×3, tři 2×2 a tři 1×1.

Musíme ještě ověřit, zda tyto čtverce skutečně jdou poskládat na papír 9×9 tak, aby se nepřekrývaly a pokryly celý papír. Na obrázcích vidíte dvě možná pokrytí.



Poznámky:

Většina úlohu vyřešila bez problémů s menším či větším zdůvodňováním, proč volí právě těchto deset čtverců (což zadání vůbec nevyžadovalo, jako důkaz stačil i samotný obrázek jednoho z možných rozložení). Část řešitelů opomněla ověřit, zda čtverce jdou na papír naskládat. Několik z vás si pak vyložilo zadání tak, že můžeme kromě deseti čtverců dostat i další útvary. Na závěr se pak sešla dvě řešení pokoušející se dokázat, že papír rozstříhat nelze.

(Anička Doležalová & Lukáš Zavřel)

Úloha 2. (167; 134; 1,99; 2,0)

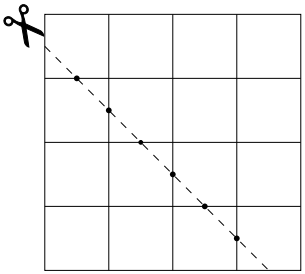
Martin má čtverečkovaný papír $n \times n$. Rozstřihl ho rovně na dva kusy. Kolik nejvíce čtverečků mohl přestřihnout?[12] *Svou odpověď zdůvodněte.* *(Vít „Vejtek“ Musil)*

Řešení:

Dokážeme, že Martin mohl přestřihnout maximálně $2n - 1$ čtverečků.

Čtverečkovaný papír $n \times n$ se celkem skládá z $2n-2$ vnitřních a čtyř obvodových úseček. Řez procházející napříč čtverečkovaným papírem může protnout maximálně $2n-2$ vnitřních úseček. Získáme tedy maximálně $2n - 2$ průsečíků odpovídajících $2n - 1$ částem, na které bude přímka představující rozstřižení rozdělena. To znamená, že protíná nejvýše $2n - 1$ čtverečků.

Takový řez je skutečně možné sestrojit, stačí posunout úhlopříčku směrem dolů o polovinu délky strany malého čtverečku. Takto v prvním řádku protneme jeden čtvereček a ve všech ostatních $n - 1$ řádcích dva čtverečky, takže celkem protneme $2n - 1$ čtverečků.



Poznámky:

Většina řešitelů správně určila maximální počet přestřižených čtverečků. Bohužel valná část řešení neobsahovala „přesvědčivý“ důkaz, že se opravdu jedná o maximum. To byl hlavní důvod stržení bodů. Také se objevilo pár velice zajímavých řešení využívajících otočení čtverečkovaného papíru či rekurentního vyjádření maximálního počtu čtverečků.

(Anička „Anagnina“ Zavadilová & Alexander „Olin“ Slávik)

Úloha 3. (130; 98; 2,37; 3,0)

Mějme na všechny strany nekonečný čtverečkovaný papír. Do každého průsečíku namalujeme puntík jednou ze čtyř barev tak, aby vrcholy každého čtverečku měly různé barvy. Dokažte, že pak se na nějaké (svislé nebo vodorovné) čáře vyskytují body pouze dvou barev.

(Martina Vaváčková)

Řešení:

Dokažme tvrzení sporem. Předpokládejme, že v každém sloupci i řádku jsou puntíky alespoň tří barev. Pak jistě existuje trojice různobarevných puntíků, které leží bezprostředně vedle sebe v jednom řádku[13].

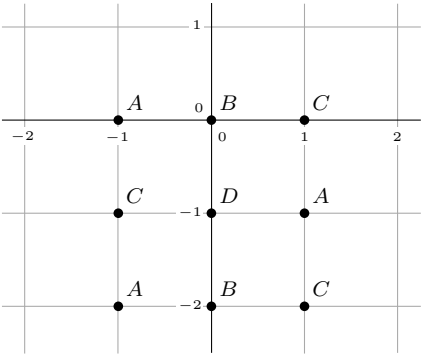
Zvolme souřadný systém tak, aby na pozicích $[-1, 0]$, $[0, 0]$ a $[1, 0]$ byly tyto puntíky s barvami po řadě A, B, C. Pak ale na pozici $[0, -1]$ je nutně puntík jiné barvy, neboť v každém čtverci jsou puntíky různých barev. Tuto barvu označíme D.

[12] Čtvereček je přestřižený, jestliže na každém z dílů je aspoň kousek jeho obsahu.

[13] Existenci takové trojice dokážeme sporem. Nechť ve zvoleném řádku zmíněná trojice neexistuje. Pak každá trojice bezprostředně sousedících puntíků na tomto řádku má jen dvě barvy (je tvaru $X\ Y\ X$), tedy zjevně se tyto dvě barvy střídají na celém řádku, což je kýžený spor.

Ze stejného důvodu je jistě barva C na pozici $[-1,-1]$ a barva A na $[1,-1]$. Analogicky musí být barva B na $[0,-2]$, A na $[-1,-2]$ a C na $[1,-2]$. Dostáváme tak trojici puntíků se stejnými barvami jako na začátku a můžeme úvahy zopakovat.

Postupně tak pro všechna nezáporná celá k dostaneme, že na pozicích $[0,-2k]$ je barva B a na pozicích $[0,-2k-1]$ je barva D. Totožně můžeme postupovat od původní trojice opačným směrem. Na všech pozicích sloupce nula tak musí být barva B nebo D, což je spor s předpokladem.



Poznámky:
Většina řešitelů úlohu dokázala sporem, nicméně kromě správných řešení se objevila i mnohá s více či méně podstatnými nedostatky. Nejčastější chybou bylo rozebrání několika případů bez vysvětlení, jak bude mřížka pokračovat do nekonečna. Jiní řešitelé nesprávně předpokládali, že se v nějaké čáře vyskytují všechny čtyři barvy. A bohužel se objevili i tací, kteří jen nakreslili obrázek, v němž byly dvoubarevné čáry. Návrh takového obarvení části sítě ovšem není důkazem zadaného tvrzení. *(Bára Kociánová & Míša Hubatová)*

Úloha 4. (86; 58; 3,17; 4,0)

Mějme čtverečkovaný papír $m \times n$. Kolika způsoby můžeme strany všech čtverečků obarvit pomocí tří barev tak, aby každý čtvereček měl právě dvě strany obarvené jednou barvou a zbývající dvě nějakou jinou jednou barvou? Strany, kterými se sousedící čtverečky dotýkají, považujeme za totožné. *(Alexander „Olin“ Slávik)*

Řešení:
Barvy, se kterými budeme pracovat, si označme A, B, C. Nejprve vypozorujeme, že pokud už má nějaký jednotkový čtverec obarvené dvě strany, mohou nastat dva případy:

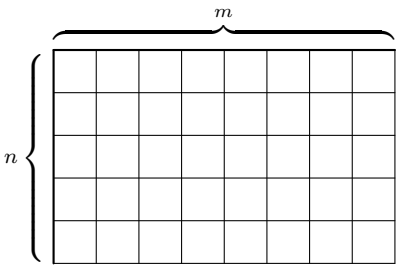
(i) Obě strany jsou obarveny jednou barvou (BÚNO[14] A): Obě zbylé strany musíme obarvit barvou B, nebo C. Máme tedy dvě možnosti, jak to udělat.
(ii) Strany jsou obarveny různými barvami (BÚNO A, B): Jednu ze zbývajících stran musíme obarvit barvou A a druhou barvou B, nebo naopak. I zde tedy máme dvě možnosti obarvení.

Z toho vyplývá, že pokud budeme obarvovat čtverec, který má už dvě strany obarvené, můžeme tak učinit vždy právě dvěma způsoby.

Nyní začněme obarvovat. Nejdříve levou a horní hranu papíru (na obrázku naznačeny tučně), které se sestávají z m resp. n stran jednotkových čtverců. Obarvení jednotlivých stran je na sobě

[14] Bez újmy na obecnosti.

nezávislé, takže každou můžeme nabarvit třemi způsoby. Daných stran je přitom $m+n$, takže aplikací pravidla kombinatorického součinu dostáváme 3^{m+n} možností.



Dále obarvujme políčka od levého horního rohu „ve směru čtení“, tedy zleva doprava a shora dolů. Zjevně přitom vždy budeme obarvovat čtverec, který už má dvě strany nabarvené, takže jej můžeme obarvit dvěma způsoby. Těchto čtverečků je $m \cdot n$, takže aplikací pravidla kombinatorického součinu zjišťujeme, že počet možností, jak to udělat, je 2^{mn}.

Nyní stačí aplikovat pravidlo kombinatorického součinu ještě jednou a získat tak počet všech možných způsobů obarvení $3^{m+n} \cdot 2^{mn}$. Papír tedy můžeme obarvit $3^{m+n} \cdot 2^{mn}$ způsoby.

Poznámky:
Přibližně jedna třetina řešitelů si s úlohou hravě poradila. Většina správných řešení se ale nedržela vzorového. Řešitelé obarvovali už od začátku „po čtverečkách“, čímž si přidělali práci navíc. Těm, kteří se jí naopak vyhnuli, jsem udělil imaginární bod. Z ostatních došlých řešení mě nepříjemně překvapilo, jak velké množství řešitelů používalo místo pravidla kombinatorického součinu pravidlo kombinatorického součtu. Ještě více lidí ale nepochopilo zadání a řešilo jinou úlohu, proto bych rád doporučil všem, kteří mají ohledně zadání jakékoliv nejasnosti, aby se nebáli zeptat. *(Martin „E. T.“ Sýkora & Michael „Majkl“ Bílý)*

Úloha 5. (91; 42; 2,31; 1,0)

Vejtek si na čtverečkovaný papír nakreslil trojúhelník. Tvrdí, že všechny jeho vrcholy, střed kružnice opsané, střed kružnice vepsané, průsečík výšek i těžiště leží ve vrcholech nějakých čtverečků. Může mít pravdu? *(Martina Vaváčková)*

Řešení:
Ak nájdeme trojuholník vyhovujúci zadaniu, znamená to, že Vejtek môže mať pravdu. Skúsme dokázať, že zadaniu vyhovuje pravouhlý trojuholník ABC s pravým uhlom pri vrchole C so súradnicami $A = [0, 18]$, $B = [24, 0]$, $C = [0, 0]$.

Keďže je to pravouhlý trojuholník, tak priesečník výšok bude totožný s bodom C, teda bude ležať na vrchole štvorčeka. Z toho istého dôvodu bude stred opísanej kružnice (označme si ho S) ležať v strede prepony AB trojuholníka. Čiže bod S má súradnice $S = (A + B)/2 = [12, 9]$. Ďalej polohu ťažiska T vyrátame pomocou známeho vzorca

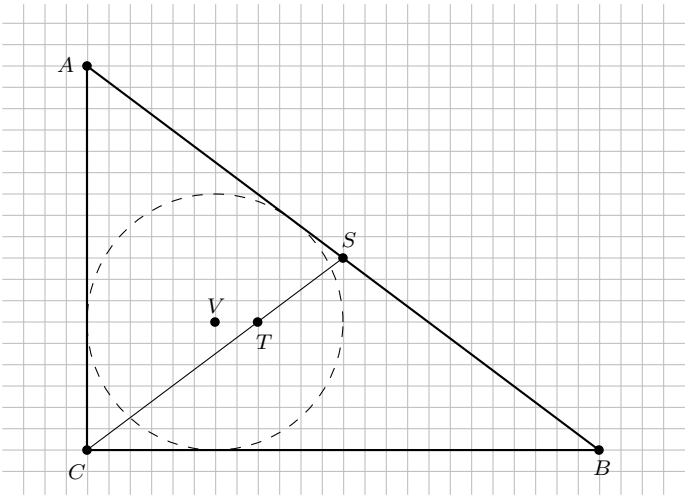
$$T = \frac{A+B+C}{3} = \left[\frac{0+24+0}{3}, \frac{18+0+0}{3}\right] = [8, 6],$$

takže tiež leží na vrchole štvorčeka.

Zostáva nám už len ukázať, že tam leží aj stred kružnice vpísanej. Pre polomer kružnice vpísanej do trojuholníka platí $\rho = 2S/O$, kde S je obsah a O je obvod trojuholníka. Keďže je to pravouhlý trojuholník, obsah ľahko vyjadríme ako $S = |AC| \cdot |CB|/2$. Teda pre polomer platí

$$\rho = \frac{|AC| \cdot |CB|}{O} = \frac{18 \cdot 24}{18 + 24 + 30} = 6.$$

A keďže strany splývajú s osami x a y, tak z toho vidno, že stred vpísanej kružnice musí mať súradnice $V = [6, 6]$. Takže sme ukázali, že všetky body ležia na vrcholoch štvorčekov v sieti.

