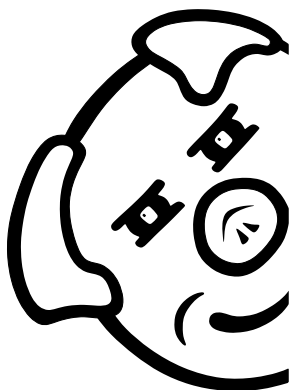


# Matematický korespondenční seminář

## Milý příteli !



Podzimní část semináře se pomalu chýlí ke konci. Zbývá nám už jen cizojazyčná série, která však umí celkovým pořadím ještě řádně zamíchat. Ti nejlepší z vás se poté budou moct těšit na jarní soustředění. Jestliže se vám na podzim nedařilo, nevěšte hlavu, není vše ztraceno! Na podzimní soustředění totiž zveme naopak nejlepší řešitele jarní části. Šance na úspěch je velká, neboť podle pravidel nejsou na podzimní soustředění zvaní maturanti. Ani ti ale nepřijdou zkrátka – stále mohou soutěžit o zajímavé ceny.

Za organizátory zdraví

Martina Vaváčková

### Co dále najdeš v komentářích?

- Povídání ke druhé jarní sérii
- Vzorové řešení 2. a 3. podzimní série
- Vzorové řešení 1. seriálové série
- Seriál – Teorie čísel II
- Výsledkové listiny
  
- Příloha: Zadání 1. a 2. jarní série a 2. seriálové série

### Podzimní soustředění v Horních Lysečínách

Odměnou za jarní část semináře je každoročně podzimní soustředění. V listopadu se tak nejlepší řešitelé (v domnění, že jedou do Krkonoš) objevili v Matrixu, kde bojovali proti zlým agentům a snažili se zachránit svět. K tomu, aby uspěli, podstoupili systematickou přípravu, na vesmírné lodi prohlubovali své matematické znalosti, mezi přednáškami sportovali, učili se taktizovat v hrách a ve skvělém kolektivu znovu načerpali síly. Veškeré hrozící nebezpečí bylo tedy odvráceno a všichni se v pořádku vrátili domů.

Těšíme se na další soustředění!

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



## Co se chystá

**Soustředění iKS** (neděle 9. března – pátek 14. března). Československý seminář pro borce iKS má své historicky třetí soustředění, opět pojaté jako příprava na celostátní kolo Matematické olympiády. Bližší informace o iKSkou naleznete na jeho stránkách [www.iksko.org](http://www.iksko.org).

**Jarní výlet** (sobota 22. března 2013). Tradiční akce PraSátka – sraz organizátorů, řešitelů a přátel semináře. Pojed s námi strávit jarní den do přírody, popovídat si, potkat nové i známé řešitele a organizátory a užít si spoustu legrace. Bližší informace se včas se objeví na webu semináře, pozvánku dostaneš s příštími komentáři.

**Náboj** (pátek 11. dubna 2014). Náboj je týmová matematická soutěž, kterou pro vás pořádáme ve spolupráci s bratislavským Matematickým korespondenčním seminářem, a to v Praze, Opavě, Bratislavě, Košicích a nově i bavorském Pasově (a možná i jinde). Další informace a přihlášku naleznete na webu soutěže [www.naboj.org](http://www.naboj.org).

**Jarní soustředění** (neznámé datum). Místo i téma jarního soustředění je tradičně tajné. Prozatím je tajné i datum, ale informace budou včas na webu i v dopisních schránkách.

# Povídání ke druhé jarní sérii

Tématem druhé jarní série jsou iracionální čísla. Většina z vás je už určitě zná ze školy, jistě však nebude na škodu si o nich něco připomenout. V běžném životě často pracujeme s čísly přirozenými a celými. K tomu, abychom mohli bez problémů dělit, byla zavedena čísla racionální. To jsou všechna čísla, která se dají napsat ve tvaru  $\frac{a}{b}$ , kde  $a$  je celé a  $b$  přirozené. Jsou-li navíc  $a$  a  $b$  nesoudělná, je tento zápis jednoznačný a říkáme, že zlomek  $\frac{a}{b}$  je v základním tvaru.

Všechna racionální čísla se v desítkové soustavě (ale i v jiných soustavách) dají vyjádřit pomocí desetinného zápisu, který je buď ukončený (tj. za desetinnou čárkou je pouze konečně mnoho číslic), nebo periodický (tj. od určitého místa za desetinnou čárkou se opakuje stále stejná konečná posloupnost číslic). Periodu obvykle značíme „nadčarou“. Uvedeme několik příkladů racionálních čísel:  $\frac{3}{5} = 0,6$ ,  $\frac{41}{80} = 0,5125$ ,  $\frac{2}{3} = 0,\overline{6}$ ,  $\frac{116}{495} = 0,2\overline{34}$ . Není těžké si rozmyslet, že součet, rozdíl, součin i podíl dvou racionálních čísel je opět racionální (u podílu musíme předpokládat, že dělitel není roven nule).

Na kladná racionální čísla můžeme pohlížet jako na délky úseček – udávají vzdálenost dvou bodů. Přirozeně vyvstává otázka, zdali existují i vzdálenosti, které se nedají zapsat jako podíl dvou celých čísel. Odpověď znali už staří Řekové, kteří uměli dokázat, že takové vzdálenosti opravdu existují. Příkladem je délka úhlopříčky ve čtverci o straně 1, jak uvidíme později. Tato čísla – spolu s čísly k nim opačnými – nazýváme iracionální.

Racionální čísla spolu s iracionálními tvoří čísla reálná. Iracionální čísla nelze zapsat ve tvaru podílu dvou celých čísel, což je ekvivalentní tomu, že mají neukončený neperiodický desetinný rozvoj. Řadí se mezi ně slavná čísla jako  $\pi$ , udávající poměr obvodu a průměru kružnice, nebo Eulerovo číslo  $e$ . Kromě těchto čísel, o kterých je relativně obtížné dokázat, že opravdu jsou iracionální, existují i taková, o kterých to jde dokázat relativně snadno.

**Tvrzení.** Číslo  $\sqrt{2}$  je iracionální.

*Důkaz.* Pro spor předpokládejme, že  $\sqrt{2}$  je racionální. Existují tedy dvě celá čísla  $p, q$  taková, že  $\sqrt{2} = p/q$ . Po umocnění na druhou a následném vynásobení  $q^2$  dostaneme, že musí platit  $2q^2 = p^2$ . Jelikož  $p, q$  jsou celá čísla, musí být v prvočíselných rozkladech  $p^2, q^2$  dvojka v sudé mocnině. To ale znamená, že na levé straně poslední rovnice je dvojka v liché mocnině, zatímco na pravé straně v sudé. Tato rovnost tedy nemůže platit pro žádná celá  $p, q$ , a proto je  $\sqrt{2}$  iracionální.

Výše uvedený důkaz lze zobecnit. Zjistíme tak, že pokud přirozené číslo není druhou mocninou jiného přirozeného čísla, pak už je jeho odmocnina nutně iracionální. Podobně lze důkaz upravit i pro vyšší odmocniny.

Přestože je obecně velmi těžké dokázat iracionalitu nějakého čísla, ukazuje se, že v jistém smyslu je iracionálních čísel mnohem více než racionálních.<sup>1</sup> Není těžké si rozmyslet a dokázat, že součet či součin nenulového racionálního čísla s iracionálním je vždy iracionální. Tento fakt

---

<sup>1</sup>Jak porovnat velikosti nekonečných množin? Toto téma je zajímavé, leč velmi rozsáhlé a nesouvisející s touto sérií. Zvědavý čtenář se o něm může dozvědět v knihovně na našich internetových stránkách: <http://mks.mff.cuni.cz/archive/21/10.pdf>

můžete ve svých řešeních bez důkazu používat. O součtu či součinu dvou iracionálních čísel však nelze obecně nic říct (např.  $\sqrt{2} + \sqrt{3}$  je iracionální, ale  $\sqrt{2} + (10 - \sqrt{2})$  je racionální).

Na závěr si ukážeme ještě jeden příklad, jak dokázat, že je nějaké číslo iracionální.

**Úloha.** Dokažte, že číslo  $0,1234567891011\dots$ , ve kterém za desetinnou čárku postupně píšeme všechna přirozená čísla, je iracionální.

*Řešení.* Pro spor předpokládejme, že toto číslo je racionální. Jeho desetinný rozvoj zjevně není ukončený, proto musí být periodický. Nechť má tedy periodu délky  $n$  a předperiodu délky  $m$ . Za desetinnou čárkou však umíme najít posloupnost alespoň  $m + n$  nul za sebou (například v čísle  $10^{m+n}$ ). Z těchto nul je nejvýše  $m$  v předperiodě a alespoň  $n$  za ní, takže perioda musí být složena ze samých nul. Podobně ale umíme najít i posloupnost  $m + n$  jedniček, dvojek,  $\dots$ , čímž dostáváme spor. Původní předpoklad tedy neplatí a číslo  $0,1234567891011\dots$  je skutečně iracionální.

Nyní už víte vše, co potřebujete, tak směle do řešení další série!

# Podobnost a shodnost

2. PODZIMNÍ SÉRIE

VZOROVÉ ŘEŠENÍ

## Úloha 1.

(105; 67; 1,94; 3,0)

*Alča jednou ve svém sešitě našla naryšované dva trojúhelníky, které se shodovaly ve velikostech všech vnitřních úhlů a v délkách dvou stran, ale přesto nebyly shodné. Nalezněte dva takové trojúhelníky.*

(Pepa Tkadlec)

ŘEŠENÍ:

Uvažujme trojúhelníky  $ABC$  a  $DEF$  a jejich strany  $a, b, c, d, e, f$  takové, že čtveřice čísel  $a, b = d, c = e, f$  tvoří geometrickou posloupnost. Platí  $a : d = b : e = c : f = k$ , trojúhelníky si tedy jsou podobné, a tudíž mají stejné vnitřní úhly.

Požadavkům vyhovují například čísla 8, 12, 18, 27. Musíme ještě ověřit, zda mohou tvořit trojúhelníky, tj. jestli nejdelší strana trojúhelníku je kratší než součet zbylých dvou. Vskutku  $8 + 12 > 18$ ,  $12 + 18 > 27$ , trojúhelníková nerovnost tedy platí.

Příkladem hledané dvojice trojúhelníků je  $\triangle ABC$  s délkami stran 8, 12, 18 a  $\triangle DEF$  s délkami stran 12, 18, 27.

POZNÁMKY:

Ačkoliv stačilo v podstatě jen najít dva vhodné trojúhelníky, správných řešení bylo jen lehce přes půlku. Část z nich uvažovala pravoúhlý trojúhelník a díky Pythagorově větě se pak nemusela řešit trojúhelníková nerovnost. Mnoho z ostatních pohořelo na jejím opomenutí (a snažilo se pak vydávat úsečky o délkách 1, 2, 4 za trojúhelník). Další skupinu pak tvořili ti, kteří zaslali trojúhelníky, které si nebyly podobné či neměly dvě strany stejně dlouhé. Někteří se také omezili na pouhé konstatování vlastností takových trojúhelníků nebo jen na naryšování bez jakéhokoli popisu stran.

Na závěr bych ráda podotkla, že když máte nalézt dva trojúhelníky daných vlastností a zadání říká, že existují, pak nemá cenu dokazovat jejich existenci ani neexistenci :) (Pokusů o jedno či druhé bylo dvojciferně.)

(Anička Doležalová)

## Úloha 2.

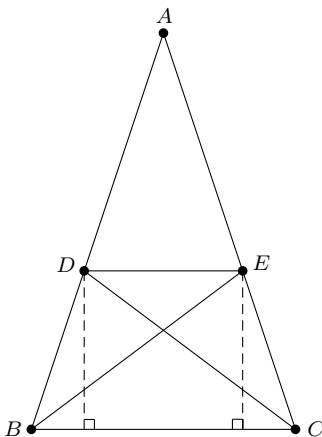
(100; 75; 2,28; 3,0)

*V trojúhelníku  $ABC$  leží body  $D, E$  po řadě na stranách  $AB$  a  $AC$  tak, že trojúhelníky  $ABC, CBD$  a  $BEC$  jsou podobné. Dokažte, že pokud jsou přímky  $BC$  a  $DE$  rovnoběžné, pak je trojúhelník  $ABC$  rovnoramenný.*

(Martin „E.T.“ Sýkora)

ŘEŠENÍ (PODLE KRISTÝNY ŠMÍDOVÉ):

Protože  $DE \parallel BC$ , tak výška trojúhelníku  $CBD$  na stranu  $BC$  je shodná s výškou trojúhelníku  $BEC$  na stranu  $BC$ . Obsahy těchto trojúhelníků jsou tedy shodné, a protože ze zadání víme, že  $\triangle CBD \sim \triangle BEC$ , jsou shodné i samotné trojúhelníky. Díky tomu je koeficient podobnosti  $k$  mezi trojúhelníky  $ABC$  a  $CBD$  stejný jako koeficient podobnosti mezi trojúhelníky  $ABC$  a  $BEC$ .



Z podobnosti  $\triangle ABC \sim \triangle CBD$  plyne  $|AB| = k \cdot |BC|$  a z podobnosti  $\triangle BEC \sim \triangle ABC$  plyne  $k \cdot |BC| = |AC|$ , celkem tedy  $|AB| = k \cdot |BC| = |AC|$  a trojúhelník  $ABC$  je rovnoramenný.

POZNÁMKY:

Většina řešitelů úlohu řešila postupem, na který navádí hinty na chatu našich internetových stránek. Jiní si zapsali podobnost jako shodnost poměrů délek stran podobných trojúhelníků a postupnými úpravami se dostali k rovnosti  $|AB| = |AC|$ . Oba způsoby vedly k řešení. Za originální myšlenku shodnosti podobných trojúhelníků uvedenou ve vzorovém řešení bych chtěl speciálně pochválit *Kristýnu Šmídovou* a *Eduarda Batmendijna*.

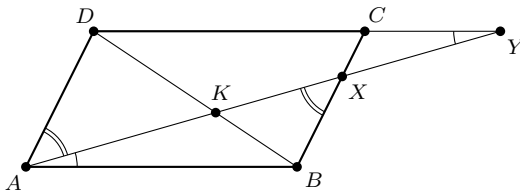
Závěrem bych chtěl upozornit na to, že pokud řekneme, že trojúhelníky  $ABC$  a  $XYZ$  jsou si podobné, myslíme tím, že jejich vrcholy si odpovídají v tomto pořadí, a tedy, že  $|\sphericalangle ABC| = |\sphericalangle XYZ|$ . I když jsme tuto skutečnost v zadání zmiňovali, mnozí ji nevezli v potaz a úlohu si zbytečně zkomplikovali. (Martin „E.T.“ Šýkora)

### Úloha 3.

(79; 56; 2,18; 3,0)

Na úhlopříčce  $BD$  rovnoběžníku  $ABCD$  je dán bod  $K$  tak, že přímka  $AK$  protne úsečku  $BC$  v bodě  $X$  a přímku  $CD$  v bodě  $Y$ . Dokažte, že  $|AK|^2 = |KX| \cdot |KY|$ . (Pepa Tkadlec)

ŘEŠENÍ:



Trojúhelníky  $BAK$  a  $DYK$  jsou si navzájem podobné podle věty  $uu$  ( $\sphericalangle BAK$  a  $\sphericalangle DYK$  jsou střídavé,  $\sphericalangle AKB$  a  $\sphericalangle YKD$  vrcholové). Odtud plyne vztah

$$\frac{|AK|}{|KY|} = \frac{|BK|}{|DK|}.$$

Obdobně i trojúhelníky  $BXK$  a  $DAK$  jsou podobné ( $\sphericalangle B XK$  a  $\sphericalangle DAK$  jsou střídavé,  $\sphericalangle XKB$  a  $\sphericalangle AKD$  vrcholové), což nám dává

$$\frac{|KX|}{|AK|} = \frac{|BK|}{|DK|}.$$

Porovnáním levých stran obou vztahů dostáváme

$$\frac{|AK|}{|KY|} = \frac{|KX|}{|AK|},$$

a to po úpravě dává dokazovanou rovnost.

POZNÁMKY:

Řešení byla převážně správná a podobná vzorovému, i když nezřídka zbytečně komplikovaná. Většina nezdařených pokusů bohužel ztroskotala na nepochopení zadání – jejich autoři měli za to, že přímka  $AK$  musí protnout stranu  $CD$ , a vyřešili tedy pouze případ, kdy prochází bodem  $C$ .

Další řešitelé si všimli, že dokazovaná rovnost připomíná Eukleidovu větu o odvěsné nebo mocnost bodu ke kružnici, a vymysleli si pomocnou konstrukci, na kterou pak to či ono použili. Nikomu z nich se však nepodařilo uspokojivě ukázat, že takovou konstrukci lze opravdu sestrojít.

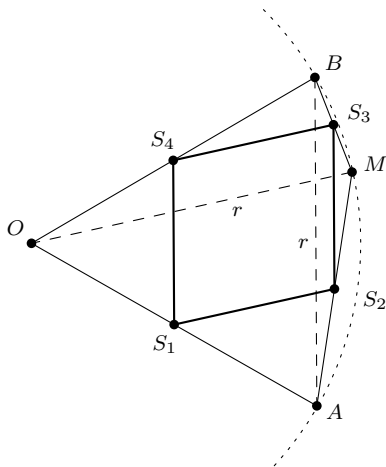
Imaginární bod obdržel *Miroslav Psota* za jediné správné řešení, které se zásadně odlišovalo od vzorového. (Ondřej Cířka)

#### Úloha 4.

(97; 74; 3,66; 5,0)

Na kružnici se středem  $O$  zvolme body  $A, B$  tak, aby platilo  $|\sphericalangle AOB| = 60^\circ$ . Na kratším oblouku  $AB$  zvolme bod  $M$ . Dokažte, že spojnice středů úseček  $BM$  a  $AO$  je kolmá na spojnici středů úseček  $AM$  a  $BO$ . (Martina Vaváčková)

ŘEŠENÍ:



Označme  $r$  polomer kružnice a body  $S_1, S_2, S_3, S_4$  postupne stredy úsečiek  $OA, AM, MB, BO$ . Pretože  $|\sphericalangle AOB| = 60^\circ$  a  $|AO| = |OB| = r$ , trojuholník  $ABO$  je rovnostranný. Preto aj  $|AB| = r$ . Uvažujme rovnoľahlosť so stredom v bode  $O$  a koeficientom  $1/2$ , bod  $A$  sa zobrazí na  $S_1$ , bod  $B$  na  $S_4$ . A teda  $|S_1S_4| = |AB|/2 = r/2$ . Analogicky rovnoľahlosť so stredom v bode  $M$  a koeficientom  $1/2$  nám zobrazí úsečku  $AB$  na  $S_2S_3$ , rovnoľahlosť so stredom v bode  $A$  a koeficientom  $1/2$  zobrazí úsečku  $OM$  na  $S_1S_2$  a konečne rovnoľahlosť so stredom v bode  $B$  a koeficientom  $1/2$  zobrazí úsečku  $OM$  na  $S_3S_4$ . Dostávame

$$|S_1S_4| = |S_2S_3| = \frac{1}{2}|AB| = \frac{1}{2}r = \frac{1}{2}|OM| = |S_1S_2| = |S_3S_4|.$$

Štvoruholník  $S_1S_2S_3S_4$  je teda kosoštvorec a v kosoštvorci sú uhlopriečky na seba vždy kolmé.

POZNÁMKY:

Na úlohu sa dalo nahliadnúť viacerými spôsobmi, či už pomocou podobných trojuholníkov, alebo stredných priecok, ako to robila väčšina z vás. Našlo sa aj pár riešiteľov, ktorí úlohu (vy)riešili pomocou nejakých iných metód, uhlením, prípadne s využitím vhodných zobrazení. Takéto riešenia boli však väčšinou dvakrát dlhšie. Nakoniec pripomínam, že búiť analytikou do takéhoto roztomilého príkladíku je priam barbarstvo, a každý, kto tak koná, mal by sa nad sebou zamyslieť ;-)

(Marta Kossaczká)

**Úloha 5.**

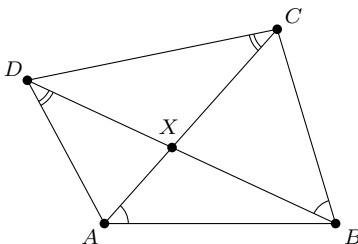
(69; 49; 3,45; 5,0)

Pepa si nakreslil konvexní čtyřúhelník  $ABCD$ , v němž současně platilo  $|\sphericalangle CBD| = |\sphericalangle CAB|$  a  $|\sphericalangle ACD| = |\sphericalangle ADB|$ . Dokažte, že z úseček  $AC$ ,  $AD$  a  $BC$  se mu podaří sestavit pravouhlý trojúhelník.

(Pepa Tkadlec)

ŘEŠENÍ:

Označme  $X$  průsečík úhlopříček konvexního čtyřúhelníku  $ABCD$ . Protože je čtyřúhelník konvexní, leží bod  $X$  uvnitř úsečky  $AC$ , platí tedy rovnost  $|AX| + |CX| = |AC|$ .



Trojúhelníky  $ABC$  a  $BXC$  jsou podobné, protože podle zadání platí  $|\sphericalangle CAB| = |\sphericalangle CBD|$  a vnitřní úhel u vrcholu  $C$  mají společný. Z podobnosti plyne:

$$\frac{|BC|}{|AC|} = \frac{|XC|}{|BC|}, \quad \text{neboli} \quad |BC|^2 = |AC| \cdot |XC|.$$

Obdobně i trojúhelníky  $CDA$  a  $DXA$  jsou podobné, protože podle zadání platí  $|\sphericalangle ACD| = |\sphericalangle ADB|$  a mají společný úhel u vrcholu  $A$ . Z podobnosti plyne:

$$\frac{|DA|}{|CA|} = \frac{|XA|}{|DA|}, \quad \text{neboli} \quad |DA|^2 = |CA| \cdot |XA|.$$

Sečtením těchto dvou rovností dostaneme:

$$|AD|^2 + |BC|^2 = |AC| \cdot (|XC| + |XA|) = |AC|^2.$$

Délky úseček  $AC$ ,  $AD$  a  $BC$  splňují podmínku obrácené Pythagorovy věty, a proto z nich lze sestavit pravouhlý trojúhelník.

ALTERNATIVNÍ PŘÍSTUP:

Místo podobnosti trojúhelníků můžeme také využít úsekového úhlu a z  $|\sphericalangle CAB| = |\sphericalangle CBD|$  vyvodit, že  $CB$  je tečna ke kružnici opsané trojúhelníku  $AXB$ . Mocnost bodu  $C$  k této kružnici pak dává kžženou rovnost  $|BC|^2 = |AC| \cdot |XC|$ . Obdobně samozřejmě i pro druhou dvojici stejně velkých úhlů.



POZNÁMKY:

Většina řešení byla v pořádku, ale občas bych ocenil větší množství slovního popisu. Někteří řešitelé končili tím, že ukázali rovnost  $|AD|^2 + |BC|^2 = |AC|^2$ , ale už nezdůvodnili, proč je tím pádem úloha vyřešena. Nejvíce mě zklamalo, že se našlo i několik řešitelů, kteří nepochopili zadání a místo obecného důkazu řešili nějaký jeden konkrétní případ (obvykle pro čtverec).

(Martin Töpfer)

**Úloha 6.**

(42; 25; 2,57; 4,0)

Je dán lichoběžník  $ABCD$  ( $AB \parallel CD$ ). Středů kružnic opsaných trojúhelníkům  $ABC$  a  $ACD$  označme postupně  $O_1$  a  $O_2$ , průsečík přímk  $AD$  a  $BC$  označme  $E$ . Dokažte, že přímky  $EO_1$  a  $EO_2$  jsou osově souměrné podle osy úhlu  $AEB$ .  
(Pepa Tkadlec)

ŘEŠENÍ:

BÚNO můžeme předpokládat, že  $|AB| > |CD|$ ; rovnost nastat nemůže, jelikož při ní by neexistoval bod  $E$ , a při opačné nerovnosti provedeme přeznačení.