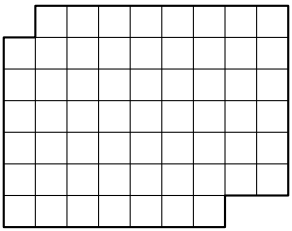


Poznámky:
Zadaniu samozrejme vyhovujú aj iné trojuholníky, ale nám to stačí dokázať pre jeden, aby Vejtek mohol mať pravdu. Veľa z vás nakreslilo obrázok, v ktorom sa zdalo, že vyhovuje zadaniu, ale po dôkladnejšom počítaní sa ukázalo, že to nie je pravda. V dôkaze musíte jednoznačne ukázať, že vaše tvrdenie je pravdivé, inak vám za to nemôžeme dať body. Niektorí z vás ani vyhovujúci trojuholník nenašli, čo je celkom škoda, lebo potom ste svoje tvrdenie, že taký trojuholník neexistuje, ani nemohli dokázať, a za to išli body opäť dole. Ale našťastie vás bolo dosť aj takých, ktorí trojuholník našli a aj poriadne dokázali, že vyhovuje zadaniu.

(Lucka Magurová & Viktor Szabados)

Úloha 6. (87; 42; 2,56; 1,0)

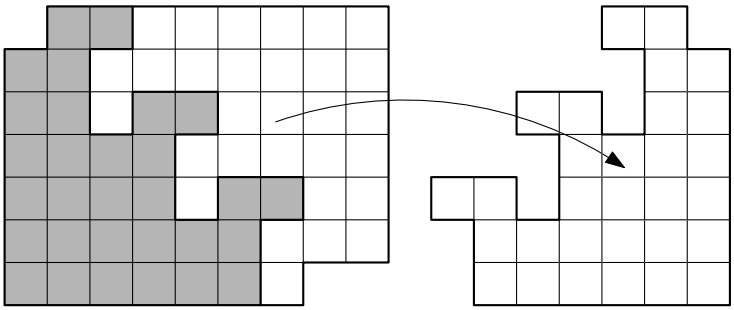
Je možné rozstřihnout útvar na obrázku na dvě části stejného tvaru[15] *a velikosti, je-li dovoleno stříhat pouze po vyznačených čarách?*



(Martina Vaváčková)

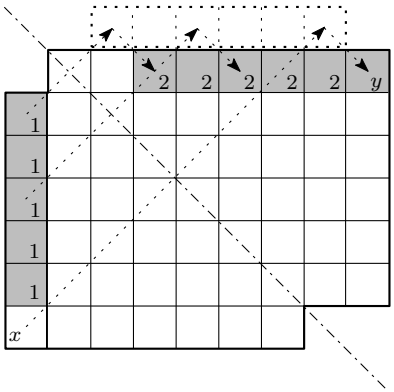
[15] Přípustné je otáčení a zrcadlové převracení.

Řešení:
Ano, je to možné, viz obrázek.



Jak se na to dalo přijít:
U úloh tohoto typu nám uvedené řešení skutečně stačí. Způsob, jak se k němu dopracovat, nastíníme v této části. Předpokládejme, že zadaný útvar lze rozdělit podle zadání. Zřejmě existuje nějaké shodné zobrazení převádějící jednu část útvaru na druhou. Každé shodné zobrazení v rovině je posunutí, otočení nebo osová souměrnost podle osy o následovaná posunutím ve směru o (tzv. osové posunutí), jak se můžete dočíst v seriálu Geometrická zobrazení k 31. ročníku. Posunutí i otočení po chvíli zkoušení vyloučíme (např. otočení o přímý úhel, tedy středovou souměrnost, kvůli tomu, že náš útvar není středově souměrný, ostatní možnosti jsou trochu otravnější).

Rozeberme tedy poslední možnost, osové posunutí. Aby se čtverečky zobrazily na čtverečky, musí osa být vodorovná, svislá, nebo svírající $\pm 45°$ s vodorovným směrem a procházet buď vrcholy mřížky, nebo středy hran mřížky. Pro každý směr už je jednoznačně daná tím, že musí útvar obsahově půlit – všechno, co bylo na jedné straně osy, se totiž musí (nezávisle na tom, které části to patřilo) zobrazit na všechno na druhé straně. Tím pádem už máme jednoznačně určenou osu mířící doprava dolů (ostatní tři osy nevedou ani vrcholy, ani středy), viz obrázek.



Čtverečky x, y jsou nejdál od osy, čili se musejí zobrazit na sebe. Z toho nám vychází vektor posunutí při zobrazení x na y roven $(1, -1)$ (mřížku BÚNO prohlašme za jednotkovou). Postupně rozhodneme i pro všechny ostatní čtverečky, do které části patří. Do každého čtverečku napíšeme buď 1, nebo 2. Začneme tím, že do políčka x napíšeme jedničku a do y dvojku. Pro každý

čtvereček jsou dva jeho potenciální protějšky dané zrcadlením podle o a posunutím o $(1,-1)$, resp. $(-1,1)$. Podívejme se na sloupec čtverečků nad x (obrázek). Co budou jejich protějšky? Je jasné, že posunutí jejich zrcadlového obrazu o $(-1,1)$ by je zobrazilo mimo náš útvar, což nelze. Musejí tedy být součástí útvaru 1. A opravdu, posunutí o $(1,-1)$ už nedělá problém. Obdobným postupem (občas se trefíme sice dovnitř, ale do již jinak určeného čtverečku) lze každý čtvereček jednoznačně zařadit do 1 nebo do 2 a dopracovat se tak k rozdělení z prvního obrázku.

Poznámky:
Úloha se ukázala být docela problematická, protože většina řešení se pokoušela dokázat neexistenci požadovaného rozdělení. To bylo pochopitelně tentokrát nemožné, ale obecně platí, že důkaz neexistence řešení v podobných případech je těžký a zdlouhavý, rozebírající mnoho možností (jistě je vám jasné, že kapitolka „Jak se na to dalo přijít“ má k důkazu daleko). Takže se spíš vyplatí zkoušet řešení najít, případně se pokusit něco o něm obecně zjistit (tentokrát svoje úvahy nemusíme sepisovat a dokazovat), například zredukovat počet „typů“ řešení, jako jsme to udělali my.

Ti, kteří úlohu nevyřešili, mohli dostat až dva body za nějaká pozorování (v drtivé většině šlo o jeden bod za zjištění, že útvar má sudý počet políček, což nebrání existenci hledaného rozdělení). Rád bych takových bodů rozdal více a mnozí z vás ve svých řešeních skutečně tvrdili daleko méně triviální věci, ale bohužel byli také vesměs daleko od jejich důkazu (čemuž se nelze divit, jak bylo řečeno výše). Kladný imaginární bod obdržela *Karolína Kuchyňová* za podle mého nejlepší popis postupu, který ji k řešení dovedl. Kuriózní je ovšem to, že si v obrázku s řešením přidala jeden řádek navíc, takže výsledné rozdělení měla „špatně“, čímž dosáhla neobvyklého bodového zisku $4+i$. Nakonec bych chtěl pochválit ty, kteří projevili dost trpělivosti a invence a řešení našli, a všem potom popřát hodně štěstí a dobrých nápadů do dalších sérií.

(David Hruška & Martina Vaváčková)

Úloha 7. (71; 32; 2,24; 1,0)

Martina a Olin hrají na čtverečkovaném papíru o rozměrech 6×6 následující hru. Střídavě píšou do jednotlivých čtverečků reálná čísla, která se na papíře ještě nevyskytují. Po vyplnění celého papíru zeleně vybarví maximum v každém řádku. Olin vyhraje, pokud existuje cesta shora dolů vedoucí pouze skrz zelené čtverečky[16]*, v opačném případě vyhrává Martina. Kdo vyhraje, když Olin začíná a oba volí nejlepší možnou strategii?* *(Alexander „Olin“ Slávik)*

Řešení:
Vyhraje Martina. Předvedeme si pro ni dvě možné jednoduché vyhrávající strategie.

První strategie – spárování dvou řádků:
Martina se zaměří na první dva řádky a políčka prvního řádku spáruje s políčky druhého řádku podle následujícího obrázku.

A	B	C	D	E	F
D	E	F	A	B	C

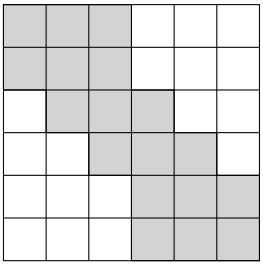
Kdykoli Olin napíše číslo mimo první dva řádky, Martina zahraje také mimo – to může udělat, protože před každým Olinovým tahem bude v této oblasti sudý počet políček.

Dále, pokud Olin zahraje do prvních dvou řádků, Martina vyplní spárované políčko. Navíc, pokud Olin napsal číslo, které je právě i-té největší ve svém řádku, napíše i Martina takové číslo, aby bylo i-té nejvyšší.

[16] Dva čtverečky, které sousedí pouze rohem, považujeme také za sousední.

Takto bude na konci vyplněna zeleně některá dvojice spárovaných políček a zelená cesta nepovede ani přes první dva řádky.

Druhá strategie – ochranná zeď:
Martina si představí v každém řádku tři šedě vybarvená políčka podle následujícího obrázku.



Vždy, když Olin někam zahraje, zareaguje Martina ve stejném řádku. A to tak, že když umístil Olin číslo na bílé políčko, dá Martina nižší číslo na šedé, a když napíše Olin číslo na šedé políčko, dá Martina vyšší číslo na bílé. Takto po každém Martinině tahu bude v každém řádku vyplněno stejně bílých jako šedých políček a v žádném šedém nebude nejvyšší číslo řádku.

Zelená cesta tak nemůže vést shora až dolů, protože nemůže překřížit šedou oblast.

Poznámky:
Naprostá většina řešitelů postupovala podle jednoho ze dvou vzorových řešení. Nesprávná řešení většinou předpokládala něco, co nemusela být pravda. Nejčastěji to, že už znají maximum v nějakém řádku a podle toho hrají dál – zapomněli ale, že některá z dalších políček už mohla být vyplněná. Velká část řešitelů také pouze napsala, že Martina vyhraje, protože může v každém řádku doplnit poslední číslo a tím určit maximum. To je sice skoro pravda, ale jako důkaz takové tvrzení nestačí. Za tato řešení jsem dával 0–2 bodů. Dále se bohužel našlo i pár takových, kteří špatně pochopili zadání a předpokládali, že hráči vyplňují políčka popořadě. Těmto řešitelům jsem za vyřešení mnohem jednodušší úlohy udělil dva body. *(Martin Čech & Mirek Olšák)*

Úloha 8. (65; 24; 1,68; 0,0)

Na čtverečkovaném papíru o rozměrech $n \times n$ ($n \geq 3$) vybarvíme některé čtverečky černě a následně dva protější okraje slepíme. Ukažte, že na vzniklém válci jsou alespoň dva řádky, sloupce nebo rovnoběžné diagonály, které obsahují tentýž počet černých čtverečků.

(Alexander „Olin“ Slávik)

Řešení:
Dokážeme to sporom. Predpokladajme, že existuje ofarbenie, v ktorom žiadne dva riadky (stĺpce, rastúce ani klesajúce diagonály) nemajú rovnaký počet čiernych štvorčekov, a označme počet čiernych políčok v i-tomu riadku, stĺpci, klesajúcej a rastúcej diagonále postupne r_i, s_i, d_i a u_i. Ďalej označme C celkový počet čiernych štvorčekov. Pretože každé políčko náleží práve jednému riadku, stĺpci aj diagonále oboch smerov, musí platiť

$$C = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} s_i = \sum_{i=1}^{n} d_i = \sum_{i=1}^{n} u_i.$$

Každý riadok, stĺpec aj diagonála obsahuje práve n štvorčekov, teda určite $0 \leq r_i, s_i, d_i, u_i \leq n$. Podľa predpokladu vieme, že čísla r_i (s_i, d_i, u_i) musia byť rôzne, preto musíme použiť všetky čísla $0, \ldots, n$ okrem jedného – označme ho r (analogicky pre ostatné smery s, d, u). Potom platí

$$C = \frac{n(n+1)}{2} - s = \frac{n(n+1)}{2} - r = \frac{n(n+1)}{2} - d = \frac{n(n+1)}{2} - u,$$

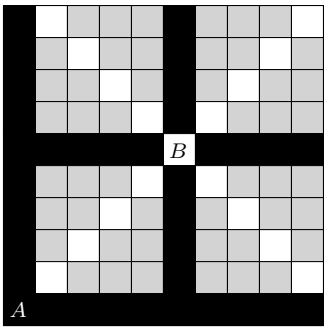
z čoho dostávame rovnosť $r = s = d = u$.

V prípade, že $0 < r < n$, musí existovať nejaký celočierny aj celobiely riadok, ale zároveň aj celočierny a celobiely stĺpec, čo nie je možné. Preto $r = 0$ alebo $r = n$, BUNV zvoľme $r = 0$, v opačnom prípade iba zinvertujeme farby. Máme teda $1 \leq r_i, s_i, d_i, u_i \leq n$.

Uvažujme teraz celočierny riadok a stĺpec – tie sa pretnú v štvorčeku A. Keďže každá diagonála zdieľa s každým riadkom aj stĺpcom jeden štvorček, musia diagonály oboch smerov s práve jedným čiernym políčkom prechádzať štvorčekom A, zvyšky týchto diagonál musia byť biele. V prípade, že sa tieto diagonály už v inom štvorčeku nepretnú, tak v každom riadku okrem celočierneho sú už určite 2 biele štvorčeky, každý z jednej diagonály. Preto neexistuje riadok, v ktorom je práve jeden biely štvorček, čo je spor.