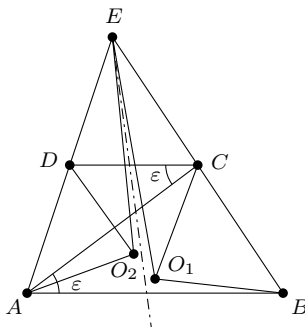
Díky rovnoběžnosti  $AB$  a  $CD$  platí  $|\sphericalangle BAC| = |\sphericalangle ACD|$ , označme velikost tohoto úhlu  $\varepsilon$ . Je-li  $\varepsilon = 90^\circ$ , pak jsou trojúhelníky  $ABC$ ,  $ABD$  pravoúhlé a  $O_1 \in EB$ ,  $O_2 \in EA$ , tvrzení ze zadání tedy triviálně platí. Předpokládejme dále, že tomu tak není, tedy  $\varepsilon \neq 90^\circ$ ,  $O_1 \notin EB$  a  $O_2 \notin EA$ .

Úhel  $BO_1C$  je (vzhledem ke kružnici opsané trojúhelníku  $ABC$ ) středovým úhlem s příslušným obvodovým úhlem  $BAC$ , v tomtéž vztahu jsou i úhly  $AO_2D$  a  $ACD$ . Protože zmiňované obvodové úhly mají stejnou velikost  $\varepsilon$ , mají stejnou velikost i středové úhly, neboli  $|\sphericalangle BO_1C| = |\sphericalangle AO_2D|$ . Z téhož důvodu také platí, že úhly  $BO_1E$ ,  $AO_2E$  jsou vždy opačně orientované – oba jsou buď vně úhlu  $AEB$  (pokud  $\varepsilon > 90^\circ$ ), nebo do něj oba zasahují (pokud  $\varepsilon < 90^\circ$ ). Díky tomu nám pro důkaz osové souměrnosti přímk  $EO_1$ ,  $EO_2$  podle osy úhlu  $AEB$  stačí ukázat  $|\sphericalangle BO_1E| = |\sphericalangle AO_2E|$ .

Předně si všimněme, že trojúhelníky  $BO_1C$ ,  $AO_2D$  jsou oba rovnoramenné se stejně velkými úhly proti základně, jsou tedy podobné (*sus*) a je  $|\sphericalangle EBO_1| = |\sphericalangle CBO_1| = |\sphericalangle DAO_2| = |\sphericalangle EAO_2|$ . Dále jsou podobné i trojúhelníky  $EAB$  a  $EDC$  (díky  $AB \parallel CD$ ), takže  $|EA| : |EB| = |ED| : |EC|$ ; označíme tento poměr  $k$ . Ještě si všimněme, že

$$\frac{|AD|}{|BC|} = \frac{|EA| - |ED|}{|EB| - |EC|} = \frac{k \cdot |EB| - k \cdot |EC|}{|EB| - |EC|} = k,$$

ovšem díky podobnosti  $\triangle BO_1C$  a  $\triangle AO_2D$  máme také  $|AO_2| : |BO_1| = |AD| : |BC| = k$ . Trojúhelníky  $EAO_2$  a  $EBO_1$  jsou tedy podobné dle věty *sus*, z čehož dostáváme požadovanou rovnost  $|\sphericalangle BO_1E| = |\sphericalangle AO_2E|$ .



POZNÁMKY:

Úloha nebyla nijak zvláště obtížná, ale velká většina řešitelů získala pouhé čtyři body kvůli přílišnému upnutí k jedné konfiguraci bodů  $A, B, C, D$ , typicky k takové, jako je znázorněna na obrázku výše. Poté se jali víceméně správně dokazovat rovnost  $|\sphericalangle BO_1E| = |\sphericalangle AO_2E|$ , ovšem již nezduvodnili, že tyto úhly jsou opačně orientované, bez čehož požadovanou osovou souměrnost ještě dokázanou nemáme. S případem  $\varepsilon = 90^\circ$  si taky nikdo příliš hlavu nelámá, ačkoliv v této situaci je velmi ošemetné argumentovat trojúhelníkem  $EBO_1$  a podobnými (pro takoveto „trojúhelníky“ např. neplatí věta *uu*). Pouze *František Couf* a *Martin Raszyk* podali dostatečně důkladný rozbor situace, čímž si vysloužili plný počet bodů. Konečně *Antonín Češík* a *Miroslav Stankovič* poslali zajímavé řešení využívající geometrických zobrazení, čímž se výše provedeným diskusím elegantně vyhnuli a vysloužili si  $+i$ . (Alexander „Olin“ Slávik)

**Úloha 7.**

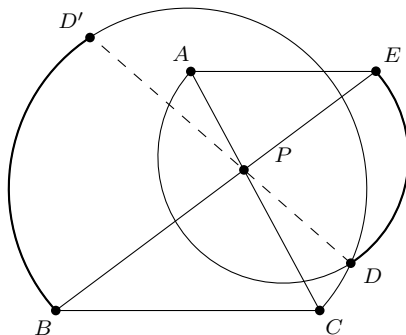
(34; 15; 2,18; 1,0)

Konvexní pětiúhelník  $ABCDE$  má strany  $AE$  a  $BC$  rovnoběžné a pro jeho vnitřní úhly platí  $|\sphericalangle ADE| = |\sphericalangle BDC|$ . Označme  $P$  průsečík úhlopříček  $AC$  a  $BE$ . Dokažte, že  $|\sphericalangle EAD| = |\sphericalangle BDP|$  a  $|\sphericalangle CBD| = |\sphericalangle ADP|$ . (Alča Skálová)

ŘEŠENÍ:

Stačí ukázat  $|\sphericalangle EAD| = |\sphericalangle BDP|$ , druhá rovnost se dokáže analogicky prohozením bodů  $A$  a  $B$  a bodů  $E$  a  $C$ .

Úsečky  $AE$  a  $CB$  jsou rovnoběžné a opačně orientované, proto existuje záporná stejnolehlost se středem v  $P$ , která zobrazí  $A$  na  $C$  a  $E$  na  $B$ . Díky rovnosti  $|\sphericalangle ADE| = |\sphericalangle BDC|$  a tomu, že bod  $D$  leží mezi rovnoběžkami  $AE, BC$ , se v této stejnolehlosti zobrazí oblouk  $EDA$  na oblouk  $BDC$ .



Dále obraz bodu  $D$  označme  $D'$ , pak body  $D, P, D'$  leží na jedné přímce a podoblouk  $ED$  se ve stejnolehlosti zobrazí na podoblouk  $BD'$ . Těmto podobloučkům proto odpovídají stejné obvodové úhly, a tak  $|\sphericalangle BDD'| = |\sphericalangle AED|$ , což jsme chtěli dokázat. Ještě dodejme, že bod  $D$  neleží na podoblouce  $BD'$ , protože leží v opačné polorovině určené přímkou  $EB$ .

POZNÁMKY:

Řešení se v zásadě dělí na dva typy – víceméně vzorová (za 5 bodů) a ta, co tvrdila, že takový pětiúhelník nutně musí být osově souměrný (za 0 bodů). Pak ještě dorazilo několik delších řešení pomocí sinových vět. Žádné z nich se ale nedokázalo dobře popasovat se skutečností, že funkce kosinus není prostá, za což jsem strhával jeden bod. (Mírek Olšák)

### Úloha 8.

(27; 13; 2,30; 1,0)

Osa strany  $AC$  trojúhelníku  $ABC$  protne stranu  $BC$  v bodě  $M$ . Dále nechť  $K$  je průsečík osy úhlu  $AMB$  a kratšího oblouku  $AB$  kružnice opsané trojúhelníku  $ABC$ . Dokažte, že přímka spojující středy kružnic vepsaných trojúhelníkům  $AMK$  a  $BMK$  je kolmá na osu úhlu  $AKB$ .

(Alča Skálová)

ŘEŠENÍ:

Trojúhelník  $AMC$  je rovnoramenný, neboť  $M$  leží na ose úsečky  $AC$ . Spolu s využitím faktu, že přímka  $MK$  je osa úhlu  $AMB$ , dostáváme:

$$|\sphericalangle ACB| = \frac{1}{2}(180^\circ - |\sphericalangle CMA|) = \frac{1}{2}|\sphericalangle AMB| = |\sphericalangle AMK| = |\sphericalangle BMK|.$$

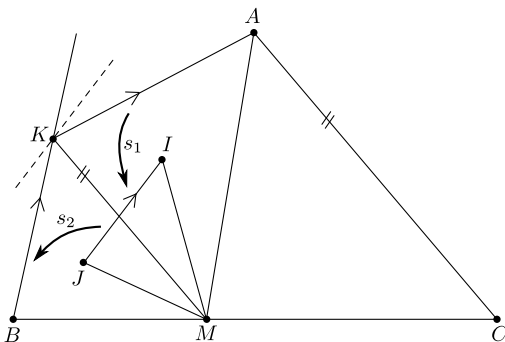
Z rovnosti  $|\sphericalangle ACB| = |\sphericalangle BMK|$  plyne rovnoběžnost přímek  $AC$  a  $MK$ .

Nyní ukážeme, že trojúhelníky  $AMK$  a  $KMB$  jsou podobné pomocí věty  $uu$ . Jak již víme, platí  $|\sphericalangle AMK| = |\sphericalangle BMK|$ . Druhou rovnost úhlů dostaneme takto:

$$\begin{aligned} |\sphericalangle KBM| &= 180^\circ - |\sphericalangle KAC| = 180^\circ - |\sphericalangle KAM| - |\sphericalangle MAC}| = \\ &= 180^\circ - |\sphericalangle KAM| - |\sphericalangle AMK}| = |\sphericalangle AKM}|. \end{aligned}$$

(V první rovnosti jsme využili, že čtyřúhelník  $AKBC$  je tětíkový.)

Označme  $I$  (resp.  $J$ ) střed kružnice vepsané trojúhelníku  $AMK$  (resp.  $KMB$ ). Protože  $\triangle AMK$  a  $\triangle KMB$  jsou podobné, jsou také podobné trojúhelníky  $AMI$  a  $KMJ$ . Z toho plyne  $|AM| : |IM| = |KM| : |JM|$ . Zároveň platí, že  $I$  (resp.  $J$ ) leží na ose úhlu  $AMK$  (resp.  $KMB$ ), a proto  $|\sphericalangle IMJ| = |\sphericalangle IMK}| + |\sphericalangle KMJ}| = (|\sphericalangle AMK}| + |\sphericalangle KMB}|)/2 = |\sphericalangle AMK}|$ , takže spolu s rovností poměrů délek stran dostáváme, že  $\triangle IMJ$  je také podobný trojúhelníkům  $AMK$  a  $KMB$ .



Uvažme spirální podobnost<sup>2</sup>  $s_1$  (resp.  $s_2$ ) zobrazující trojúhelník  $AMK$  (resp.  $IMJ$ ) na podobný trojúhelník  $IMJ$  (resp.  $KMB$ ) se středem v  $M$  a úhlem otočení  $AMI$  (resp.  $KMJ$ ). Protože  $|\sphericalangle AMI| = |\sphericalangle KMJ}|$ , mají úhly otočení  $s_1$  a  $s_2$  stejnou velikost. Pro spirální podobnost platí, že (orientovaný) úhel mezi přímkou a jejím obrazem je roven úhlu příslušného otočení. To v našem případě znamená, že orientované<sup>3</sup> přímky  $KA$  a  $JI$  svírají stejný orientovaný úhel ( $AMI$  dle  $s_1$ ) jako orientované přímky  $JI$  a  $BK$  ( $KMJ$  dle  $s_2$ ). Přímka  $JI$  je proto rovnoběžná s osou úhlu mezi orientovanými přímkami  $BK$  a  $KA$ . Konečně tato osa úhlu je kolmá na osu vedlejšího úhlu – tedy úhlu  $BKA$ . Přímka  $IJ$  je tak kolmá na osu úhlu  $BKA$ , což jsme chtěli dokázat.