Ak sa tieto diagonály pretnú ešte v jednom štvorčeku (označíme ho B), tak vo všetkých riadkoch, okrem tých obsahujúcich A alebo B, sú aspoň dva biele štvorčeky. Preto riadok s jediným bielym políčkom musí byť ten prechádzajúci cez políčko B. Analogicky identifikujeme aj stĺpec s jedným bielym štvorčekom.

Pozrime sa na riadok s práve jedným čiernym políčkom. Určite neobsahuje štvorček A ani B, lebo tieto riadky majú n alebo $n-1$ čiernych políčok. Všetky ostatné riadky ale obsahujú jeden čierny štvorček zo stĺpca s políčkom A a druhý čierny štvorček zo stĺpca s B. Opäť dostávame spor. Tvrdenie v zadaní teda musí platiť.



Poznámky:

Príklad bol na osmičku pomerne ľahký, zarmucujúce ale je, že dosť veľa riešiteľov nepochopilo zadanie. Druhým kameňom úrazu bolo uvedomiť si, že diagonály sa môžu pretnúť až v dvoch bodoch. *(Marta Kossaczká & Peter „πtr“ Korcsok)*

Seriál – Teorie čísel I

Počínaje 17. ročníkem probíhá každý rok v PraSátku seriál na pokračování. Jde o výklad nějakého odvětví matematiky, se kterým se na střední škole s velkou pravděpodobností setkáš jen v omezené míře či vůbec ne, ale které je přesto možné vyložit tak, aby bylo středoškolákům přístupné. Cílem seriálu je tedy rozšířit Tvé matematické obzory o nějaký zajímavý kout matematiky. Letošní seriál na téma *Teorie čísel* pro Tebe píší Pepa Svoboda a Štěpán Šimsa. V prvních, druhých a třetích komentářích vyjde vždy jeden díl a k němu trojice úloh, k jejichž vyřešení by Ti měly stačit znalosti nabyté přečtením a plným pochopením doposud vydaných dílů. Na rozdíl od ostatních sérií se Ti z této do výsledného bodového hodnocení započítají všechny (tři) příklady.

Jak seriál číst?

Letošní téma je natolik zajímavé, obsáhlé a užitečné, že jsme se rozhodli udělat seriál vydatnější[17] než obvykle. Proto Tě v prvním díle seznámíme s důležitými základy, bez kterých bychom se v dalších dílech neobešli. Budeš-li mít pocit, že některou část seriálu máš v malíčku, můžeš ji s klidem přeskočit. Jestliže naopak nějakou část napoprvé nepochopíš, nezoufej a zkus to ještě jednou. Pokud to nepomůže, neboj se zeptat se na chatu nebo prostřednictvím e-mailu některého z autorů.[18]

Dohoda

Abychom se nezbláznili, budeme celá čísla (tj. -2, -1, 5, 0 apod.) označovat pouze jako „čísla“, protože s nimi budeme pracovat prakticky pořád. Pokud v seriálu použijeme neznámé a, b, c, d, myslíme tím vždy čísla (tedy celá!). Neznámé m, n máme vyhrazené pro čísla přirozená.

Úvod

Můžeš si blahopřát k výběru toho nejlepšího[19] tématu, kterým je Teorie čísel. Jde o obor zabývající se především vlastnostmi přirozených a celých čísel. Přestože mohou přirozená čísla působit jednoduše, opak je pravdou. Skrývají mnoho tajemství a nevyřešených problémů. Kde jinde se dají najít otevřené problémy s tak přístupným zadáním?

Příkladem mohou být takzvaná *dokonalá čísla*. Dokonalé je takové číslo, které je rovno součtu svých dělitelů s výjimkou sebe sama. Například číslo šest je dokonalé, protože $1 + 2 + 3 = 6$. Dalšími dokonalými čísly jsou 28, 496, 8 128, 33 660 336. Dohromady jich zatím známe jen 48, přičemž největší z nich má přes 17 miliónů cifer.

Cvičení. Dokaž, že součet převrácených hodnot dělitelů dokonalého čísla n je 2. (Například $\frac{1}{6} + \frac{1}{3} + \frac{1}{2} + 1 = 2$.)

[17] Občas se v poznámce pod čarou vyskytne vtip. Ten bude označen takto.[17]

[18] E-maily najdeš například na stránce *http://mks.mff.cuni.cz/organizatori.php*.

[19] My vlastně ani jiná témata ne(u)zná(vá)me.[17]

Návod. Poděl definici číslem n.

Velkou záhadou zůstává, jestli existuje i nějaké liché dokonalé číslo. Víme, že pokud by existovalo, tak by muselo splňovat mnoho podmínek. Například by bylo větší než 10^{300}, po dělení číslem 468 by dávalo zbytek 117, mělo by přes sto tisíc dělitelů a podobně.

Než si sami budeme moci dokázat něco pěkného o dokonalých číslech, musíme si vysvětlit základy, na kterých je celá teorie postavena. Ale neboj se, už v tomto díle se dozvíš spoustu zajímavých věcí, které Ti ve škole nejspíše neprozradí. Tak s chutí do toho!

Dělitelnost

Definice. Číslo b *je dělitelné* číslem $a \neq 0$, právě když existuje číslo c takové, že $ac = b$. Tento fakt zapisujeme $a \mid b$. Číslo a nazýváme *dělitelem* čísla b a b *násobkem* čísla a.[20]

Dělitelnost je základní pojem teorie čísel. Budeme se s ní setkávat na každém kroku, proto se s ní seznam v následujících cvičeních.

Cvičení. Dokaž si následující tvrzení.[21] Nechť platí $a, b \neq 0$.

(i) Platí $1 \mid a$ a $a \mid 0$.
(ii) Pokud $a \mid c$, tak i $a \mid cd$ a pokud $ab \mid c$, tak $a \mid c$.
(iii) Pokud $a \mid b$ a $b \mid c$, tak $a \mid c$. (Proto si můžeme dovolit zkrácený zápis $a \mid b \mid c$.)
(iv) Pokud $a \mid c$ a $b \mid d$, tak $ab \mid cd$.
(v) Pokud $a \mid c$, tak $c = 0$ nebo $|a| \leq |c|$.
(vi) Pokud $a \mid b$ a $b \mid a$, tak $|a| = |b|$.
(vii) Pokud $a \mid c$ a $a \mid d$, tak $a \mid c + d$.

Všimni si, že v posledním případě platí i $a \mid c - d$, ba dokonce $a \mid kc + ld$ pro libovolná čísla k, l.

Úloha. Urči všechna přirozená čísla m, n taková, že n dělí $2m - 1$ a m dělí $2n - 1$.
(MO 59–A–II–3)

Návod. Uvědom si, že pokud v části (v) je $c \neq 0$ a $|a| \neq |c|$, tak dokonce platí $2|a| \leq |c|$.

Cvičení. Rozmysli si, že obecně **neplatí**:

(i) Pokud $a \mid c$ a $b \mid d$, tak $a + b \mid c + d$.
(ii) Pokud $a \mid c$ a $b \mid c$, tak $ab \mid c$.
(iii) Pokud $a \mid cd$, tak $a \mid c$ nebo $a \mid d$.

Následuje jednoduché tvrzení, se kterým ses jistě již setkal a které často využíváme.

Tvrzení. (dělení se zbytkem) *Pro libovolná čísla a, b existuje jediná dvojice čísel q, r taková, že $a = bq + r$ a $0 \leq r < |b|$. Číslo q nazýváme* celočíselný podíl čísel a a b; *r nazýváme* zbytek po dělení čísla a číslem b.

NSD – největší společný dělitel

Nyní se seznámíme s největším společným dělitelem, vyzkoušíme si, jak se s ním pracuje, a

[20] Velmi často také říkáme, že a *dělí* b, ale pozor! To znamená, že a dělí b, a ne, že b dělí a.[17]
[21] $|x|$ je absolutní hodnota čísla x definovaná jako $|x| = x$ pro $x \geq 0$ a $|x| = -x$ pro $x < 0$.

ukážeme si snadný a rychlý způsob, jak jej vypočítat. Nejprve si ujasněme, co se pod tímto pojmem skrývá.

Definice. *Největší společný dělitel* (NSD) čísel $a_1, a_2, \ldots, a_n$ (která nejsou všechna nulová) je největší přirozené číslo, které dělí všechna čísla $a_1, a_2, \ldots, a_n$. Budeme jej značit kulatými závorkami, tedy $(a_1, a_2, \ldots, a_n)$. Podobně *nejmenší společný násobek* (nsn)[22] je nejmenší přirozené číslo, které je násobkem všech čísel $a_1, a_2, \ldots, a_n$. Budeme jej značit hranatými závorkami $[a_1, a_2, \ldots, a_n]$.

Cvičení. Pro mírné seznámení si vypočítej hodnoty těchto NSD.

(i) $(-15, 24)$
(ii) $(n(n+1), 2)$

Řešení. Jediní dělitelé čísla -15 jsou čísla 1, 3, 5, 15 (a čísla jim opačná). Číslo 24 má kladné dělitele 1, 2, 3, 4, 6, 8, 12, 24. Společní dělitelé jsou jen -3, -1, 1, 3, z nichž největší je číslo 3. V části (ii) je určitě jedno z čísel n, $n+1$ sudé, tedy číslo $n(n+1)$ je dělitelné dvěma. To je ale největší dělitel čísla 2, takže i největší společný dělitel čísel $n(n+1)$ a 2.

Podívejme se nyní na NSD z jiného hlediska. K tomu bude potřeba začít něčím zdánlivě nesouvisejícím. Mějme daná čísla a, b, z nichž alespoň jedno je nenulové. Vezměme si množinu M všech čísel tvaru $ka + lb$, kde k, l jsou libovolná čísla (v množině jsou tedy například čísla a, $5a - 3b$, $-7b$ apod.). Všimněme si, že množina M má zajímavou vlastnost – kdykoliv do ní patří čísla i, j, tak do ní také patří jejich součet i rozdíl a také libovolný násobek jednoho z nich.

Nějaké číslo z množiny M musí být kladné (např. pro $k = a$ a $l = b$). Ze všech kladných čísel z M vyberme to nejmenší a označme ho r. Dokážeme, že všechna ostatní čísla v množině M (i ta záporná) jsou jeho násobkem. Pro spor předpokládejme, že nějaké číslo s není dělitelné číslem r. Nyní jej podělíme se zbytkem číslem r. Jinými slovy najdeme taková čísla u, v, pro která $s = ru + v$ a přitom $0 < v < r$ (v nemůže být nula, protože $r \nmid s$). Ale číslo r patří do naší množiny. Takže tam patří i číslo ru a dokonce i číslo $s - ru = v$. Tím jsme ale našli menší kladné číslo z množiny M, což je spor s předpokladem, že to nejmenší bylo r.

Jak to tedy ale všechno souvisí s NSD? Jak již možná tušíš, NSD čísel a, b není nic jiného než r. Víme totiž, že r patří do M, stejně jako čísla a, b. Takže $r \mid a$ a zároveň $r \mid b$. Ještě potřebujeme dokázat, že r je největší číslo s touto vlastností. Pro spor předpokládejme, že existuje takové větší číslo r'. Pak $r' \mid ka + lb$ pro všechna k, l, tedy dělí i r, protože $r = xa + yb$ pro nějaká x, y (patří do M). To je spor s tím, že je r' větší.

A dokázali jsme si hustou věc o NSD! Ale co víc – triviálně nám z tohoto důkazu plyne velice užitečná věta, jak v okamžení uvidíš.

Věta. (Bézoutova[23]) *Pro libovolná čísla a, b, z nichž alespoň jedno je nenulové, existují čísla k, l taková, že $ka + lb = (a, b)$.*

Důkaz. Jak víme z předchozích odstavců, tak (a, b) není nic jiného než r, které se dá zapsat jako $xa + yb$.

Když nastane případ $(a, b) = 1$, říkáme, že čísla a a b jsou *nesoudělná*. V opačném případě se jedná o čísla *soudělná*.

Příkladem použití Bézoutovy věty je důkaz následujícího tvrzení.

Tvrzení. *Nechť $a \neq 0$, b jsou nesoudělná čísla a platí $a \mid bc$. Potom také $a \mid c$.*

[22] V angličtině se používají zkratky gcd – greatest common divisor a lcm – least common multiple.

[23] Étienne Bézout (1730–1783) byl francouzský matematik.

Důkaz. Z Bézoutovy věty plyne, že existují čísla k, l tak, že $ak + bl = (a, b) = 1$. Celou rovnici vynásobíme číslem c a dostaneme $ack + bcl = c$. Ale $a \mid ack$, dále $a \mid bc \mid bcl$, takže $a \mid ack + bcl = c$, což jsme chtěli dokázat.

Cvičení. V následujících cvičeních platí $(a, b) = 1$. Dokaž:

(i) Pokud $a \mid c, b \mid c$, pak $ab \mid c$.
(ii) $[a, b] = ab$.

Úloha. Nechť a, b jsou dvě kladná nesoudělná čísla, m a n přirozená čísla a součet

$$\frac{ma - 1}{b} + \frac{nb - 1}{a}$$

je celočíselný. Dokaž, že platí nerovnost

$$\frac{m}{b} + \frac{n}{a} > 1.$$

(zobecnění MO 61–A–I–4)

Řešení. Sečteme-li zlomky, vidíme, že musí platit $ab \mid a(ma - 1) + b(nb - 1)$.

Speciálně tedy $b \mid a(ma - 1) + b(nb - 1)$, a jelikož $b \mid b(nb - 1)$, tak i $b \mid a(ma - 1)$. Ale a, b jsou nesoudělná čísla, takže $b \mid ma - 1$. Analogicky $a \mid nb - 1$. Vynásobením dostáváme:

$$ab \mid (ma - 1)(nb - 1) = mnab - (ma + nb - 1),$$
$$ab \mid ma + nb - 1.$$

Z toho plyne buď $ma + nb - 1 = 0$ (což však neplatí, protože $m, a, n, b \geq 1$), nebo $ab \leq ma + nb - 1$. To už jen jednoduše upravíme

$$ab < ma + nb,$$
$$\frac{m}{b} + \frac{n}{a} > 1.$$

Přesně to jsme chtěli dokázat.

Abychom mohli využívat silných vlastností nesoudělnosti, můžeme často udělat jednoduchý, ale účinný trik. Označíme si (a, b) například d a řekneme $a = du$, $b = dv$. Potom jsou čísla u, v nesoudělná, čehož právě využijeme. Vyzkoušej si to na následujících cvičeních.

Cvičení.

(i) Nechť $a \mid c, b \mid c$. Dokaž $[a, b] \mid c$.
(ii) $(a, b)[a, b] = ab$.

Nyní si můžeš dokázat další užitečnou vlastnost NSD.[24]

Cvičení. Dokaž:

(i) Pokud $(a, b) = d$ a $d' \mid a$, $d' \mid b$, tak $d' \mid d$.
(ii) Pokud $[a, b] = q$ a $a \mid q'$, $b \mid q'$, tak $q \mid q'$.

Návod. Postupuj sporem. Kdyby $d' \nmid d$, uvažte číslo $[d', d]$. Podobně v (ii).

Cvičení. Dokaž:

(i) Pokud $(a, c) = 1$ a $(b, c) = 1$ tak $(ab, c) = 1$.
(ii) $(a, b) = 1$, právě když $(a^2, b) = 1$.
(iii) Pokud $(b, c) = 1$, tak $(a, bc) = (a, b)(a, c)$.
(iv) $(a, bc) \mid (a, b)(a, c)$.

[24] Ta se někdy používá přímo jako definice NSD.

Eukleidův[25] algoritmus

Jak jsme slíbili, ukážeme si praktický způsob, jak NSD vypočítat. K tomu se využívá tzv. *Eukleidův algoritmus*. Nejprve si ale dokažme jednoduché pomocné tvrzení, že $(a, b) = (a-b, b)$. Označme $d = (a, b)$ a $d' = (a - b, b)$. Pak $d \mid a$, $d \mid b$, proto $d \mid a - b$, takže i $d \mid (a - b, b) = d'$. Na druhou stranu $d' \mid a - b$, $d' \mid b$, proto $d' \mid (a - b) + b = a$, takže i $d' \mid (a, b) = d$. Vidíme, že $d \mid d' \mid d$, tedy $d = d'$. Tím je důkaz pomocného tvrzení hotov a můžeme si ukázat samotný Eukleidův algoritmus.

Když dostaneme zadaná dvě čísla a, b, odečteme menší od většího a dostaneme novou dvojici (která má stejný největší společný dělitel jako ta původní). Když takto budeme vždy odečítat menší číslo od většího, postupně se budou čísla zmenšovat, až jedno bude nula a druhé nějaké c. Pak ale zřejmě $(0, c) = c$, takže c je také NSD čísel a, b.

Tento výpočet se dá ještě urychlit, když čísla nebudeme odčítat, ale když je budeme dělit se zbytkem. Například $(72, 21)$. Podělíme-li číslo 72 číslem 21, dostaneme 3 a zbytek 9. Tedy $(72, 21) = (72 - 3 \cdot 21, 21) = (9, 21)$. Takto můžeme pokračovat:

$$(72, 21) = (9, 21) = (9, 21 - 2 \cdot 9) = (9, 3) = (9 - 3 \cdot 3, 3) = (0, 3) = 3.$$

Cvičení. Rozmysli si, proč funguje i tento urychlený způsob.

Tohoto algoritmu můžeme vhodně využít i v případě, že neznáme konkrétní čísla. Například

$$(a, (a + 1)(a + 3)) = (a, a^2 + 4a + 3) = (a, a^2 + 4a + 3 - (a + 4)a) = (a, 3).$$

Díky tomu víme, že hledaný největší společný dělitel je buď 3, nebo 1 (podle toho, jestli $3 \mid a$, nebo ne). Nyní si vyzkoušej následující cvičení, aby ses s NSD lépe seznámil a uměl ho rychle počítat.

Cvičení. Urči, čemu se mohou rovnat tyto NSD. Předpokládej $(a, b) = 1$.

(i) $(a + b, a - b)$
(ii) $(a + b, ab)$
(iii) $(a^2 + ab, a + b)$
(iv) $(a^2 + a, a^2 + 3a + 2)$

Cvičení. (těžké) Nechť $m = ax+by$, $n = cx+dy$ a platí $ad-bc = \pm 1$. Ukaž, že $(m, n) = (x, y)$.

Celá část čísla

V tomto oddíle trošku odbočíme od celých čísel a seznámíme s dolní a horní celou částí. Co to tedy je?

Definice. *Dolní celá část* reálného čísla x je největší celé číslo, které není větší než x. Značíme ji $\lfloor x \rfloor$. *Horní celá část* reálného čísla x je nejmenší celé číslo, které není menší než x. Ta se značí $\lceil x \rceil$.

Jinak řečeno, dolní celá část zahazuje to, co je za desetinnou čárkou (ovšem pozor na záporná čísla). Takže například $\lfloor \frac{7}{3} \rfloor = 2$; $\lfloor 4 \rfloor = 4$; $\lfloor -5{,}352 \rfloor = -6$; $\lceil 5{,}8 \rceil = 6$. Ještě se hodí znát pojem *desetinná část* čísla, který vyjadřuje hodnotu $x - \lfloor x \rfloor$ a značí se $\{x\}$. Například $\{\frac{7}{3}\} = \frac{1}{3}$,

[25] Eukleides (nebo Eukleidés) byl řecký matematik, který působil v Egyptě v Alexandrii. Žil přibližně v letech 325 př. n. l. – 260 př. n. l. Napsal významné dílo Základy (první opravdovou učebnici s axiomy a důkazy, prý druhou nejvydávanější knihu po Bibli).

$\{-5{,}352\} = 0{,}648$. Všimni si, že pokud je x celé číslo, tak $\lfloor x \rfloor = \lceil x \rceil = x$ a $\{x\} = 0$, jinak $\lceil x \rceil = \lfloor x \rfloor + 1$ a $0 < \{x\} < 1$.

To, jak se s celou částí pracuje, si ukážeme na následujícím příkladě.

Příklad. Pro reálné číslo r platí

$$\left\lfloor r + \frac{19}{100} \right\rfloor + \left\lfloor r + \frac{20}{100} \right\rfloor + \cdots + \left\lfloor r + \frac{91}{100} \right\rfloor = 546.$$

Zjisti $\lfloor 100r \rfloor$. (AIME 1991)

Řešení. Na levé straně je $91 - 19 + 1 = 73$ členů. Všechny z nich mají hodnotu buď $\lfloor r \rfloor$, nebo $\lfloor r \rfloor + 1$. Jelikož $7 \cdot 73 < 546 < 8 \cdot 73$, tak $\lfloor r \rfloor = 7$. Navíc $546 = 7 \cdot 73 + 35$, takže prvních 38 členů má hodnotu 7 a zbylé členy mají hodnotu 8. Speciálně

$$\left\lfloor r + \frac{56}{100} \right\rfloor = 7, \quad \left\lfloor r + \frac{57}{100} \right\rfloor = 8.$$

Proto $r + \frac{56}{100} < 8$, $r + \frac{57}{100} \geq 8$ a z toho plyne $743 \leq 100r < 744$, takže $\lfloor 100r \rfloor = 743$.

Jako cvičení si zkus dokázat tyto vlastnosti celých částí:

Cvičení. Nechť jsou x, y reálná čísla a nechť je a celé.

(i) $\lfloor x + a \rfloor = \lfloor x \rfloor + a$ a $\lceil x + a \rceil = \lceil x \rceil + a$.
(ii) Dolní celá část je neklesající, tedy pro $x \leq y$ platí $\lfloor x \rfloor \leq \lfloor y \rfloor$.
(iii) $\lfloor x + \frac{1}{2} \rfloor$ zaokrouhluje x k nejbližšímu celému číslu.
(iv) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
(v) Počet kladných násobků čísla n nepřekračujících kladné x je roven $\lfloor \frac{x}{n} \rfloor$.
(vi) Dokaž si tvrzení o dělení se zbytkem.
(vii) $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \lfloor \frac{x}{n} \rfloor$.

Návod. V (iv) rozepiš $x = \lfloor x \rfloor + \{x\}$. Tato finta je velice často používaná. V (vi) uvaž číslo $\lfloor \frac{a}{b} \rfloor$.

Příklad. Dokaž, že

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \cdots = n.$$

(IMO 1968)

Řešení. Nejprve si uvědomíme, že pro $n = 1$ tvrzení platí (první člen je 1 a ostatní jsou nulové). Pro spor předpokládejme, že tvrzení pro nějaké n neplatí, a vezměme nejmenší takové n.[26] Vyřešme případ, kdy n je sudé, tedy $n = 2m$. Jelikož m je menší než n, tak pro něj tvrzení ze zadání platí.

$$\left\lfloor \frac{m+1}{2} \right\rfloor + \left\lfloor \frac{m+2}{4} \right\rfloor + \left\lfloor \frac{m+4}{8} \right\rfloor + \cdots = m.$$

Rozšíříme všechny zlomky na levé straně dvěma a dostaneme

$$\left\lfloor \frac{2m+2}{4} \right\rfloor + \left\lfloor \frac{2m+4}{8} \right\rfloor + \cdots = m.$$

Zbývá nám přičíst $\lfloor \frac{2m+1}{2} \rfloor = m$, čímž dostaneme po dosazení $n = 2m$ požadovaný spor.

Pro liché n je důkaz jen lehce těžší, zkus si jej dokončit sám.

[26] To, že takové n můžeme vybrat, je důležitá vlastnost přirozených čísel. Využíváme ji i při důkazu matematickou indukcí.

Prvočísla

Nyní se dostáváme k asi nejdůležitějšímu pojmu teorie čísel. *Prvočíslo.* Pravděpodobně víš ze školy, že prvočísla jsou taková čísla, která mají právě dva kladné dělitele – jedničku a sama sebe (takzvaní triviální dělitelé). Ostatní přirozená čísla nazýváme *složená* (pouze jedničku nepovažujeme ani za prvočíslo, ani za číslo složené[27]). Začneme klíčovým tvrzením o prvočíslech, které se také často používá jako definice.[28]

Tvrzení. (klíčové) *Přirozené číslo p je prvočíslo právě tehdy, když pro každá a, b platí, že pokud $p \mid a \cdot b$, tak $p \mid a$ nebo $p \mid b$.*

Důkaz. Nejprve předpokládejme, že p není prvočíslo. Pak podle naší definice existuje dělitel $1 < a < p$, tudíž $\frac{p}{a}$ je celé číslo. Platí $p \mid a \cdot \frac{p}{a}$, ale přitom $p \nmid a$ a $p \nmid \frac{p}{a}$, protože $p > a$ a $p > \frac{p}{a}$.

Druhou (obtížnější) implikaci dokážeme sporem. Mějme tedy prvočíslo p a nechť platí $p \mid ab$, ale přitom $p \nmid a$, $p \nmid b$. Z $p \mid ab$ plyne $(p, ab) = p$. Ze cvičení (iv) na straně 26 víme, že $(p, ab) \mid (p, a)(p, b)$. Ale (p, a) může být jen 1 nebo p (protože p nemá jiné dělitele). Jelikož ale $p \nmid a$, tak musí být $(p, a) = 1$. Analogicky dostaneme $(p, b) = 1$. Pak ale $p \mid 1 \cdot 1$, což je požadovaný spor.

Cvičení. Nechť k, l, m jsou přirozená čísla.

(i) Dokaž, že pokud $k + l + m \mid klm$, tak je $k + l + m$ složené.
(ii) Mějme prvočíslo $p = 2k + 3$. Dokaž $p \nmid 2k^3 + 7k^2 + 3k$.

Návod. Rozlož na součin a využijte definici prvočísla.

Nyní jsme připravení vrhnout se na důkaz zásadního tvrzení, které nám říká, že veškerá informace o přirozeném čísle se ukrývá v prvočíslech, která jej dělí.

Tvrzení. (Základní věta aritmetiky) *Každé přirozené číslo $n > 1$ lze jednoznačně (až na pořadí) zapsat jako součin $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kde $p_1, p_2, \dots, p_k$ jsou po dvou různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k$ jsou přirozená čísla.*

Důkaz. Pro spor si vezměme nejmenší přirozené n, které nemá prvočíselný rozklad. Nemůže to být prvočíslo, protože to by zřejmě rozklad mělo. Jelikož je n složené, tak $n = ab$ pro nějaká a, $b < n$. Čísla a, b mají rozklad na prvočinitele (n je první číslo, které ho nemá), takže má prvočíselný rozklad i jejich součin, tj. n. Ještě ale nevíme, jestli je tento rozklad jednoznačný.