<sup>2</sup>Spirální podobnost je složení stejnoolehlosti a otočení podle stejného středu.

<sup>3</sup>U orientovaných přímek bereme v potaz pořadí vrcholů, které ji udávají. Například orientovaná přímka  $KA$  je „jiná“ (opačná) než orientovaná přímka  $AK$ .

## POZNÁMKY:

Sešlo se 26 řešení, z toho 12 bylo dobře. Správná řešení většinou využívala počítání úhlů a posléze nějakou variantu spirální podobnosti. Elegancí při použití spirální podobnosti vynikla řešení *Eduarda Batmendijna* a *Miroslava Psoty*, za což si jmenovaní vysloužili  $+i$ . Další  $+i$  dostal *Jakub Svoboda* za velmi odlišný přístup využívající „mrkvovo-salámové“ a „Bismarckovo“ lemma, neboli originálně pojmenované úvahy o Švrčkově bodu.<sup>4</sup> *Radovan Švarc* ve svém řešení využíval dokonce kruhovou inverzi. Nesprávná řešení obvykle obsahovala pouze jeden konkrétní příklad v podobě obrázku, byť pečlivě narysovaného, případně nějaká pozorování, která ale nebyla dostatečně odůvodněná. (*Pepa Svoboda*)

---

<sup>4</sup>Švrčkův bod příslušející vrcholu  $A$  v trojúhelníku  $ABC$  je střed oblouku  $BC$  kružnice opsané trojúhelníku  $ABC$ , neobsahujícího bod  $A$ .

# Funkce

3. PODZIMNÍ SÉRIE

VZOROVÉ ŘEŠENÍ

## Úloha 1.

(91; 89; 2,86; 3,0)

Z jednoho znaku  $x$ , tří jedniček, tří minusů a čtyř svislých čar (tj. symbolů použitelných pro zápis absolutní hodnoty) složte výraz, jehož hodnota je nulová pro alespoň čtyři reálná čísla  $x$ .  
(Anička Doležalová)

ŘEŠENÍ:

Myslenka úlohy spočívá v tom, že do sebe vnoříme dvě absolutní hodnoty. Příkladem řešení je funkce  $f(x) = ||x| - 1 - 1| - 1$ , která je nulová pro  $x = \pm 1$  a  $x = \pm 3$ .

POZNÁMKY:

U této úlohy mě překvapila invence některých řešitelů, kteří se snažili část znaků umístit do exponentu. Bohužel si často neuvědomili, že  $0^0$  nemá definovanou hodnotu, a tak nalezené funkce neměly za definiční obor všechna reálná čísla. Objevilo se ale i několik řešitelů, kterým se povedlo najít funkci identicky rovnou nule. Příkladem takové funkce je  $f(x) = |-1^1| - |-1^x|$ .  
(Martin Töpfer)

## Úloha 2.

(49; 42; 2,49; 3,0)

Nalezněte nekonstantní funkci  $f: \mathbb{R} \rightarrow \mathbb{R}$  takovou, že funkce  $f(2x)$  a  $(f(x))^2$  jsou periodické a mají stejnou nejkratší periodu.  
(Martin Sýkora)

PRVNÍ ŘEŠENÍ:

Definujeme funkci

$$f(x) = \begin{cases} 1 & \text{pro } x \text{ celá sudá,} \\ -1 & \text{pro } x \text{ celá lichá,} \\ 0 & \text{pro } x \in \mathbb{R} \setminus \mathbb{Z}. \end{cases}$$

Tato  $f$  je tedy dobře definována na  $\mathbb{R}$ . Ukážeme, že  $f(2x)$  a  $(f(x))^2$  jsou periodické a mají stejnou nejkratší periodu.

$$f(2x) = \begin{cases} 1 & \text{pro } x \text{ celá,} \\ -1 & \text{pro } x = \frac{k}{2}, \text{ kde } k \text{ je liché,} \\ 0 & \text{pro ostatní } x \in \mathbb{R}. \end{cases}$$

Tedy  $f(2x)$  je periodická a má nejkratší periodu rovnou jedné.

$$(f(x))^2 = \begin{cases} 1 & \text{pro } x \in \mathbb{Z}, \\ 0 & \text{pro } x \in \mathbb{R} \setminus \mathbb{Z}. \end{cases}$$

Tedy  $(f(x))^2$  má nejkratší periodu také rovnou jedné.

Funkce  $f(2x)$  a  $(f(x))^2$  jsou periodické a mají stejnou nejkratší periodu, proto je zvolená  $f$  řešením úlohy.

DRUHÉ ŘEŠENÍ:

Ukážeme, že pro  $f(x) = \sin(x)$  mají funkce  $f(2x)$  a  $(f(x))^2$  stejnou nejkratší periodu. Protože funkce  $\sin(x)$  má nejkratší periodu  $2\pi$ , pro funkci  $\sin(2x)$  je to  $\pi$ . Nyní určíme nejkratší periodu funkce  $\sin^2(x)$ .

Platí  $\sin x = -\sin(x + \pi)$ , tedy  $\sin^2(x) = \sin^2(x + \pi)$ , proto  $\pi$  je perioda funkce  $\sin^2 x$ . Pro  $x \in (0, \pi)$  platí, že  $\sin x \neq 0$ , tedy také  $\sin^2 x \neq 0$ , ale  $\sin^2(0) = 0$ , proto  $\pi$  je nejkratší perioda funkce  $\sin^2 x$ .

Tedy funkce  $\sin(2x)$  a  $\sin^2 x$  jsou periodické a mají stejnou nejkratší periodu, proto  $f(x) = \sin x$  je řešením úlohy.

POZNÁMKY:

Drtivá většina řešitelů volila  $f(x) = \sin x$ , ale ne všichni úspěšně ukázali, že skutečně  $\sin(2x)$  a  $\sin^2 x$  mají stejnou nejkratší periodu. O tom ale přece byla tahle úloha – vybrat si takovou  $f$ , u které umím ukázat nejen jaká je perioda  $f(2x)$  a  $(f(x))^2$ , ale dokonce jaká je nejkratší perioda těchto funkcí. Z tohoto hlediska se mi první vzorové řešení zdá mnohem snazší, je to na něm totiž opravdu „vidět“.

(Michaela „Míša“ Hubatová)

### Úloha 3.

(52; 34; 1,96; 2,0)

Jsou dány ryze<sup>5</sup> monotónní funkce  $f, g: \mathbb{R} \rightarrow \mathbb{R}$  takové, že funkce  $f(g(x))$  je rostoucí. Dokažte, že funkce  $g(f(x))$  je rovněž rostoucí.

(David Hruška)

ŘEŠENÍ:

Funkce  $f, g$  jsou podle zadání ryze monotónní, čili každá z nich je buď rostoucí, nebo klesající. Předpokládejme nejprve, že  $g$  je klesající. Vezměme si dvě libovolná reálná čísla  $x_1, x_2$  splňující  $x_1 < x_2$ . Z předpokladu a definice klesající funkce plyne  $g(x_1) > g(x_2)$ . Ze zadání víme, že  $f(g(x_1)) < f(g(x_2))$ . Pokud by  $f$  byla rostoucí, platila by poslední nerovnost obráceně, čili  $f$  musí být klesající funkcí (víme už, že je rostoucí, nebo klesající). Potom již dvojím použitím definice klesající funkce pro každá dvě reálná  $x_1 < x_2$  dostáváme  $f(x_1) > f(x_2)$ , a následně  $g(f(x_1)) < g(f(x_2))$ , což znamená, že složená funkce  $g(f(x))$  je opravdu rostoucí, jak jsme měli dokázat.

Pokud je  $g$  rostoucí, dostaneme stejným postupem jako v prvním případě pro každá dvě reálná  $x_1 < x_2$  nerovnost  $g(x_1) < g(x_2)$ . To spolu s  $f(g(x_1)) < f(g(x_2))$  znamená, že  $f$  nemůže být klesající, proto je rostoucí. Opět tedy dostáváme  $g(f(x_1)) < g(f(x_2))$ , čili  $g(f(x))$  je rostoucí funkce.

POZNÁMKY:

Úloha byla jednoduchá, přesto byla zhruba polovina řešení zmatených nebo vyloženě scestných. Někteří z vás si správně všimli, že se monotónní funkce při skládání chovají jako násobení kladných/záporných čísel (známá pravidla typu „minus krát minus je plus“), ale místo důkazu tato „odporovaná“ pravidla jen používali. Jádrem úlohy byla právě manipulace s definicemi rostoucích a klesajících funkcí, takže za prohlašování těchto pravidel za zřejmá jsem bod(y) strhával. Několik řešitelů se také pokoušelo úlohu derivovat (v PraSeti se důrazně nedoporučuje) a bohužel došlo i na klasický přístup – ověření tvrzení pro jednu konkrétní dvojici funkcí, což přesně v úlohách typu „Dokažte . . .“ od řešitelů nechceme, ale o tom bylo již řečeno a napsáno dost. Na druhou stranu přišlo i mnoho správných a stručných řešení, nad kterými jsem si spravil náladu.

(David Hruška)

<sup>5</sup>O funkci řekneme, že je ryze monotónní, pokud je rostoucí nebo klesající.

#### Úloha 4.

(60; 48; 3,93; 5,0)

Je dána funkce  $f: \mathbb{N} \rightarrow \mathbb{N}$  splňující současně následující dvě podmínky:

- (i) Pro každá dvě nesoudělná<sup>6</sup> kladná celá čísla  $a, b$  platí  $f(ab) = f(a) \cdot f(b)$ .
- (ii) Pro každá dvě (ne nutně různá) prvočísla  $p, q$  platí  $f(p + q) = f(p) + f(q)$ .

Dokažte, že  $f(3) = 3$ .

(Filip Hlásek)

ŘEŠENÍ:

Předpokládejme, že  $f$  je funkce vyhovující podmínkám v zadání. Speciálně tedy splňuje podmínku (i) pro nesoudělná  $a = 2, b = 3$ :

$$f(6) = f(3 \cdot 2) = f(3) \cdot f(2).$$

Zároveň pro funkci  $f$  platí podmínka (ii) pro prvočísla  $p = 3, q = 3$ :

$$f(6) = f(3 + 3) = f(3) + f(3) = 2f(3).$$

Vydělením předchozích dvou rovností získáváme  $f(2) = 2$  (všechny členy jsou přirozená čísla).

Dále využijeme platnosti první podmínky pro nesoudělná  $a = 3, b = 4$ :

$$f(12) = f(3 \cdot 4) = f(3) \cdot f(4).$$

Poté několikrát použijeme druhou podmínku pro prvočísla 2, 3, 5, 7 a dosadíme předem zjištěné hodnoty. Tím získáme

$$\begin{aligned} f(4) &= f(2 + 2) = f(2) + f(2) = 4, \\ f(5) &= f(2 + 3) = f(2) + f(3) = 2 + f(3), \\ f(7) &= f(2 + 5) = f(2) + f(5) = 4 + f(3), \\ f(12) &= f(5 + 7) = f(5) + f(7) = 6 + 2f(3). \end{aligned}$$

Důkaz dokončíme srovnáním hodnoty  $f(12)$ :

$$\begin{aligned} f(3)f(4) &= 6 + 2f(3), \\ 4f(3) &= 6 + 2f(3), \\ f(3) &= 3. \end{aligned}$$

POZNÁMKY:

Úloha vypadala na první pohled poměrně jednoduše, ale když do ní člověk zkusil něco dosadit, brzy zjistil, že zrovna hodnotu  $f(3)$  není snadné vyjádřit. V podstatě všechna správná řešení se k výsledku dopracovala stejně jako v tom autorském za použití hodnoty  $f(12)$ . Bez chyby bylo také jedno, které mimo jiné používalo  $f(11), f(13), f(19), f(20)$  a  $f(22)$ .