Nyní si pro spor vezměme nejmenší n, jehož prvočíselný rozklad není jednoznačný, tedy $n = p_1 p_2 \dots p_k = s_1 s_2 \dots s_l$, kde $p_1 \le p_2 \le \dots \le p_k$ ($s_1 \le s_2 \le \dots \le s_l$) jsou ne nutně různá prvočísla. Kdyby $p_1 \neq s_1$, tak můžeme BÚNO[29] předpokládat $p_1 < s_1$. Jelikož je p_1 prvočíslo, tak musí dělit alespoň jedno z čísel $s_1, \dots, s_l$, to jsou ale všechno prvočísla větší než p_1, což je spor. Proto $p_1 = s_1$, a tedy číslo $\frac{n}{p_1} < n$ nemá jednoznačný rozklad, protože můžeme psát

$$\frac{n}{p_1} = p_2 p_3 \dots p_k = s_2 s_3 \dots s_l.$$

Dospěli jsme ke sporu s tím, že n je nejmenší číslo, které má nejednoznačný rozklad.

Nabízí se otázka, kolik je vůbec prvočísel. Ukážeme si snadný, leč trikový důkaz, že jich je nekonečně mnoho.

Tvrzení. *Existuje nekonečně mnoho prvočísel.*

[27] Zlé jazyky ovšem tvrdí, že jednička je jediné složené prvočíslo.[17]
[28] K tomu matematici mají hlubší důvody, které jsou ovšem nad rámec tohoto seriálu.
[29] BÚNO je oblíbená matematická zkratka znamenající „bez újmy na obecnosti“.

Důkaz. Předpokládejme, že prvočísel je jen konečně mnoho, a označme si je $p_1, p_2, \ldots, p_k$. Uvažme číslo $n = p_1 p_2 \ldots p_k + 1$. Díky existenci rozkladu na prvočísla musí být toto číslo dělitelné nějakým prvočíslem p_i, kde $i \in \{1, 2, \ldots, k\}$. Pak ale $p_i \mid n$ a současně $p_i \mid n - 1$, takže i $p_i \mid n - (n-1) = 1$, což je spor.

Cvičení. (těžké) Ukaž, že existuje nekonečně mnoho prvočísel ve tvaru $4k + 3$.

Kongruence

Nyní se naučíme jeden velice užitečný zápis. Budeme ho používat, když nebudeme potřebovat pracovat s čísly jako takovými, ale pouze s jejich zbytky po dělení nějakým číslem.

Definice. Skutečnost $m \mid (b - a)$ zapisujeme $a \equiv b \pmod{m}$ a čteme „*a je kongruentní s b modulo m*“.

Uvedenému výrazu se pak říká *kongruence*. Rozmysli si, že dvě čísla jsou kongruentní, právě když dávají stejný zbytek po dělení číslem m. Proto například $5 \equiv 17 \pmod{6}$ nebo $-2 \equiv 13 \pmod{5}$. Kongruence jsou velice přirozené díky své podobnosti s obyčejnými rovnicemi. Počítá se s nimi skoro stejně, což ukazuje následující tvrzení.

Tvrzení. *Pokud* $a \equiv b \pmod{m}$ a k *je libovolné číslo, tak platí:*

(i) $a + k \equiv b + k \pmod{m}$.
(ii) $a \cdot k \equiv b \cdot k \pmod{m}$.

Jinými slovy, k oběma stranám kongruence můžeme přičíst celé číslo a můžeme je také celým číslem vynásobit.

Tvrzení. *Pokud* $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, *tak platí:*

(iii) $a + c \equiv b + d \pmod{m}$.
(iv) $ac \equiv bd \pmod{m}$.

Důkaz. (iv) Víme, že $m \mid b - a$ a $m \mid d - c$. Proto $b = a + km$ a $d = c + lm$. Takže $bd = ac + m(kc + la + klm)$. Jinými slovy $bd - ac = m(kc + la + klm)$, což znamená $m \mid bd - ac$.

Cvičení. Jako cvičení si dokaž (i), (ii), (iii).

Vidíme, že kongruence můžeme navzájem sčítat (odčítat) a násobit. Nabízí se tedy otázka, jestli v nich lze – podobně jako v rovnicích – i dělit celým číslem. Odpověď je, že jen částečně.

Tvrzení. *Pokud* $a \cdot c \equiv b \cdot c \pmod{m}$ a $(m, c) = 1$, *tak* $a \equiv b \pmod{m}$.

Důkaz. Víme, že $m \mid c(b - a)$. Jelikož $(m, c) = 1$, platí i $m \mid (b - a)$.

V důkazu pěkně vidíme, proč je nesoudělnost potřeba. Opravdu, pokud například $8 \equiv 2 \pmod{6}$, tak z toho neplyne $4 \equiv 1 \pmod{6}$.

Viděli jsme, že jsme s kongruencemi proti obyčejným rovnicím v něčem trochu omezeni (byť jen zdánlivě, protože dělit soudělným číslem je podobné jako dělit nulou). Ale ještě nám zbývá zmínit vlastnosti, které zase mohou závidět rovnice.

Tvrzení. *Předpokládáme* $a \equiv b \pmod{m}$, m' *je přirozené číslo. Pak platí:*

(i) $a + k \cdot m \equiv b \pmod{m}$.
(ii) $m' \mid m$, *pak* $a \equiv b \pmod{m'}$.
(iii) (vylepšené dělení) *Pokud* $ca \equiv cb \pmod{m}$, *tak* $a \equiv b \pmod{\frac{m}{(m,c)}}$.

Cvičení. Zmíněná tvrzení si dokaž.

Návod. V (iii) polož $(m, c) = d$ a $m = du$, $c = dv$.

Úloha. Dokaž, že neexistuje přirozené číslo n takové, že $89^2 \mid n^2 + n - 22$. (MKS 30–2–6)

Řešení. Pro spor předpokládejme, že jsme našli n, pro které je podmínka splněna. Pak ale musí platit, že

$$\begin{aligned} n^2 + n - 22 &\equiv 0 \pmod{89^2}, \\ 4(n^2 + n - 22) &\equiv 0 \pmod{89^2}, \\ (2n+1)^2 &\equiv 89 \pmod{89^2}. \end{aligned}$$

Nyní můžeme přejít k modulu $89 \mid 89^2$ a zjistíme

$$\begin{aligned} (2n+1)^2 &\equiv 89 \pmod{89}, \\ (2n+1)^2 &\equiv 0 \pmod{89}. \end{aligned}$$

Proto $89 \mid (2n+1)^2$, a jelikož je 89 prvočíslo, tak i $89 \mid 2n+1$. Pak ale $89^2 \mid (2n+1)^2$, takže

$$0 \equiv (2n+1)^2 \equiv 89 \pmod{89^2},$$

což je spor.

Uvedené vlastnosti kongruencí můžeme dobře shrnout. Pokud máme nějaký výraz, kde se jen násobí a sčítá, můžeme do něj dosadit dvě kongruentní čísla a výsledky budou také kongruentní. To je formálněji vyjádřeno v následujícím cvičení.

Cvičení. Mějme $a \equiv b \pmod{m}$.

(i) Pak $a^n \equiv b^n \pmod{m}$.

(ii) Nechť P je polynom[30] s celočíselnými koeficienty. Pak platí $P(a) \equiv P(b) \pmod{m}$. Jinými slovy – posloupnost zbytků, které dávají hodnoty polynomu v celých číslech, je periodická.

Návod. Polynom si rozepiš podle definice a pro každou mocninu použij (i).

Kvadratické zbytky

Zajímavou partií teorie kongruencí jsou kvadratické zbytky.

Definice. Číslo a nesoudělné s m je *kvadratický zbytek* modulo m, pokud existuje číslo x takové, že $x^2 \equiv a \pmod{m}$. Pokud takové x neexistuje, říkáme, že číslo je *nezbytek* modulo m.

Přestože jsme si kvadratické zbytky zavedli pro libovolné přirozené modulo m, nejzajímavější a nejužitečnější případ nastává, když je m prvočíslo. Tomuto případu se proto budeme věnovat více.

Pro prvočíselné modulo p můžeme kvadratické zbytky dobře popisovat tzv. *Legendreovým*[31] *symbolem*. Ten značíme $\left(\frac{a}{p}\right)$. Definujeme ho následujícím způsobem:

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

[30] Polynom neboli mnohočlen je funkce tvaru $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, kde $a_n \neq 0$. Čísla $a_n, a_{n-1}, \ldots, a_0$ nazýváme koeficienty polynomu. Je to přesně ten výraz, kde se pouze sčítá a násobí.

[31] Adrien-Marie Legendre [ležándr] byl francouzský matematik žijící v letech 1752–1833.

Která čísla jsou tedy kvadratickými zbytky? Všechna, nebo jen některá? Zkusíme-li to na malých případech, snadno zjistíme, že všechna to nebudou. Už pro modulo $m = 3$ dávají čísla 0^2, 1^2, 2^2 zbytky 0, 1, 1 (z nich je kvadratický zbytek pouze číslo 1, protože 0 není nesoudělná s m). Můžeme tedy dostat zbytek 2? Odpověď je, podle očekávání, ne. Kdybychom za x dosadili něco jiného, nepomohlo by nám to, protože

$$(x + 3a)^2 = x^2 + 6a + 9a^2 = x^2 + 3(2a + 3a^2) \equiv x^2 \pmod 3.$$

Všechna další x^2 už tedy budou dávat stejný zbytek jako jedno z čísel 0^2, 1^2, 2^2, tj. pouze 0 nebo 1 (všimni si, že jsme jen dosadili dvě kongruentní čísla, museli jsme tedy dostat stejný zbytek).

To už nám dává návod, jak zjistit, která čísla jsou kvadratické zbytky modulo nějaké m. Stačí si postupně spočítat zbytky po dělení čísel $0^2, 1^2, \ldots, (m-1)^2$. Takto například zjistíme, že modulo 4 je kvadratický zbytek pouze 1 a modulo 7 pak 1, 2, 4.

Příklad. Dokaž, že liché číslo, které se dá napsat jako součet dvou čtverců[32], je nutně tvaru $4k + 1$ pro číslo k.

Důkaz. Nechť $c = a^2 + b^2$. Na tuto rovnici se můžeme podívat modulo 4. Víme, že x^2 modulo 4 může dávat pouze zbytky 0 a 1, takže součet $a^2 + b^2$ může nabývat pouze zbytků 0, 1, 2. Jelikož se ale má jednat o liché číslo, tak musí jít o zbytek 1, tedy $c = 4k + 1$.

Cvičení. Urči hodnoty těchto Legendreových symbolů za předpokladu, že p je prvočíslo:

$$\left(\frac{1}{p}\right), \quad \left(\frac{4-p^2}{p}\right), \quad \left(\frac{3}{5}\right), \quad \left(\frac{p}{2}\right).$$

Cvičení. Předpokládej, že $\left(\frac{-1}{p}\right) = -1$ pro prvočíslo p. Dokaž $\left(\frac{-4}{p}\right) = -1$.

Návod. Vezmi si $x^2 \equiv -4$ a zaměř se na číslo $\frac{x}{2}$, případně $\frac{x+p}{2}$.

Mohlo by nás zajímat, kolik vlastně je kvadratických zbytků (mezi čísly $1, \ldots, p-1$). Pokud si to vyzkoušíme na malých případech,[33] lehko tipneme, že odpověď je $\frac{p-1}{2}$ pro prvočíselné modulo p. Nejdříve si uvědomíme, že více jich nebude. Druhá mocnina má totiž užitečnou vlastnost $x^2 = (-x)^2$. Toho můžeme využít i zde, neboť

$$x^2 = (-x)^2 \equiv (p - x)^2 \pmod p.$$

To znamená, že čísla 1, $p - 1$, dále 2, $p - 2$, atd. dávají po umocnění na druhou stejný zbytek. Kvadratických zbytků bude tedy nejvýše $\frac{p-1}{2}$.

Zbývá dokázat, že jich bude alespoň tolik. To je ekvivalentní s tím, že čísla $1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ dávají po dvou různé zbytky. Stačí nám tedy dokázat, že pro celá čísla $a \neq b$, která splňují $0 < a, b \leq \frac{p-1}{2}$, neplatí $a^2 \equiv b^2 \pmod p$. Pro spor předpokládejme, že by to platilo. Pak

$$\begin{aligned} a^2 &\equiv b^2 \pmod p, \\ a^2 - b^2 &\equiv 0 \pmod p, \\ (a-b)(a+b) &\equiv 0 \pmod p. \end{aligned}$$

Má tedy platit $p \mid (a-b)(a+b)$. Ale p je prvočíslo, takže $p \mid (a-b)$ nebo $p \mid (a+b)$. Víme, že $a \neq b$, takže $a - b \neq 0$. Navíc $-\frac{p-1}{2} < a - b < \frac{p-1}{2}$, takže určitě $p \nmid (a-b)$. (To plyne z toho,

[32] Čtvercem myslíme druhou mocninu celého čísla.

[33] Do olympiády doporučujeme si zapamatovat kvadratické zbytky pro malá čísla.

že mezi $-\frac{p-1}{2}$ a $\frac{p-1}{2}$ je jen číslo 0 dělitelné p.) Ale $0 < a + b \leq (p-1)$, takže i $p \nmid (a+b)$. To je požadovaný spor.

Malá Fermatova[34] věta

V tomto odstavci se více podíváme na to, jak se zbytky násobí a mocní. Vezměme libovolné číslo a nesoudělné s m, umočňujme ho a počítejme zbytky mod m. Protože zbytků je jen konečně mnoho, najdeme dvě čísla $k > l$ tak, že $a^k \equiv a^l \pmod{m}$. To znamená, že $a^{(k-l)} \equiv 1 \pmod{m}$, neboť kongruenci můžeme vydělit číslem a^l nesoudělným s m. Našli jsme tedy přirozené číslo $r = k - l$ takové, že $a^r \equiv 1 \pmod{m}$. Nejmenší přirozené číslo s touto vlastností nazýváme *řád* prvku a modulo m a značíme jej $\mathrm{ord}_m(a)$. (Nebo pouze r, pokud to je z kontextu jasné.) Pokud číslo a je soudělné s m, řád neexistuje: pokud umočňujeme třeba 2 (mod 4), dostáváme $2, 0, 0, 0, \ldots$ a nikde žádná jednička.

Cvičení. Proč čísla soudělná s modulem nemají řád?

Návod. Pokud $a^r \equiv 1 \pmod{m}$, pak také $a^r \equiv 1 \pmod{(a, m)}$.

Cvičení. Jaký je řád 2 mod 5?

Tvrzení. („zbytky lze dělit") *Pro každé číslo a nesoudělné s m existuje právě jedna inverze modulo m, tj. prvek a' takový, že $aa' \equiv 1 \pmod{m}$. Obvykle inverzi značíme $\frac{1}{a}$ nebo a^{-1}.*

Důkaz. Nejprve si dokážeme, že takové číslo existuje alespoň jedno. Stačí si zvolit $a' = a^{r-1}$. Pak $a \cdot a' \equiv a \cdot a^{r-1} \equiv a^r \equiv 1 \pmod{n}$, tedy toto a' vyhovuje zadané podmínce.

Nyní si dokážeme, že je takové číslo (modulo m) jen jedno. Kdyby existovaly dvě různé inverze a' a a'' modulo n, tak $a \cdot a' \equiv 1 \equiv a \cdot a'' \pmod{m}$, a jelikož čísla a a m jsou nesoudělná, tak můžeme kongruenci $a \cdot a' \equiv a \cdot a'' \pmod{m}$ podělit číslem a. Tím dostaneme $a' \equiv a'' \pmod{m}$, což je spor s tím, že a' bylo různé od a''.

Cvičení. Dokažte předchozí tvrzení pomocí Bézoutovy věty.

To pro nás znamená, že v kongruencích můžeme používat i zlomky. Zlomkem $\frac{a}{b}$ jednoduše myslíme $a \cdot b^{-1}$. V kongruencích se tedy klidně může vyskytnout něco jako $\frac{1}{3} + \frac{1}{4} \equiv 0 \pmod{7}$. To proto, že inverze k číslu 3 modulo 7 je 5 (platí $3 \cdot 5 \equiv 1 \pmod{7}$) a inverze k číslu 4 je číslo 2. Takže $\frac{1}{3} + \frac{1}{4} \equiv 5 + 2 \equiv 0 \pmod{7}$. Naopak nemá v kongruencích modulo 6 smysl výraz $\frac{1}{2}$, protože čísla 2 a 6 jsou soudělná, a tedy číslo 2 nemá inverzi modulo 6.

Cvičení. Dokaž, že čísla, která jsou soudělná s m, inverzi modulo m nemají.

Cvičení. Dokaž, že zlomky můžeme v kongruencích upravovat podobně jako v obyčejných rovnicích. Tedy, že pro b, d nesoudělná s m platí:

(i) $\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod{m}$.
(ii) $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{m}$.

Nyní si ukážeme, k čemu se inverze například hodí, na důkazu Wilsonovy[35] věty.

Věta. (Wilsonova) *Nechť p je prvočíslo. Pak $(p-1)! \equiv -1 \pmod{p}$.*[36]

Důkaz. Podívejme se na číslo a mezi 1 a $p-1$. To je nesoudělné s p, takže má inverzi a^{-1}. Pokud $a \equiv a^{-1} \pmod{p}$, tak platí $a^2 \equiv 1 \pmod{p}$, neboli $(a+1)(a-1) \equiv 0 \pmod{p}$. Takže

[34] Pierre de Fermat (1601–1665) byl francouzský matematik amatér, povoláním právník.

[35] Wilsonova věta byla prý poprvé uvedena Ibn al-Haythamem (cca 1000 n. l.) a potom Waringem, jehož žákem byl Wilson. Ani jeden ze jmenovaných ji nedokázal, to udělal až Lagrange.

[36] Znakem $n!$ [n faktoriál] myslíme číslo $n \cdot (n-1) \cdots 1$.

$p \mid a+1$ nebo $p \mid a-1$. To ale znamená, že a je $p-1$ nebo 1. V ostatních případech tudíž platí $a \not\equiv a^{-1} \pmod p$. Ale pokud a má inverzi a^{-1}, tak zřejmě a^{-1} má inverzi a. Pokud tedy vynásobíme všechny zbytky od 2 do $p-2$, tak se každý zbytek popáruje se svojí inverzí a jejich součin bude 1. Proto

$$(p-1)! = (p-1)\cdot 1\cdot (2\cdot 3\cdots (p-2)) \equiv (-1)\cdot 1\cdot 1 \equiv -1 \pmod p.$$

Cvičení. Dokaž si ještě opačnou implikaci. Tedy pokud $(p-1)! \equiv -1 \pmod p$, tak p je prvočíslo.

Následující tvrzení popisuje důležitou vlastnost řádu.

Tvrzení. *Nechť a, n jsou nesoudělná čísla. Pak $a^n \equiv 1 \pmod p$ právě tehdy, když $r \mid n$.*

Návod. U jedné implikace stačí kongruenci umocnit. U druhé podělte n číslem r se zbytkem a ukažte, že r není řád, čímž dostanete spor.

Věta. (Malá Fermatova) *Nechť p je prvočíslo a a je číslo s ním nesoudělné. Potom $a^{p-1} \equiv 1 \pmod p$.*

Důkaz. Postupovat můžeme mnoha způsoby, například indukcí. My však předvedeme trochu jiný, poučný důkaz.

Vezměme r jako řád čísla a modulo p. Pro každé b od 1 do $p-1$ uvažujme množinu A_b obsahující zbytky čísel $b, ba, ba^2, \ldots, ba^{r-1}$ po dělení p. Dokažme si, že takováto množina má r prvků. Opravdu, kdyby $ba^k \equiv ba^l \pmod p$, kde $k > l$, dostali bychom $a^{k-l} \equiv 1 \pmod p$. Ale $k-l$ je menší než r, což je spor s tím, že r je řád, tedy nejmenší přirozené číslo, pro které platí $a^r \equiv 1 \pmod p$.

Pokud dvě z těchto množin A_b a A_c mají společný prvek $ba^k \equiv ca^l \pmod p$, potom pro libovolné i platí $ba^i \equiv ca^{(l-k)i} \equiv ca^x \pmod p$, kde x je zbytek čísla $(l-k)i$ po dělení r. Ale ca^x leží v A_c, tedy ba^i leží v A_c pro každé i od 0 do $p-1$. Jinak řečeno, každý prvek A_b je také prvkem A_c. Obdobně dostaneme i to, že prvky A_c jsou v množině A_b. To znamená, že $A_b = A_c$. Každé dvě množiny jsou tedy buď disjunktní (nemají žádný společný prvek), nebo se sobě rovnají.

Pokud označíme počet různých množin A_b (pro b od 1 do $p-1$) jako s, dostáváme, že $rs = p-1$, neboť sjednocením všech množin A_b dostaneme celou množinu zbytků (až na 0), tedy $p-1$ čísel. Z toho plyne, že $r \mid p-1$, takže $a^{p-1} \equiv 1 \pmod p$ podle předchozího tvrzení.

Díky MFV[37] se můžeme dozvědět více o kvadratických zbytcích.

Příklad. Nechť p je liché prvočíslo. Ukaž, že pokud je -1 kvadratický zbytek modulo p, potom je p tvaru $4k+1$ pro nějaké číslo k.

Řešení. Pro spor předpokládejme, že $p = 4k+3$. Protože $x^2 \equiv -1 \pmod p$ pro nějaké x, máme $x^{p-1} \equiv x^{4k+2} \equiv (x^2)^{2k+1} \equiv -1 \pmod p$, což je spor s MFV.

Nyní si ukážeme užitečný způsob, jak zjistit, jestli je číslo zbytek, nebo nezbytek.

Tvrzení. (Eulerovo[38] kritérium) *Nechť p je liché prvočíslo a a je číslo nesoudělné s p, potom $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.*

Důkaz. Předpokládejme, že a není kvadratický zbytek modulo p. Chceme dokázat, že potom $a^{\frac{p-1}{2}}$ dává zbytek -1 po dělení p. Pro spor předpokládejme, že to neplatí. Mějme číslo b mezi 1 a $p-1$. Pak má kongruence $bx \equiv a \pmod p$ právě jedno řešení v x modulo p, a to $b' = ab^{-1}$. Kdyby $b' = b$, tak by platilo $b^2 \equiv a \pmod p$, tedy a by byl kvadratický zbytek modulo p, což

[37] Takto budeme označovat Malou Fermatovu větu.

[38] Leonhard Euler (1707–1783) byl švýcarský matematik působící (hlavně) v Petrohradu.

je spor. Musí tudíž platit $b' \neq b$. Pak se čísla 1 až $p-1$ po vynásobení popárují do dvojic se zbytkem a, a tedy bude platit

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

Z Wilsonovy věty plyne, že $(p-1)!$ dává zbytek -1 po dělení p, takže $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Sám si jako cvičení dokaž opačnou implikaci.

Pomocí Eulerova kritéria si můžeš dokázat, že v předešlém příkladu platí i opačná implikace:

Cvičení. Ukaž, že pokud je prvočíslo p tvaru $4k+1$, tak -1 je kvadratický zbytek modulo p.

Cvičení. (těžké) Dokaž, že prvočísel tvaru $4k+1$ je nekonečně mnoho.

Návod. Uvaž číslo $(n!)^2+1$ a ukaž, že má prvočíselného dělitele p tak, že -1 je kvadratický zbytek modulo p.

Nyní se seznámíme s důležitou funkcí, se kterou se budeme setkávat během celého seriálu.

Definice. *Eulerova funkce* $\varphi(n)$ je počet přirozených čísel nesoudělných s n a menších či rovných n.

Podívejme se, jak se funkce chová na prvočíslech. Mějme prvočíslo p. Potom každé přirozené číslo menší než p je s p nesoudělné. Proto $\varphi(p) = p-1$.

Pro mocniny prvočísel je situace podobně jednoduchá. Pokud máme číslo p^k, kde p je prvočíslo, tak nesoudělná čísla jsou právě ta, která nejsou dělitelná p. Ale čísel dělitelných p od 1 do p^k je $\frac{p^k}{p} = p^{k-1}$. Proto je nesoudělných čísel $p^k - p^{k-1}$.

Abychom mohli funkci spočítat pro libovolné n, musíme ještě dokázat zásadní vlastnost Eulerovy funkce, kterou nazýváme *multiplikativita*.

Tvrzení. *Eulerova funkce je multiplikativní, tedy pro nesoudělná čísla a, b platí $\varphi(ab) = \varphi(a)\varphi(b)$.*

Důkaz. Napišme si všechna čísla $0, 1, \ldots, ab-1$ do tabulky – jednoduše po řádcích zleva doprava.

0	1	2	...	$a-1$
a	$a+1$	$a+2$	...	$2a-1$
...	...	...	...	...
$a(b-1)$	$a(b-1)+1$	$a(b-1)+2$	...	$ab-1$

Koukněme se na číslo v řádku i a sloupci j, přičemž řádky a sloupce značíme od nuly. Pak je na tomto místě napsané číslo $ia+j$. Zajímá nás, zda je soudělné s ab. Jelikož jsou ale čísla a a b nesoudělná, tak stačí zjistit, jestli je $ia+j$ nesoudělné jak s a, tak s b. Aby bylo číslo nesoudělné s a, tak musí být $(ia+j, a) = 1$, tedy $(j, a) = 1$. To ale znamená, že čísla nesoudělná s ab mohou být jen ve sloupcích označených čísly, která jsou nesoudělná s a. Těchto sloupců je $\varphi(a)$.

Podívejme se na čísla v jednom z těchto sloupců. Jsou to čísla $j, a+j, 2a+j, \ldots, (b-1)a+j$. Tato čísla dávají navzájem různé zbytky modulo b. (Rozmysli si, že to platí – předpokládej, že by dvě čísla byla navzájem kongruentní modulo b, a dojdi ke sporu.)