Mnoho řešitelů si také správně povšimlo, že lze snadno ukázat  $f(1) = 1$ . Tohoto poznatku ale není možné v dalším řešení nijak použít a je potom vcelku zbytečné to do čistopisu vůbec psát.

Řešení, která nedostala plný počet bodů, se dají rozdělit do dvou skupin. První část se mě snažila (ať už úmyslně či neúmyslně) přesvědčit, že číslo 1 je prvočíslo, což bohužel není pravda. V jiné úloze by to nebyl takový problém, ale v této se jednalo o neúměrné zjednodušení, které zadaný problém činilo triviálním.

<sup>6</sup>Dvě celá čísla jsou *nesoudělná*, jestliže je jejich největší společný dělitel roven jedné.

Druhá častá chyba byla, že se někteří zaměřili pouze na jednu podmínku ze zadání (např. (i)) a tvrdili, že jí vyhovuje pouze značně omezená množina funkcí (např.  $f(x) = k \cdot x^n$ ). To lze poté snadno dosadit do druhé z podmínek a ověřit, že jediná vyhovující funkce je  $f(x) = x$ . Úloha by takto byla jednoduchá a takové tvrzení obecně neplatí (naš příklad vyvrací funkce  $f(x) = 2^{\text{počet\_prvočísel\_v\_rozkladu}(x)}$ ).

Kdo se nad úlohou zamýšlel dále, jistě ho napadlo zjistit, zda existuje i jiná funkce než očividná  $f(x) = x$ , která by vyhovovala podmínkám v zadání. Pokusme se společně dokázat, že jiná taková funkce neexistuje.

Při důkazu použijeme Goldbachovu hypotézu, která dodnes není dokázána, očekává se ale, že je platná. Pokud však neplatí, tak ani zmíněný důkaz nefunguje. Tvrzení říká, že každé sudé přirozené číslo větší než dva lze zapsat jako součet dvou prvočísel. Díky tomuto snadnému a pochopitelnému znění se hypotéza stala jedním z nejznámějších otevřených problémů, jehož rozřešením se stále můžete proslavit.

Postupujme matematickou indukci. Použitím autorského řešení úlohy bychom pro všechna přirozená  $x \leq 12$  ukázali  $f(x) = x$ . Dále předpokládejme, že pro přirozené  $n \geq 6$  platí, že pro všechna přirozená  $x \leq 2n$  je  $f(x) = x$ . Ukážeme, že  $f(2n + 1) = 2n + 1$  a  $f(2n + 2) = 2n + 2$  rozborem případů.

- (1)  $2n + 1$  není žádná přirozená mocnina lichého prvočísla. Potom lze rozložit na součin dvou nesoudělných celých čísel  $a, b$  menších než  $2n + 1$ , takže za použití (i) a indukčního předpokladu  $f(2n + 1) = f(ab) = f(a)f(b) = ab = 2n + 1$ .
- (2)  $2n + 1$  je prvočíslu. Potom jedno ze sudých čísel  $2n + 4$  a  $2n + 6$  není mocninou čísla 2 a lze tedy rozložit na součin nesoudělných celých čísel větších než 1 a menších než  $2n$ . Použitím (i) a indukčního předpokladu dostáváme, že pro toto číslo  $x$  platí  $f(x) = x$  a důkaz indukčního kroku získáme buď použitím prvočísla 3, nebo 5 společně s  $2n + 1$  v podmínce (ii). Všimněte si, že tento postup navíc funguje pro všechna prvočísla  $p$  taková, že  $\frac{p+5}{2} \leq 2n$ , neboli  $p \leq 4n - 5$ .
- (3)  $2n + 1$  je přirozená mocnina lichého prvočísla (alespoň druhá). Potom je podle předchozího bodu pro všechna prvočísla  $p \leq 4n - 5$  pravda  $f(p) = p$ . Kdybychom ukázali, že  $f(4n + 2) = 4n + 2$ , tak máme vyhráno, neboť by stačilo použít (i) pro nesoudělná  $2n + 1$  a 2. Podle Goldbachovy hypotézy lze  $4n + 2$  zapsat jako součet dvou prvočísel. Pokud jsou obě tato prvočísla menší nebo rovna  $4n - 5$ , tak stačí využít (ii). Problém ale nastává, když jedno z nich je rovno 3 nebo 5.

Nechť tedy  $p = 4n - 3$  je prvočíslu ( $p + 5$  je potom  $4n + 2$ ). Aspoň jedno z čísel  $p + 7 = 4(n + 1)$ ,  $p + 11 = 4(n + 2)$  není mocninou dvojky. Označme ho  $x$  a díky tomu, že ho lze rozložit na součin dvou nesoudělných celých čísel, která nejsou větší než  $2n$ , tak pomocí (i) dokážeme z indukčního předpokladu, že  $f(x) = x$ . Z (ii) již poté snadno plyne  $f(p) = p$  a dále  $f(4n + 2) = 4n + 2$ , což jsme chtěli ukázat. Příklad  $4n + 2 = p + 3$  rozebereme analogicky (použijeme  $p + 5$  a  $p + 13$ ). Povšimněte si, že jsme vždy volili taková čísla, která byla dělitelná čtyřmi a šla tedy rozložit na součin dostatečně malých činitelů (nejvýše  $\frac{4n+12}{3} \leq 2n$ , pro  $n \geq 6$ , což jsme předpokládali).

To, že platí  $f(2n + 2) = 2n + 2$ , dokážeme opět snadno pomocí Goldbachovy hypotézy. Tím jsme dokázali úvodní výrok také pro  $n + 1$ , z principu matematické indukce tak plyne platnost tvrzení. (Filip Hlášek)

### Úloha 5.

Najděte všechna reálná čísla  $x$ , pro která platí<sup>7</sup>

(61; 47; 2,70; 3,0)

$$x \lfloor x \lfloor x \lfloor x \rfloor \rfloor \rfloor = 2001.$$

(Martin Čech)

<sup>7</sup>Symbol  $\lfloor x \rfloor$  značí dolní celou část čísla  $x$ , tedy největší celé číslo nepřevyšující  $x$ .



ŘEŠENÍ:

Jediným řešením je  $x = 2001/286$ . Aby sme toto mohli tvrďiť, rozoberme si priebeh funkcie  $f(x) = x[x[x[x]]]$ . Ukážeme, že  $f$  je na intervale  $(-1, 1)$  nulová, na  $(1, \infty)$  rastie a na  $(-\infty, -1)$  klesá.

Interval  $(-1, 1)$  si ešte rozdelíme na dva intervaly:  $(-1, 0)$  a  $(0, 1)$ . Pre každý z intervalov  $(-1, 0)$ ,  $(0, 1)$ ,  $(1, \infty)$  a  $(-\infty, -1)$  dokážeme jeho uvedenú vlastnosť zvlášť.

$$\begin{array}{ll} x \in (-1, 0), & x \in (0, 1), \\ -x \in (0, 1), & [x] = 0, \\ [x] = -1, & x[x[x[x]]] = 0 = f(x). \\ x[x] = -x, & \\ [x[x]] = 0, & \\ x[x[x[x]]] = 0 = f(x), & \end{array}$$

Takže sme ukázali, že na  $(-1, 1)$  je  $f(x) = 0$ , na tomto intervale teda  $f(x) = 2001$  riešenie určite nemá.

Ďalej ukážeme, že  $f$  je na  $(1, \infty)$  rastúca a na  $(-\infty, -1)$  klesajúca. Majme teda  $x > y$  z intervalu  $(1, \infty)$ , resp.  $(-\infty, -1)$ , potom platí:

$$\begin{array}{ll} x > y \geq 1, & y < x \leq -1, \\ [x] \geq [y] \geq 1, & [y] \leq [x] \leq -1, \\ x[x] > y[y] \geq 1, & y[y] > x[x] \geq 1, \\ [x[x]] \geq [y[y]] \geq 1, & [y[y]] \geq [x[x]] \geq 1, \\ x[x[x]] > y[y[y]] \geq 1, & \text{resp.} \quad y[y[y]] < x[x[x]] \leq -1, \\ [x[x[x]]] \geq [y[y[y]]] \geq 1, & [y[y[y]]] \leq [x[x[x]]] \leq -1, \\ x[x[x[x]]] > y[y[y[y]]] \geq 1, & y[y[y[y]]] > x[x[x[x]]] \geq 1, \\ f(x) > f(y), & f(y) > f(x). \end{array}$$

Teda  $f$  je skutočne na intervale  $(-\infty, -1)$  klesajúca a na  $(1, \infty)$  rastúca, a preto na každom z týchto intervalov môže mať rovnica  $f(x) = 2001$  maximálne jedno riešenie. Na  $(1, \infty)$  ho skutočne má:  $x = 2001/286$ .

Ukážeme ďalej, že na intervale  $(-\infty, -1)$  rovnica  $f(x) = 2001$  riešenie nemôže mať. Pre spor predpokladajme, že existuje  $x \in (-\infty, -1)$  také, že  $f(x) = 2001$ . Číslo  $z = [x[x[x]]]$  je záporné a celé. Podelením rovnice  $f(x) = 2001$  týmto číslom dostaneme, že  $x$  môžeme zapísať v tvare  $x = 2001/z$ .

Platí ale  $f(-2001/303) \doteq 2007,6 > 2007$  a  $f(-2001/304) \doteq 1994,4 < 1995$ . Teda keby  $z \geq -303$ , máme  $x = 2001/z \leq -2001/303$ , a teda z klesania  $f$  vieme, že  $f(x) > 2007 > 2001$ , čo je spor s  $f(x) = 2001$ . Keby naopak  $z \leq -304$ , platilo by  $x \geq -2001/304$ , a teda  $f(x) < 1995 < 2001$ , čo je opäť spor. Rovnici  $f(x) = 2001$  preto nevyhovuje žiadne záporné  $x$  a riešením je naozaj jedine  $x = 2001/286$ .

POZNÁMKY:

Vo väčšine správnych riešení ste postupovali ako my. Medzi častými chybami bolo, že ste nedokázali, že riešenie nemôže byť viac, síce ste túto skutočnosť ticho prepokladali a nejaké riešenie medzi 6 a 7 ste našli. V lepšom prípade ste aspoň ukázali, že na tomto intervale žiadne ďalšie riešenie byť nemôže, ale väčšinou ste sa moc nepokúšali dokázať, prečo by inde (na kladných

číslach) nemohlo byť ďalšie riešenie (a podobne na záporných). Zopár riešiteľov dokonca „našlo“ aj záporné riešenie. (Marta Kossaczka)

### Úloha 6.

(36; 31; 3,58; 4,0)

Pro daná dvě celá čísla  $p, q$  uvažme kvadratickou funkci  $f: \mathbb{R} \rightarrow \mathbb{R}$  určenou předpisem

$$f(x) = x^2 + px + q.$$

Řekneme, že celé číslo  $t$  je dobré, jestliže čísla  $f(t)$  a  $f(t+1)$  jsou různá a jedno je násobkem druhého. Dokažte, že je-li počet dobrých čísel konečný, pak je sudý. (Martin „E.T.“ Sýkora)

ŘEŠENÍ:

Nejprve si uvědomme, že graf funkce  $f$  je parabola s vrcholem v bodě  $-p/2$ , která je osově souměrná podle osy  $x = -p/2$ . Proto můžeme nabýt podezření, že pokud bude nějaké dobré číslo na jednom rameni paraboly, bude nějaké jiné i na tom druhém, a tedy že je počet dobrých čísel sudý. V následujících řádcích tuto ideu formálně dokážeme.

Povšimněme si, že pro všechna reálná čísla  $x$  platí  $f(x) = f(-x - p)$ . Dosazením  $x + 1$  a  $(-p - 1)/2$  za  $x$  dostáváme rovnosti  $f(x + 1) = f(-x - p - 1)$  a  $f((-p - 1)/2) = f((-p - 1)/2 + 1)$ . Z druhé z nich vyplývá, že číslo  $(-p - 1)/2$  není dobré (je-li vůbec celé).