Čísla tedy dávají v nějakém pořadí zbytky $0, 1, \ldots, b-1$ modulo b. Právě $\varphi(b)$ z nich je nesoudělných s b, a tedy i s ab. V každém z uvažovaných $\varphi(a)$ sloupců máme $\varphi(b)$ čísel nesoudělných s ab, dohromady je tedy čísel nesoudělných s ab přesně $\varphi(a)\varphi(b)$, což jsme chtěli dokázat.

Díky multiplikativitě dostáváme pro $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ vztah

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Cvičení. Uprav vzoreček do tvaru

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right).$$

Seriál zakončíme kouzelnou formulí.

Tvrzení. *Platí*

$$\sum_{d\mid n}\varphi(d) = n.$$

Pokud Tě zaráží symbol $\sum$, rádi Ti ho vysvětlíme. Říká se mu *suma* a značí součet několika členů. Například $\sum_{k=1}^{n} a_k$ znamená $a_1 + a_2 + \dots + a_n$ (tj. sečti a_k pro k od 1 do n). Když pod sumou píšeme $d \mid n$, tak tím myslíme součet přes všechny kladné dělitele d čísla n. Například $\sum_{d\mid 6}\varphi(d) = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1+1+2+2 = 6$.

Naše formule tedy říká, že pokud sečteme $\varphi(d)$ přes všechny dělitele d čísla n, tak dostaneme přesně n. Ale ještě si to musíme dokázat! Držte si klobouky.

Důkaz. Budeme potřebovat rozklad čísla n na prvočísla $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Nejprve si musíme uvědomit, že součet všech dělitelů se dá zapsat takto:

$$\sum_{d\mid n} d = \big(1+p_1+p_1^2+\dots+p_1^{\alpha_1}\big)\big(1+p_2+p_2^2+\dots+p_2^{\alpha_2}\big)\dots\big(1+p_k+p_k^2+\dots+p_k^{\alpha_k}\big).$$

Pokud totiž roznásobíme všechny závorky na pravé straně, dostaneme každého dělitele čísla n právě jednou. Ale s využitím toho, že funkce φ je multiplikativní, můžeme psát i toto:

$$\sum_{d\mid n}\varphi(d) = \big(\varphi(1)+\varphi(p_1)+\dots+\varphi(p_1^{\alpha_1})\big)\dots\big(\varphi(1)+\varphi(p_k)+\dots+\varphi(p_k^{\alpha_k})\big).$$

My ale víme, že $\varphi(p^k) = p^k - p^{k-1}$, takže

$$\varphi(1)+\varphi(p_i)+\dots+\varphi(p_i^{\alpha_i}) = 1+(p_i-1)+(p_i^2-p_i)+\dots+(p_i^{\alpha_i}-p_i^{\alpha_i-1}) = p_i^{\alpha_i}.$$

To nám dohromady dává

$$\sum_{d\mid n}\varphi(d) = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k} = n.$$

1. podzimní série – Čtverečkovaný papír

Výsledková listina

1.–6.	*Eduard*	*Batmendijn*	3	CGStĽubovňa	– – – 5 5 5 5 5	25	**25,00**
1.–6.	*Filip*	*Bialas*	1	GOpatovPH	3 3 3 5 5 5 5 5 5	25	**25,00**
1.–6.	*Martin*	*Hora*	4	GMikul23PL	– 3 – 5 5 5 5 5	$25+i$	**25,00**
1.–6.	*Katarína*	*Krajčiová*	3	GAlejKošic	3 – 3 5 5 5 5 5	$25+i$	**25,00**
1.–6.	*Václav*	*Rozhoň*	3	GJirsíkaČB	3 – 3 5 5 5 5 5	25	**25,00**
1.–6.	*Radovan*	*Švarc*	3	G ČTřebová	0 0 3 5 5 5 5 5	25	**25,00**
7.	*František*	*Couf*	1	GZborovPH	3 3 3 5 5 5 5 4	$24+i$	**24,62**
8.	*Pavel*	*Turek*	1	GTomkovaOL	3 3 – 4 5 5 5 4	23	**24,07**
9.	*Václav*	*Steinhauser*	0	ZŠVranéNVl	3 3 3 5 5 5 – –	21	**23,47**
10.	*Karolína*	*Kuchyňová*	3	GMLerchaBO	3 – 3 5 5 4 5 4	$23+i$	**23,37**
11.	*Marko*	*Puza*	4	GPošKošice	3 – – 5 5 5 5 4	24	**23,17**
12.	*Jakub*	*Löwit*	2	GČeskoliPH	3 3 3 1 5 5 5 4	22	**22,93**
13.	*Ondřej*	*Darmovzal*	3	GJarošeBO	3 3 3 5 5 5 – 4	22	**22,91**
14.	*Martin*	*Surma*	3	GJWolkraPV	3 3 3 4 5 5 5 1	22	**22,59**
15.	*Anh Dung*	*Le*	4	G Tachov	3 3 – 5 5 5 5 4	24	**22,33**
16.–17.	*Jakub*	*Svoboda*	4	G KomHavíř	0 3 – 4 5 5 5 4	23	**22,17**
16.–17.	*Martin*	*Špilar*	3	G Vyškov	3 2 3 – 5 5 5 –	21	**22,17**
18.	*Jan*	*Soukup*	3	G Klatovy	3 3 – 3 5 5 5 5	23	**21,92**
19.	*Miroslav*	*Stankovič*	4	GPošKošice	3 – – 5 – 5 5 5	$23+i$	**21,80**
20.	*Markéta*	*Horová*	2	GMikul23PL	3 3 3 5 – 5 – –	19	**21,52**
21.	*Martin*	*Kopřiva*	2	GMikul23PL	3 3 3 5 0 5 – –	19	**21,45**
22.	*Miroslav*	*Psota*	4	GHlinŽilina	3 – – 5 5 – 5 4	$22+i$	**21,26**
23.	*Anna*	*Steinhauserová*	4	G Dačice	3 2 3 5 5 5 – 5	23	**21,18**
24.	*Jan*	*Krejčí*	4	G Bílovec	3 3 – 4 5 5 3 5	22	**21,17**
25.	*Daniela*	*Šindelářová*	2	GaSOŠ Telč	3 2 3 5 1 5 – 0	18	**20,84**
26.	*Mikuláš*	*Zindulka*	3	GMikul23PL	3 3 3 5 5 2 – –	19	**20,63**
27.	*Jakub*	*Šebek*	4	GKepleraPH	3 3 3 4 5 2 5 4	21	**20,52**
28.	*Antonín*	*Češík*	4	SPŠElek PA	3 3 3 5 5 5 – –	21	**20,01**
29.	*Vojtěch*	*Suchánek*	3	GJarošeBO	3 3 3 5 – – – 4	18	**19,83**
30.	*Victoria María*	*Nájares Romero*	0	GZborovPH	3 2 3 – – – 5 –	13	**19,76**
31.	*Andrea*	*Kučerová*	2	G ČKrumlov	3 3 3 5 2 0 – –	16	**19,37**
32.	*Kateřina*	*Nová*	1	G Vimperk	3 3 3 4 – – 1 –	14	**19,28**
33.	*Viktor*	*Němeček*	3	GJMasar JI	3 3 – 5 4 – – 5	20	**19,21**
34.	*Tomáš*	*Fiala*	3	GLedečNSáz	3 3 3 5 – 1 4 3	$18-i$	**19,14**
35.	*Vojtěch*	*Lanz*	0	GZborovPH	3 2 3 3 1 – 1 –	12	**19,02**
36.	*Jakub*	*Dargaj*	4	GPošKošice	3 0 3 5 5 5 – –	21	**18,60**
37.	*Anežka*	*Michálková*	2	GaSOŠ Telč	3 2 3 – 2 5 – –	15	**18,59**
38.	*Jiří*	*Češka*	1	CMGProstěj	3 2 3 3 2 – – –	13	**18,52**
39.	*Zuzana*	*Svobodová*	2	G FrýdlNOs	3 3 3 2 1 5 – –	16	**18,43**

40.	*Petr*	*Jakubčík*	0	PORG PH	3 2 1 5 – – – –	11	**18,23**
41.–42.	*Vojtěch*	*Linhart*	3	SlovanG OL	3 3 3 – – 5 2 –	16	**18,15**
41.–42.	*Lukáš*	*Sadlek*	3	G Čadca	3 2 1 5 1 5 1 1	16	**18,15**
43.	*Kristýna*	*Šmídová*	4	GMensaPH	3 3 3 5 – 5 – –	19	**18,02**
44.	*Martin*	*Minasjan*	4	GKepleraPH	3 3 3 – 5 – 5 0	19	**17,82**
45.	*Jan*	*Kadlec*	3	G Klatovy	3 2 3 3 5 5 – 0	19	**17,79**
46.	*Štefan*	*Račák*	2	GTajBanBys	3 0 2 1 3 5 1 0	14	**17,77**
47.	*Tereza*	*Kislingerová*	1	G Klatovy	3 2 3 3 1 – 1 –	12	**17,70**
48.	*Jakub*	*Hledík*	3	GSŘMRSkuteč	3 3 – 5 – 5 – –	16	**17,40**
49.	*Minh Tri*	*Pham*	2	NPorg	3 3 3 5 – – – –	14	**17,34**
50.–51.	*Minh Thao*	*Nguyen*	2	GEBenešeKL	3 3 1 5 – 0 1 –	13	**16,90**
50.–51.	*Marian*	*Poljak*	2	GJŠkodyPŘ	3 2 3 – 5 – – –	13	**16,90**
52.	*Jan*	*Šorm*	2	GJarošeBO	3 2 3 5 1 – – –	14	**16,57**
53.	*Lenka*	*Kopfová*	0	CZŠSL HnM	3 3 3 – – – – –	9	**16,42**
54.	*Miroslav*	*Krabec*	4	G KomHavíř	3 3 3 4 5 – 3 –	18	**16,11**
55.–57.	*Daniel*	*Backov*	2	G Ružomb	3 1 3 4 0 1 1 0	12	**16,00**
55.–57.	*Michaela*	*Brabcová*	2	G Jírov ČB	3 2 – 1 5 1 – 0	12	**16,00**
55.–57.	*Patricie*	*Klosse*	2	G ČKrumlov	3 2 3 4 – – – –	12	**16,00**
58.	*Marie*	*Vonzino*	1	GTomkovaOL	2 2 3 2 1 1 1 –	10	**15,89**
59.	*Martin*	*Raszyk*	4	G Karviná	3 3 3 4 5 5 – –	20	**15,53**
60.	*Tereza*	*Rašková*	3	GTomkovaOL	3 2 1 – – 5 2 0	13	**15,43**
61.	*Dominik*	*Krasula*	1	G Krnov	3 3 3 1 1 – 0 1	11	**15,32**
62.	*Markéta*	*Ospálková*	1	G Uničov	3 2 – – 2 – 2 0	9	**14,89**
63.–64.	*Radim*	*Bárta*	3	GJarošeBO	3 3 – 2 – 3 1 –	12	**14,47**
63.–64.	*Jan*	*Knížek*	3	G Strakon	3 1 3 5 – – – –	12	**14,47**
65.	*Kristýna*	*Šudomová*	2	GValašKlob	3 2 1 – 0 5 – 0	11	**14,38**
66.–67.	*Matěj*	*Konečný*	3	G Jírov ČB	3 3 3 – 5 – – –	14	**14,27**
66.–67.	*Přemysl*	*Šťastný*	0	G Žamberk	3 3 – – 1 – – –	7	**14,27**
68.–72.	*Petr*	*Červenka*	2	GNadKavaPH	3 2 3 0 1 1 1 0	10	**14,05**
68.–72.	*Jozef*	*Mišt*	2	GAHŠ VKrtíš	3 2 3 – – 1 1 –	10	**14,05**
68.–72.	*Jakub*	*Starý*	2	VOŠKutHora	3 2 3 1 1 0 0 0	10	**14,05**
68.–72.	*Jakub*	*Ševčík*	2	GKukučPopr	3 3 3 1 – – – 0	10	**14,05**
68.–72.	*Jana*	*Vráblíková*	2	GLesníZlín	3 2 3 1 0 – 1 –	10	**14,05**
73.	*David*	*Ucháč*	1	VOŠDoprPH	3 2 2 – – 0 1 –	8	**13,81**
74.	*Marián*	*Poppr*	3	GJNerudyPH	3 2 3 1 1 5 2 –	15	**13,69**
75.	*Emese*	*Szabó*	3	GZKMJ Gal	3 2 – – 1 5 – –	11	**13,47**
76.	*Barbora*	*Pešlová*	3	G Vimperk	3 3 1 3 2 1 1 0	12	**13,41**
77.	*Jan*	*Jurka*	3	GMLerchaBO	3 3 – – 5 – – –	11	**13,33**
78.–85.	*Martin*	*Konečný*	2	GStrážnice	3 2 3 – 0 – 1 –	9	**13,00**
78.–85.	*Mihály*	*Kotiers*	2	GHSelyhoKM	3 3 3 – – – – –	9	**13,00**
78.–85.	*Tomáš*	*Kuzma*	2	GAB Senec	3 2 1 – 1 1 2 0	9	**13,00**
78.–85.	*Vojtěch*	*Lukeš*	2	G LPika PL	3 3 3 – – – – –	9	**13,00**
78.–85.	*Matyáš*	*Medek*	4	GMozartovaPA	3 1 3 4 2 1 1 0	13	**13,00**
78.–85.	*Jakub*	*Schinko*	2	GNadKavaPH	3 2 3 – – – 1 0	9	**13,00**
78.–85.	*Jan*	*Václavek*	2	G Ústí n O	3 3 3 – – – – 0	9	**13,00**
78.–85.	*Lukáš*	*Zíb*	2	GPísnickPH	3 2 2 1 0 1 0 0	9	**13,00**
86.–87.	*Jakub Josef*	*Slavík*	1	BiskG Brno	3 2 0 1 0 – 1 –	7	**12,64**
86.–87.	*Jáchym*	*Solecký*	1	PORG PH	3 2 – – – – 2 –	7	**12,64**
88.–89.	*Jakub*	*Sláma*	3	GOpatovPH	3 2 3 – 1 0 1 –	10	**12,45**
88.–89.	*Martin*	*Šourek*	3	GCoubTábor	3 2 3 1 – 1 – –	10	**12,45**
90.–98.	*Michaela*	*Brezinová*	2	GKomTrebiš	3 2 3 – – – – 0	8	**11,89**