Ostatní celá čísla (bez  $(-p - 1)/2$ , pokud by bylo celé) pak popárujeme takovým způsobem, že v každé dvojici jsou čísla  $a$  a  $b$  právě tehdy, je-li jejich součet  $-p - 1$ . Protože je  $-p - 1$  celé číslo, je toto párování korektní, neboť každému celému číslu  $a$  do dvojice skutečně přiřadí celé číslo  $b$  různé od  $a$ . Z již dříve objevených rovností  $f(x) = f(-x - p)$  a  $f(x + 1) = f(-x - p - 1)$  dosazením  $a$  za  $x$  pak vyplývá, že číslo  $a$  je dobré právě tehdy, když  $b = a - p - 1$  je dobré.

V každém páru tak buď obě čísla jsou, nebo obě čísla nejsou dobrá. Jiná čísla být dobrými nemohou, a tak je počet všech dobrých čísel – za předpokladu, že je konečný – sudý.

POZNÁMKY:

Většina došlých řešení více či méně kopírovala vzorové řešení. Řešitelé se snažili najít párování dobrých čísel a většinou volili správný postup. Bohužel ale velice často chyběla diskuse kolem čísla  $(-p - 1)/2$ . Mnoho řešitelů opomnělo zdůvodnit, že nalezená „dobrá čísla“ jsou celá, což byla jedna z podmínek v zadání. Za tyto a podobné nešvary jsem strhával podle závažnosti jeden až dva body.

Několik řešitelů také argumentovalo tím, že na množině dobrých čísel (označme si ji  $\chi$ ) našli bijekci. To je sice jedna ze správných cest ke správnému řešení, ale ještě je třeba dodat, že daná bijekce je symetrická (tedy se rovná svému inverzu) a že každému prvku přiřadí nějaký jiný prvek. Pokud toto nezmíníte, může být bijekci například cyklická záměna nebo dokonce identita, které počet prvků množiny  $\chi$  nijak neomezuji.

Vzhledem k tomu, že chybovali i zdatní řešitelé, dovolím si k bijekci přidat ještě pár slov. Pokud naleznete bijekci mezi dvěma množinami  $\Omega$  a  $\Psi$ , znamená to, že obě množiny mají stejný počet prvků. Nalezením bijekce na jedné množině (tedy  $z \in \Omega$  na  $\Omega$ ) jen ukážete, že  $|\Omega| = |\Omega|$ , což je ale triviálně zřejmé, takže nic takového ukazovat nemusíte. Ve skutečnosti bijekce existuje na každé množině – například výše zmíněná identita – takže objevením nějaké bijekce nezískáte informaci žádnou. (Martin „E.T.“ Sýkora)

### Úloha 7.

(38; 29; 3,11; 3,0)

Rozhodněte, zda lze funkci  $f: \mathbb{R} \rightarrow \mathbb{R}$  určenou předpisem  $f(x) = x^2$  zapsat jako součet dvou periodických funkcí. (Alexander „Olin“ Slávik)

ŘEŠENÍ:

Dokážeme sporem, že tvrzení ze zadání neplatí. Předpokládejme, že existují periodické funkce  $g, h: \mathbb{R} \rightarrow \mathbb{R}$  takové, že  $g(x) + h(x) = x^2$  pro všechna  $x \in \mathbb{R}$ , přičemž  $h$  má periodu  $p \neq 0$ .

Předpokládanou identitu přepíšeme na  $h(x) = x^2 - g(x)$ . Z periodičnosti  $h$  dostáváme pro všechna  $x \in \mathbb{R}$  rovnost

$$\begin{aligned} h(x) &= h(x+p), \\ x^2 - g(x) &= (x+p)^2 - g(x+p), \\ g(x+p) - g(x) &= 2xp + p^2. \end{aligned}$$

Jelikož je  $g$  periodická funkce, je periodická i funkce daná předpisem  $g(x+p) - g(x)$ . To je však spor, protože  $2xp + p^2$  není pro  $p \neq 0$  periodickou funkcí.

POZNÁMKY:

Přibližně polovina došlých řešení byla správně, přičemž většina z nich postupovala dosazováním hodnot  $0, p, q, p+q$  do identity  $g(x) + h(x) = x^2$ , kde  $p$ , resp.  $q$  je periodou  $g$ , resp.  $h$ . Výše uvedený postup je jen stručnější variací na tuto metodu. Autoři chybných řešení se zpravidla odvolávali na neplatná tvrzení o periodických funkcích – např. že musí být omezené či že jejich sčítáním dostaneme opět periodickou funkci.<sup>8</sup>

Ve skutečnosti jakékoliv řešení, které dostatečně nevyužívalo vlastností funkce  $x^2$ , bylo předeem odsouzeno k nízkému bodovému zisku, neboť identickou funkci  $i(x) = x$  jako součet dvou periodických překvapivě napsat lze. Pro zajímavost si nastíníme konstrukci oněch funkcí.

Zvolme libovolné iracionální číslo  $\alpha$ . Naším cílem bude zkonstruovat 1-periodickou funkci  $g$  takovou, že  $g(x) - x$  bude  $\alpha$ -periodická. Pro  $z \in \mathbb{R}$  definujme pomocnou funkci  $p_z: \mathbb{Z} \rightarrow \langle 0, 1 \rangle$  předpisem  $p_z(n) = \{n\alpha + z\}$ , kde závorkami  $\{\}$  značíme zlomkovou část čísla (jako v prvním dílu seriálu). Díky iracionalitě  $\alpha$  je  $p_z$  prostá. Ještě definujeme množinu  $M_z = \{p_z(n) \mid n \in \mathbb{Z}\}$ .

Není těžké si rozmyslet, že pokud mají dvě takovéto množiny  $M_w, M_z$  neprázdný průnik, pak již nutně  $M_w = M_z$ , můžeme tedy zkonstruovat množinu reálných čísel  $Z$  takovou, že pro každé  $x \in \langle 0, 1 \rangle$  bude existovat právě jedno  $z_x \in Z$  takové, že  $x \in M_{z_x}$ . Díky této jednoznačnosti můžeme definovat naši funkci  $g$  na  $\langle 0, 1 \rangle$  jako  $g(x) = \alpha \cdot p_{z_x}^{-1}(x)$  a na zbytku  $\mathbb{R}$  ji dodefinovat periodicky.

Z definice je  $g$  1-periodická a pro každé  $x \in \mathbb{R}$  patří čísla  $\{x\}, \{x + \alpha\}$  do téže množiny  $M_z$  pro právě jedno  $z \in Z$ , je tedy

$$g(x + \alpha) = \alpha \cdot p_z^{-1}(x + \alpha) = \alpha(p_z^{-1}(x) + 1) = g(x) + \alpha,$$

neboli  $g(x + \alpha) - (x + \alpha) = g(x) - x$ , což jsme chtěli. (Alexander „Olin“ Slávik)

## Úloha 8.

(19; 8; 2,42; 1,0)

Nalezněte všechny funkce  $f: \mathbb{R} \rightarrow \mathbb{R}$  takové, že pro všechny čtveřice reálných čísel  $x, y, u, v$  splňujících  $x + y = u + v$  platí

$$(f(x) - f(y)) \cdot (u - v) = (f(u) - f(v)) \cdot (x - y).$$

(Pepa Tkadlec)

<sup>8</sup>To máme zaručeno jen tehdy, je-li podíl period sčítaných funkcí racionální číslo.

KLASICKÉ ŘEŠENÍ:

Předpokládejme, že  $f$  splňuje zadanou rovnici pro všechna  $x, y, u, v$ , pro něž platí  $x + y = u + v$ . Pak  $f$  tutéž rovnici splňuje pro konkrétní dosazení  $x, -x, y, -y$ , neboť to rovněž splňuje  $x - x = y - y$ . Pro nenulová  $x$  a  $y$  můžeme rovnici přepsat do tvaru

$$\frac{f(x) - f(-x)}{x} = \frac{f(y) - f(-y)}{y},$$

odkud vidíme, že podíl  $(f(x) - f(-x))/x$  je pro nenulová  $x$  konstantní. Označme si tuto konstantu jako  $2b$ . Pak můžeme psát  $f(x) = 2bx + f(-x)$  pro všechna  $x \in \mathbb{R}$ , neboť pro  $x = 0$  platí rovnost triviálně. Označme ještě  $f(0) = c$  a  $f(-1) = d$ .

Buď nyní  $t$  libovolné reálné číslo. Provedme dvě dosazení do původní rovnice.<sup>9</sup> Jest

$$\begin{aligned} \left[ \frac{t-1}{2}, \frac{t+1}{2}, t, 0 \right] : & \quad \left( f\left(\frac{t-1}{2}\right) - f\left(\frac{t+1}{2}\right) \right) t = (f(t) - c)(-1), \\ \left[ \frac{t-1}{2}, -\frac{t+1}{2}, -1, 0 \right] : & \quad -\left( f\left(\frac{t-1}{2}\right) - f\left(-\frac{t+1}{2}\right) \right) = t(d - c). \end{aligned}$$

V druhé rovnici použijeme  $f\left(-\frac{t+1}{2}\right) = -2b\frac{t+1}{2} + f\left(\frac{t+1}{2}\right)$  a pak sečteme první rovnici s  $t$ -násobkem druhé. Dostaneme

$$f(t) = (d - c + b)t^2 + bt + c.$$

Protože  $t$  bylo libovolné, musí být  $f(t) = at^2 + bt + c$  pro každé  $t \in \mathbb{R}$ , kde  $a, b, c$  jsou nějaká reálná čísla nezávislá na  $t$ . Zkouškou se přesvědčíme, že všechny takové funkce zadání skutečně splňují.

LIŠÁCKÉ ŘEŠENÍ:

Předpokládejme, že  $f$  je řešením zadané úlohy. Ukážeme, že  $f$  je polynom nejvýše druhého stupně, tj. že existují reálné konstanty  $a, b, c$  takové, že  $f(x) = ax^2 + bx + c$  pro každé reálné  $x$ .

Buď  $P$  polynom nejvýše druhého stupně splňující  $P(t) = f(t)$  pro  $t = 0, 1, 2$ . Ukážeme, že pak již  $P(x) = f(x)$  pro všechna  $x \in \mathbb{R}$ . Označme si  $P(x) = ax^2 + bx + c$ . Dokažme nejprve, že pokud platí  $P(t) = f(t)$  pro nějaká různá  $t = x, y, u$ , pak tato rovnost platí i pro  $t = x + y - u$ .

Volbou  $t = x + y - u$  splníme rovnost  $t + u = x + y$ , takže tyto hodnoty lze dosadit do rovnice. Jest

$$(f(x) - f(y))(u - t) = (f(u) - f(t))(x - y).$$

V dalším kroku využijme předpoklad, že  $f(x) = P(x)$ ,  $f(y) = P(y)$  a  $f(u) = P(u)$ . Dostaneme po úpravě

$$\begin{aligned} (P(x) - P(y))(u - t) &= (P(u) - P(t))(x - y), \\ (a(x^2 - y^2) + b(x - y))(u - t) &= (au^2 + bu + c - f(t))(x - y). \end{aligned}$$

Dělením (nenulovým) výrazem  $x - y$  a nahrazením  $x + y = u + t$  dostaneme

$$\begin{aligned} (a(u + t) + b)(u - t) &= au^2 + bu + c - f(t), \\ f(t) &= a(t^2 - u^2) + b(t - u) + au^2 + bu + c, \\ f(t) &= at^2 + bt + c = P(t), \end{aligned}$$

což jsme chtěli ukázat.

Buď nyní  $x$  libovolné reálné číslo různé od 0, 1 a dále buď  $Q$  polynom nejvýše druhého stupně splňující  $f(t) = Q(t)$  pro  $t = 0, 1, x$ . Potom podle předchozího pozorování je i  $f(x + 1) = Q(x + 1)$ , neboť  $x + 1 = 1 + x - 0$ . Stejně tak  $f(2) = Q(2)$ , jelikož  $2 = 1 + (x + 1) - x$ . Celkem  $P(t) = f(t) = Q(t)$  pro  $t = 0, 1, 2$ . Protože  $P$  a  $Q$  jsou polynomy stupně nejvýše dva a shodují se ve třech různých bodech, nutně  $P = Q$ , a proto  $f(x) = Q(x) = P(x)$ , což jsme chtěli ukázat.

<sup>9</sup>Hranatými závorkami  $[a, b, c, d]$  značíme dosazení  $a$  za  $x$ ,  $b$  za  $y$ ,  $c$  za  $u$  a  $d$  za  $v$ .

MODERNÍ ŘEŠENÍ:

Označme písmenem  $M$  množinu všech řešení zadané úlohy. Snadno se ověří, že funkce  $f_0(x) = 1$ ,  $f_1(x) = x$ ,  $f_2(x) = x^2$ ,  $x \in \mathbb{R}$  patří do  $M$ . Dále si všimneme, že pokud  $f, g \in M$ , pak  $f + g \in M$  a též  $af \in M$  pro každou reálnou konstantu  $a$ . Množina  $M$  tedy obsahuje všechny polynomy stupně nejvýše dva. Buď nyní  $h \in M$  libovolná. Necht  $P(x) = ax^2 + bx + c \in M$  je polynom takový, že  $P(t) = h(t)$  pro  $t = -1, 0, 1$ . Funkce  $f(x) = h(x) - P(x)$  je pak nulová v bodech  $-1$ ,  $0$  a  $1$ . Ukážeme, že  $f$  je již nulová na celém  $\mathbb{R}$ .

Buď  $x$  libovolné reálné číslo. Dosaďme postupně tři čtveřice

$$\begin{aligned} [x + 1, x - 1, 2x, 0] : & \quad (f(x + 1) - f(x - 1))2x = 2f(2x), \\ [x - 1, -x, -1, 0] : & \quad -f(x - 1) + f(-x) = 0, \\ [-x, x + 1, 1, 0] : & \quad f(-x) - f(x + 1) = 0. \end{aligned}$$

Přičtením  $(-x)$ -násobku druhé a  $x$ -násobku třetí rovnice k první získáme  $f(2x) = 0$ . Protože  $x$  bylo libovolné,  $h = P$ , čili každé řešení je polynomem nejvýše druhého stupně.

POZNÁMKY:

Jak už to tak u osmiček bývá, řešení se dělí na ta správná a na pokusná. Hranice tentokrát byla velmi ostrá. Kdo úlohu měl a dokázal ji rozumně napsat, dostal pět bodů. Kdo střílel a trefil řešení, dostal bod.

Rozdána byla i tři  $i$ -čka. Dostali je *Ondřej Darmovzal* za rychlé a přehledné řešení pomocí soustavy, *František Couf* za řešení moderní a *Eduard Batmendijn*, který postupoval lišácky.

(Vít „Vejtek“ Musil)

# Teorie čísel

1. SERIÁLOVÁ SÉRIE

VZOROVÉ ŘEŠENÍ

## Úloha 1.

(49; 28; 2,86; 3,0)

Nechť  $n, k$  jsou přirozená čísla a  $k$  je bezčtvercové.<sup>10</sup> Předpokládejme, že

$$\frac{n^3 + 2n^2 + k}{n^2 + k}$$

je celé číslo. Dokažte, že pak už platí  $n = k$ .

(Štěpán Šimsa)

STANDARDNÍ ŘEŠENÍ:

Aby byl zlomek  $\frac{n^3 + 2n^2 + k}{n^2 + k}$  celé číslo, musí platit

$$n^2 + k \mid n^3 + 2n^2 + k,$$

tedy  $n^2 + k \mid n^3 + 2n^2 + k - (n + 2) \cdot (n^2 + k) = -nk - k$ , neboli  $n^2 + k \mid nk + k$ . Označme si<sup>11</sup>  $d = (n, k)$  a vezměme si taková čísla  $N, K$ , že  $n = Nd$  a  $k = Kd$ . Z vlastností největšího společného dělitele víme  $(N, K) = 1$ . Navíc pokud  $(K, d) = a$ , tak  $a \mid d$ ,  $a \mid K$ , takže  $a^2 \mid k$ , z čehož plyne  $a = 1$  ( $k$  je bezčtvercové). Odtud máme, že i čísla  $K$  a  $d$  jsou nesoudělná. Rozepišme si nyní  $n^2 + k \mid nk + k$  do  $N, K$  a  $d$  a upravme:

$$N^2d^2 + Kd \mid NdKd + Kd,$$

$$N^2d + K \mid NKd + K = K(Nd + 1),$$

ale protože je  $(N, K) = 1$  a  $(d, K) = 1$ , tak  $(N^2d + K, K) = (N^2d, K) = 1$ , a proto platí i  $N^2d + K \mid Nd + 1$ . Čísla  $N^2d + K$  i  $Nd + 1$  jsou obě přirozená, platí tedy  $N^2d + K \leq Nd + 1$ , což spolu s tím, že  $N^2d \geq Nd$  a  $K \geq 1$ , znamená, že musí nastat rovnosti, a tedy  $K = 1$ ,  $N = 1$ . Proto  $n = d = k$ , což jsme chtěli dokázat.

RYCHLÉ ŘEŠENÍ (PODLE MIROSLAVA STANKOVIČE):

Jako minule  $n^2 + k \mid nk + k$ , takže pro nějaké přirozené číslo  $a$  platí  $a(n^2 + k) = nk + k$ , neboli  $an^2 = k(n + 1 - a)$ . Proto  $k \mid an^2$ , ale jelikož je  $k$  bezčtvercové, tak i  $k \mid an$ , tedy  $k \leq an$ . Proto  $n + 1 - a = an^2/k \geq n$ , z čehož plyne  $a \leq 1$ . Je tedy  $a = 1$  a  $n^2 = kn$ , a tak skutečně platí  $n = k$ .

<sup>10</sup>Tedy neexistuje přirozené číslo  $a > 1$  takové, že  $a^2 \mid k$ .

<sup>11</sup>Připomeňme si, že  $(a, b)$  značí největšího společného dělitele čísel  $a, b$ .

TRIKOVÉ ŘEŠENÍ (PODLE MARKÉTY CALÁBKOVÉ):

Opět  $a(n^2 + k) = nk + k$  pro nějaké přirozené číslo  $a$ . Tuto rovnost upravíme na tvar

$$an^2 - kn + k(a - 1) = 0, \quad (\clubsuit)$$

což je kvadratická rovnice v  $n$ , jejíž jeden kořen musí být přirozené číslo. Proto její diskriminant  $k^2 - 4ka(a - 1) = k(k - 4a(a - 1))$  musí být druhá mocnina celého čísla. Proto musí  $k$  dělit celou druhou závorku (díky bezčtvercovosti), tedy  $k \mid k - 4a(a - 1)$ , a tedy  $k \mid 4a(a - 1)$ . Aby však měla rovnice ( $\clubsuit$ ) vůbec řešení, musí být  $k \geq 4a(a - 1)$ , takže je  $4a(a - 1)$  buď rovno  $k$ , nebo je to 0, nebo záporné číslo. Poslední možnost nemůže nastat, protože  $a$  je přirozené číslo. Dále  $k \neq 4a(a - 1)$ , protože jinak by  $k$  bylo dělitelné čtyřmi, tedy by nebylo bezčtvercové. Proto  $4a(a - 1) = 0$ , z čehož plyne  $a = 1$ . Rovnice ( $\clubsuit$ ) tedy přejde na tvar  $n^2 - kn = 0$ , což má jediné kladné řešení  $n = k$ .

POZNÁMKY:

Ti, co se vydali standardní cestou, obvykle úlohu úspěšně dokončili a získali tak plný počet bodů. Poté se objevilo poměrně hodně rychlejších a trikovějších řešení, podobných jako ta citovaná, která byla ohodnocena imaginárním bodem. Bohužel se ale objevilo i hodně řešení se závažnou chybou, kterou bylo například tvrzení, že pokud  $n^2 + k \mid n^2(n + 1)$ , tak  $n^2 + k \mid n^2$  nebo  $n^2 + k \mid n + 1$  (které neplatí, jak si můžete rozmyslet). Konečně někteří bohužel dokazovali jinou úlohu, když dosadili  $n = k$  a zjistili, že se jedná o celé číslo. Bylo třeba dokázat přesně opačnou implikaci. (Štěpán Šimsa)

## Úloha 2.

(29; 26; 3,52; 4,0)

Mějme přirozené číslo  $n \geq 2$ . Dokažte, že každé z čísel  $n! + 2, n! + 3, \dots, n! + n$  má takového prvočíselného dělitele, který není dělitelem žádného z  $n - 2$  zbylých čísel. (Josef Svoboda)

ŘEŠENÍ:

Uvažujme pevné  $n$  a číslo  $n! + k$ . Rozebereme dva případy.

Pokud všechna prvočísla v prvočíselném rozkladu čísla  $k$  dělí i některé (ne nutně stále stejné) z ostatních čísel  $2, \dots, k - 1, k + 1, \dots, n$ , rozložíme zkoumané číslo do tvaru  $k(n!/k + 1)$ . Číslo  $(n!/k + 1)$  je větší než jedna, uvažujme některého jeho prvočíselného dělitele  $p$ . Platí  $n!/k \equiv -1 \pmod{p}$ . Prvočísla  $p$  tak nedělí žádné z čísel  $2, \dots, k - 1, k + 1, \dots, n$ , nedělí tedy ani  $k$ , a je proto větší než  $n$ . Máme tak  $p$ , které dělí  $n! + k$ , ale žádné ze zbylých  $n - 2$  čísel ze zadání, protože nejbližší další čísla dělitelná  $p$  jsou  $n + k - p$  a  $n + k + p$ . Je tedy hledaným prvočíslem.

Nyní naopak předpokládejme, že existuje prvočísla v rozkladu čísla  $k$  (označme jej  $p$ ), které žádné z čísel  $2, \dots, k - 1, k + 1, \dots, n$  nedělí. To ale znamená, že musí být  $p = k$ , protože jinak by  $p$  bylo v tomto seznamu. Navíc musí platit  $2p > n$ , protože jinak by v seznamu bylo číslo  $2p$ . Takže  $p$  dělí  $(n! + k) = p(n!/p + 1)$ , ale nedělí žádné ze zbývajících  $n - 2$  čísel ze zadání, protože nejbližší další dělitel čísla  $p$  jsou  $n!$  a  $n! + 2p$ . Je tedy opět hledaným prvočíslem.

POZNÁMKY:

Nejčastější chybou bylo opomenutí druhého případu, opravdu není pravda, že se vždy dá najít prvočísla větší než  $n$ , které dělí  $n! + k$  – stačí se podívat například na výrazy

$$2! + 2, \quad 3! + 2, \quad 3! + 3, \quad 4! + 3, \quad 5! + 5.$$

Jeden řešitel ale vznesl hypotézu, že se vždy dá najít prvočísla větší než  $n - 2$ , to pro účely úlohy stačí. Pokud se vám povede rozhodnout platnost této hypotézy, nebojte se podělit na matematickém chatu na našich stránkách ;-)

(Mírek Olšák)

### Úloha 3.

(24; 21; 3,96; 5,0)

Mějme celé číslo  $n$  a prvočíslo  $p$ . Víme, že platí

$$2^{4n} + 9^{2n} \equiv 36^n \pmod{p}.$$

Dokažte, že  $p$  je tvaru  $4k + 1$  pro nějaké celé číslo  $k$ .

(Josef Svoboda)

ŘEŠENÍ:

Nejprve snadno vyloučíme možnost, že  $p = 2$  nebo  $p = 3$ . Pro  $p = 2$  bychom dostali

$$1 \equiv 2^{4n} + 9^{2n} \equiv 36^n \equiv 0 \pmod{2},$$

což neplatí, obdobně pro  $p = 3$  bychom dostali, že 3 dělí  $2^{4n}$ , což také neplatí.