90.–98.	*Tomáš*	*Flaschka*	2	G Hlučín	3 2 3 – – – – –	8	**11,89**
90.–98.	*Jakub*	*Hrubý*	2	G Chrudim	3 2 1 1 1 1 0 0	8	**11,89**
90.–98.	*Vít*	*Kalisz*	2	FSG Pirna	3 2 3 – – 0 – –	8	**11,89**
90.–98.	*Martin*	*Kutiš*	2	G Humpolec	3 2 1 1 – – 1 0	8	**11,89**
90.–98.	*Jakub*	*Marták*	2	G GolNitra	3 2 2 1 0 0 0 0	8	**11,89**
90.–98.	*David*	*Peňáz*	2	GNeumannŽR	3 2 3 – 0 – – –	8	**11,89**
90.–98.	*Adam*	*Říha*	2	G ČesLípa	3 2 2 0 0 0 1 0	8	**11,89**
90.–98.	*Tomáš*	*Velich*	2	GJHroncaBA	3 2 1 1 1 – 0 0	8	**11,89**
99.–100.	*Markéta*	*Calábková*	3	GJŠkodyPŘ	3 3 – – 1 – – 4	11	**11,76**
99.–100.	*Pavlína*	*Hartmanová*	2	G Broumov	3 2 3 – – – – –	8	**11,76**
101.	*Vojtěch*	*Juříček*	2	G Kralupy	3 2 – 3 – – – –	8	**11,70**
102.	*Borek*	*Požár*	0	G Rakovník	3 2 – – – – – –	5	**11,66**
103.–104.	*Jiří*	*Štrincl*	3	GSRandyJN	3 2 3 – – 1 – 0	9	**11,39**
103.–104.	*Marek*	*Vícha*	3	MendelG OP	3 3 3 – – – – –	9	**11,39**
105.–106.	*Lukáš*	*Kubacki*	1	GNadKavaPH	3 3 – – – – – –	6	**11,38**
105.–106.	*Zuzana*	*Tréglová*	1	G Žatec	3 3 – – – 0 – –	6	**11,38**
107.	*Michaela*	*Bieliková*	4	G Sereď	3 3 3 4 – – – –	13	**11,26**
108.	*Henrieta*	*Micheľová*	2	GAlejKošic	3 2 3 – – – – –	8	**10,92**
109.–113.	*Jiřina*	*Duspivová*	2	G Kralupy	3 2 1 – – 1 – –	7	**10,72**
109.–113.	*Petra*	*Kratochvílová*	2	GHustopeče	3 2 1 1 – 0 – –	7	**10,72**
109.–113.	*Daniel*	*Krejbych*	2	G Litomyšl	3 2 1 1 0 0 – –	7	**10,72**
109.–113.	*Anh*	*Le Hoang*	2	GJarošeBO	3 2 1 – 1 – – –	7	**10,72**
109.–113.	*Jaroslav*	*Stránský*	2	G Tišnov	3 2 – – 1 1 – –	7	**10,72**
114.	*Nicholas*	*Čapek*	4	GBNěmcovHK	1 2 3 4 2 – – –	12	**10,52**
115.–116.	*Michael*	*Bucha*	3	G Zábřeh	3 2 3 – – – – –	8	**10,30**
115.–116.	*Marek*	*Štěpán*	3	SPŠE Fren	3 2 3 – – – – 0	8	**10,30**
117.	*Barbora*	*Hudcová*	4	PORG PH	3 1 3 4 – – – –	11	**10,09**
118.	*Petr*	*Lukeš*	4	GNeumannŽR	3 2 3 4 – – – –	12	**10,06**
119.–122.	*Dominik*	*Hodan*	1	GNadAlejPH	3 2 – – – – – –	5	**10,00**
119.–122.	*Věra*	*Tesařová*	1	MasG Plzeň	3 2 – – 0 – – 0	5	**10,00**
119.–122.	*The Minh*	*Tran*	1	PČGKarVary	3 2 – – – – – –	5	**10,00**
119.–122.	*Kateřina*	*Volková*	1	MG Vsetín	3 1 1 – 0 – 0 0	5	**10,00**
123.–127.	*Tomáš*	*Beneš*	2	GVráLevice	3 2 1 – – – – –	6	**9,48**
123.–127.	*Martin*	*Chabada*	2	G Bardejov	1 0 3 – – 1 1 0	6	**9,48**
123.–127.	*Lukáš*	*Honsa*	2	G Jírov ČB	3 – 3 – – – – –	6	**9,48**
123.–127.	*Lucie*	*Roškotová*	2	G Turnov	3 – 3 – – – – –	6	**9,48**
123.–127.	*Peter Kulcsár*	*Szabó*	2	GHSelyhoKM	3 2 – – 1 – – –	6	**9,48**
128.	*Jan*	*Erhart*	3	GFXŠaldyLI	3 2 3 – – 1 – –	9	**9,45**
129.–134.	*Cedrik*	*Horčička*	3	G ČesLípa	3 0 3 – 0 – 1 0	7	**9,17**
129.–134.	*Tereza*	*Koberová*	3	G Chrudim	1 3 3 – – 0 – –	7	**9,17**
129.–134.	*Denisa*	*Kolenčíková*	3	GNámestovo	3 2 2 – 0 – – –	7	**9,17**
129.–134.	*Jan*	*Krůza*	3	GVPavlovic	3 2 0 – 1 0 1 –	7	**9,17**
129.–134.	*Tomáš*	*Vaníček*	3	G Jírov ČB	2 1 3 1 0 – – –	7	**9,17**
129.–134.	*Peter*	*Vook*	3	GPošKošice	3 1 3 – – – – –	7	**9,17**
135.	*Daniel*	*Kočik*	4	GŠroKošice	3 3 3 – – – – –	9	**9,00**
136.	*Lenka*	*Vincenová*	0	GTomkovaOL	2 0 1 – 0 – – –	3	**8,34**
137.	*Daniel*	*Pišťák*	2	GZborovPH	1 2 3 – – 1 – –	7	**8,23**
138.–141.	*Katarína*	*Behinská*	2	G GolNitra	3 0 2 – 0 – – –	5	**8,17**
138.–141.	*Matěj*	*Kosma*	2	SOŠDoprOS	3 2 – – – – – –	5	**8,17**
138.–141.	*Dennis*	*Ryšánek*	2	SPŠÚžlabPH	1 2 1 – – 0 1 0	5	**8,17**
138.–141.	*Adéla*	*Šedová*	2	GJungmanLT	3 2 – – – – – –	5	**8,17**

142.–146.	*Antonie*	*Brožová*	4		3 2 3 – – – – –	8	**8,00**
142.–146.	*Veronika*	*Holubová*	3	PORG PH	3 1 2 – 0 – – –	6	**8,00**
142.–146.	*Jakub*	*Kříž*	4	SPŠ PB	3 2 3 – – – – –	8	**8,00**
142.–146.	*Matěj*	*Sháněl*	4	G VysMýto	3 2 1 – – 1 1 –	8	**8,00**
142.–146.	*Tomáš*	*Valovič*	4	GAHŠ VKrtíš	3 2 1 – 1 1 1 –	8	**8,00**
147.	*Vendula*	*Kotyzová*	4	WichtG OS	3 2 3 – – 1 – –	9	**7,76**
148.	*Ivona*	*Hrivová*	4	GOkrŽilina	3 2 3 1 – 0 – –	9	**7,38**
149.–151.	*Adam*	*Gálik*	4	GOlivuPopr	3 0 0 0 1 1 2 0	7	**7,00**
149.–151.	*Otto*	*Hollmann*	4	GUBalvanJN	3 2 – – – 0 2 0	7	**7,00**
149.–151.	*Marie*	*Koutná*	4	GTNovákBO	3 3 1 – – – – –	7	**7,00**
152.–156.	*Levente*	*Berky*	3	GZKMJ Gal	3 2 – – – 0 – –	5	**6,79**
152.–156.	*Michaela*	*Biová*	3	MendelG OP	3 0 2 0 – – 0 0	5	**6,79**
152.–156.	*Kristýna*	*Davídková*	1	OA Liberec	3 – – – – – – –	3	**6,79**
152.–156.	*Anna*	*Filipová*	3	G Kolín	3 2 – – – – – –	5	**6,79**
152.–156.	*Jana*	*Menšíková*	1	G Frýdlant	3 0 – – – – – –	3	**6,79**
157.–158.	*Alena*	*Košáková*	2	G Strakon	3 0 1 – – – – –	4	**6,76**
157.–158.	*Ronald*	*Luc*	2	GJarošeBO	3 1 – – – – – –	4	**6,76**
159.	*Tran Vi Thanh*	*Pham*	4	GNeumannŽR	3 2 3 – – – – –	8	**6,59**
160.	*Jaromír*	*Mielec*	1	GVolgogrOS	3 1 0 – – 0 – –	4	**6,45**
161.	*Kristýna*	*Ilievová*	3	G Milevsko	3 3 – – – – – –	6	**5,78**
162.	*Tomáš*	*Konečný*	1	GJirsíkaČB	3 – – – – – – –	3	**5,75**
163.–165.	*Stanislav*	*Kruml*	3	G Chotěboř	3 1 – – – – – –	4	**5,53**
163.–165.	*Barbora*	*Kubicová*	3	PORG PH	3 1 0 0 0 – – –	4	**5,53**
163.–165.	*Vít*	*Maroščík*	3	G Bohumín	3 0 0 1 0 0 0 0	4	**5,53**
166.–167.	*Valentína*	*Straková*	4	G Sereď	3 3 – – – – – –	6	**5,36**
166.–167.	*Ľudmila*	*Šimková*	4	GPároNitra	3 – 3 – – – – –	6	**5,36**
168.–170.	*Matěj*	*Kašťák*	2	G Hlohovec	3 0 – – – – – –	3	**5,27**
168.–170.	*Kryštof*	*Kolář*	2	GJarošeBO	3 – – – – – – –	3	**5,27**
168.–170.	*Marina*	*Pogarčenko*	2	GJungmanLT	3 – – – – – – –	3	**5,27**
171.	*Jan*	*Alfery*	2	GNPražačPH	0 3 – – – – – –	3	**5,09**
172.	*Jaromír*	*Kuchyňka*	4	GStrážnice	3 2 – – – – – –	5	**5,00**
173.	*Karel*	*Vlachovský*	2	MasG Plzeň	3 – – – – – – –	3	**4,90**
174.–176.	*Petr*	*Gintar*	3	MendelG OP	1 0 1 1 0 0 0 0	3	**4,23**
174.–176.	*Jan*	*Lukáč*	3	G ČKrumlov	3 0 – – 0 – – 0	3	**4,23**
174.–176.	*Silvia*	*Nepšinská*	3	GJChalBR	3 – – – – – – –	3	**4,23**
177.	*Ondřej*	*Broža*	4		1 1 1 0 – 0 1 0	4	**4,00**
178.	*Zuzana*	*Vlasáková*	4	G Rumburk	3 2 – – – – – –	5	**3,95**
179.	*Jaroslav*	*Cerman*	2	GJilemnice	2 0 0 – – – 0 –	2	**3,65**
180.–181.	*Ondřej*	*Havlík*	3	MSOŠ Klob	1 0 0 0 0 0 1 0	2	**2,88**
180.–181.	*Rostislav*	*Lukosz*	3	G Bohumín	2 0 – – – 0 – –	2	**2,88**
182.	*Marcela*	*Fialová*	4	SOŠ Kolín	2 0 0 0 0 – – –	2	**2,00**
183.–185.	*Irena*	*Bačinská*	4	ŠpMNDaG BA	0 0 – – – 0 – –	0	**0,00**
183.–185.	*Kateřina*	*Fuková*	1	GOhradníPH	0 0 – – – – – –	0	**0,00**
183.–185.	*Václav*	*Krchňák*	2	GJarošeBO	– 0 – – – – – –	0	**0,00**

adresa: *Korespondenční seminář*
KAM MFF UK
Malostranské náměstí 25
118 00 Praha 1
web: *http://mks.mff.cuni.cz/*
e-mail: *mks@mff.cuni.cz*