Pro přehlednost si zavedeme substituci  $a = 2^{2n}$ ,  $b = 3^n$ , zadání nyní vypadá takto:

$$a^4 + b^4 \equiv (ab)^2 \pmod{p},$$

což můžeme ekvivalentně upravit na

$$(a^2 - b^2)^2 \equiv -(ab)^2 \pmod{p}.$$

Protože jsme vyloučili možnosti  $p = 2$  a  $p = 3$ , číslo  $(ab)^2 = 2^{2n} \cdot 3^{2n}$  je nesoudělné s  $p$  a můžeme jím tedy kongruenci ekvivalentně vydělit. Dostáváme tedy kongruenci

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

ze které plyne, že  $-1$  je kvadratický zbytek modulo  $p$ . Jak jsme si v seriálu ukázali (pomocí Eulerova kritéria), z toho už plyne, že  $p$  je tvaru  $4k + 1$ , což jsme chtěli dokázat.

POZNÁMKY:

Velká část řešení postupovala stejně jako vzorové, případně s pěknou obměnou při získávání dvou čtverců – výraz  $a^4 - (ab)^2 + b^4$  můžeme vynásobit číslem  $a^2 + b^2$  a dostaneme  $(a^3)^2 + (b^3)^2$ . Nejčastější chybou bylo svévolné přecházení od kongruence modulo  $p$  ke kongruenci modulo 4. Bohužel však  $a \equiv 0 \pmod{p}$  neimplikuje  $a \equiv p \pmod{4}$ , jak si snadno ověříte třeba na případě  $a = 21$ ,  $p = 3$ .

(Pepa Svoboda)



# Seriál – Teorie čísel II

Po krátké přestávce se k Tobě dostává další díl seriálu! Jak sis možná všiml, první část seriálu byla poměrně hutná. Proto jsme se rozhodli udělat tento díl kratší, aby sis mohl dočíst z prvního dílu kapitoly, které jsi třeba předtím nestihl. Tak se do toho opři, bude to stát za to! Navíc jsme v textu odlišili náročnější pasáže, které nejsou potřeba k vyřešení seriálových úloh a k pochopení ostatní látky.

Tentokrát v seriálu najdeš návod, jak nakládat s umocňováním čísel. Nejdříve si zavedeme  $p$ -valuace, které jsou praktickým nástrojem při práci s dělitelností. Poté se seznámíme s primitivním prvkem, ukážeme si zajímavé vlastnosti kvadratických zbytků a probranou teorii využijeme v rozmanitých úlohách z olympiád.

## Rozklady a $p$ -valuace

Když pracujeme s dělitelností, vyplatí se rozkládat čísla na prvočísla. Pokud chceme například dokázat  $60^{30} \mid 30^{60}$ , tak stačí najít prvočíselný rozklad obou čísel. Vidíme  $60^{30} = 2^{60} \cdot 3^{30} \cdot 5^{30}$  a  $30^{60} = 2^{60} \cdot 3^{60} \cdot 5^{60}$ . Jelikož exponenty u každého prvočísla jsou v prvním čísle menší než v tom druhém, tak dokazovaná dělitelnost skutečně platí. Když nepracujeme s konkrétními čísly, často se vyplatí podívat se pouze na nějaké obecné prvočíslu a na mocniny, v jakých dělí zadaná čísla. A k tomu si zavedeme pojem  $p$ -valuace.

**Definice.** Nechť  $n$  je přirozené číslo a  $p$  prvočíslu. Poté  $p$ -valuací čísla  $n$  myslíme největší číslo  $k$  takové, že  $p^k \mid n$ .<sup>12</sup> Značíme ji  $v_p(n)$ .

Jinými slovy,  $p$ -valuace jsou vlastně exponenty v prvočíselném rozkladu čísla  $n$ . Například pro  $24 = 2^3 \cdot 3$  máme  $v_2(24) = 3$ ,  $v_3(24) = 1$  a  $v_7(24) = 0$ .

**Cvičení.** Uvědom si následující jednoduché vlastnosti  $p$ -valuací.

- (i)  $v_p(mn) = v_p(m) + v_p(n)$ ,
- (ii)  $v_p(m + n) \geq \min(v_p(m), v_p(n))$ ,
- (iii) Pokud  $v_p(m) \neq v_p(n)$ , pak dokonce  $v_p(m + n) = \min(v_p(m), v_p(n))$ .

Tyto vlastnosti vyplývají z toho, že se jedná jen o exponenty jednotlivých prvočísel v rozkladu. A exponenty se při násobení přece počítají. Povšimni si, že jako důsledek prvního cvičení platí například i  $v_p(a^n) = n \cdot v_p(a)$ .

Na následujících cvičeních si  $p$ -valuace trochu zažijeme.

**Cvičení.** Urči tyto hodnoty:

- (i)  $v_2(2^n + 4)$  (v závislosti na  $n$ ).
- (ii)  $v_3(v_3(18^{18}))$ .
- (iii)  $v_p((3p^3 + p^2)(p^3 + 2p^2 + 5p))$  (v závislosti na prvočíslu  $p$ ).

---

<sup>12</sup>Tento fakt občas zapisujeme jako  $p^k \parallel n$ .

**Cvičení.** Máme tři čísla, z nichž žádné není dělitelné 8 ani 125. Kolika nejvíce nulami může končit jejich součin?

Základní použití  $p$ -valuací spočívá v této snadné úvaze. Představme si, že chceme dokázat  $a \mid b$ . Místo toho nám stačí ukázat, že když si vezmeme libovolné prvočíslo  $p$ , tak  $v_p(a) \leq v_p(b)$ . Ukažme si to na příkladu.

**Příklad.** Mějme čísla  $a, b, c$ , pro která platí  $a \mid b^3, b \mid c^3, c \mid a^3$ . Dokaž, že  $abc \mid (a + b + c)^{13}$ .

*Řešení.* Vezměme si libovolné prvočíslo  $p$ . Z toho, že platí  $a \mid b^3$ , můžeme odvodit  $v_p(a) \leq v_p(b^3)$ , takže  $v_p(a) \leq 3v_p(b)$ . Podobně víme  $v_p(b) \leq 3v_p(c)$  a  $v_p(c) \leq 3v_p(a)$ . Nyní chceme dokazované tvrzení přeložit do řeči  $p$ -valuací. K tomu stačí využít výsledky (i) a (ii) z úvodního cvičení. BÚNO předpokládejme, že  $v_p(a)$  je nejmenší z čísel  $v_p(a), v_p(b), v_p(c)$ . Pak

$$v_p((a + b + c)^{13}) \geq 13 \cdot \min(v_p(a), v_p(b), v_p(c)) = 13v_p(a),$$

ale

$$v_p(abc) = v_p(a) + v_p(b) + v_p(c) \leq v_p(a) + 4v_p(c) \leq 13v_p(a) \leq v_p((a + b + c)^{13}).$$

Jelikož tato nerovnost platí pro každé prvočíslo  $p$ , tak platí i pro všechna prvočísla v rozkladu  $abc$ , a tedy opravdu  $abc \mid (a + b + c)^{13}$ .

Podobné metody můžeme využít, když chceme dokázat, že se dvě čísla  $a, b$  rovnají (až na znaménko). Dokážeme jednoduše, že  $v_p(a) = v_p(b)$  pro každé prvočíslo  $p$ . Než si tuto metodu předvedeme na příkladu, rozmyslíme si ještě, jaká je  $p$ -valuace NSD a nsn.<sup>13</sup>

**Cvičení.** Dokaž:

- (i)  $v_p((m, n)) = \min(v_p(m), v_p(n))$ .
- (ii)  $v_p([m, n]) = \max(v_p(m), v_p(n))$ .

*Návod.* Ukaž, že  $p^{\min(v_p(m), v_p(n))}$  dělí  $m$  i  $n$ , zatímco větší mocnina  $p$  už jedno z nich nedělí.

**Příklad.** Necht  $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$  jsou přirozená čísla, která splňují  $(a_i, b_i) = 1$  pro každé  $i \in \{1, 2, \dots, k\}$ . Dále buď  $m = [b_1, b_2, \dots, b_k]$ . Ukaž, že platí

$$\left( \frac{a_1 m}{b_1}, \frac{a_2 m}{b_2}, \dots, \frac{a_k m}{b_k} \right) = (a_1, a_2, \dots, a_k).$$

(IMO shortlist 1974)

*Řešení.* Vezměme si libovolné prvočíslo  $p$ . Stačí nám dokázat, že  $p$ -valuace levé ( $L$ ) a pravé ( $P$ ) strany je stejná. A to podle předchozího cvičení znamená, že

$$v_p(L) = \min \left( v_p \left( \frac{a_1 m}{b_1} \right), v_p \left( \frac{a_2 m}{b_2} \right), \dots, v_p \left( \frac{a_k m}{b_k} \right) \right),$$

$$v_p(P) = \min(v_p(a_1), v_p(a_2), \dots, v_p(a_k)).$$

Ale zároveň platí  $v_p(a_i m / b_i) = v_p(a_i) + v_p(m) - v_p(b_i)$  a  $v_p(m) = \max(v_p(b_1), \dots, v_p(b_k))$ . Nyní rozebereme dvě možnosti.

Pokud  $v_p(b_i) = 0$  pro všechna  $i$ , tak i  $v_p(m) = 0$ . Poté zřejmě  $v_p(a_i) + v_p(m) - v_p(b_i) = v_p(a_i)$  pro každé  $i$ . Pak je ale  $v_p(a_i m / b_i) = v_p(a_i)$ , a to znamená, že také  $v_p(L) = v_p(P)$ .

Nechť pro nějaké  $b_i$  platí  $v_p(b_i) \neq 0$ . Vezměme  $i$  takové, že  $v_p(b_i)$  je největší, takže  $v_p(m) = v_p(b_i)$ . Pak  $v_p(a_i) + v_p(m) - v_p(b_i) = v_p(a_i)$ . Jelikož ale  $p \mid b_i$  a protože  $(a_i, b_i) = 1$ , tak  $p \nmid a_i$ .

<sup>13</sup>Připomeneme, že NSD čísel  $a, b$  značíme  $(a, b)$ , zatímco nsn značíme  $[a, b]$ . Totéž značení používáme i pro více jak dvě čísla.

To znamená, že  $v_p(a_i) = 0$ . Proto  $v_p(a_i m / b_i) = 0$  a levá strana není dělitelná prvočíslem  $p$ , stejně jako pravá (protože  $p \nmid a_i$ ).

**Úloha.** Přirozená čísla  $a, b, c, d$  splňují  $ab = cd$ . Ukaž, že platí

$$(a, c) \cdot (a, d) = a \cdot (a, b, c, d).$$

(Polská MO, Mecz 2009)

*Návod.* Označ si  $p$ -valuace čísel  $a, b, c, d$ , rozepiš obě rovnosti do řeči  $p$ -valuací a rozeber několik případů.

**Úloha.** Víme, že pro přirozená čísla  $m, n$  platí  $m \mid n^2, n^3 \mid m^4, m^5 \mid n^6, \dots$ . Dokaž  $m = n$ .

*Návod.* Kdyby pro nějaké prvočíslo neplatilo  $v_p(m) = v_p(n)$ , tak si zvol dostatečně velké  $k$  a dojdí ke sporu s tím, že  $m^{4k+1} \mid n^{4k+2}$ , nebo s tím, že  $n^{4k+3} \mid m^{4k+4}$ .

Díky  $p$ -valuacím získáváme ještě nový pohled<sup>14</sup> na to, co je to největší společný dělitel, případně nejmenší společný násobek. Napišme si prvočíselný rozklad čísel  $m, n$ .

$$\begin{aligned} m &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \\ n &= p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \end{aligned}$$

kde  $p_1 < p_2 < \dots < p_k$  jsou prvočísla a  $\alpha_i, \beta_i$  pro  $i \in \{1, \dots, k\}$  jsou nezáporná čísla (do obvyklého prvočíselného rozkladu můžeme přidat jakékoli prvočíslo umocněné na nultou, což je jedna, a zajistit si tak v obou rozkladech stejná prvočísla). Už víme, že  $v_{p_i}((m, n)) = \min(v_{p_i}(m), v_{p_i}(n))$  a  $v_{p_i}([m, n]) = \max(v_{p_i}(m), v_{p_i}(n))$ . Z toho pak můžeme vyvodit

$$\begin{aligned} (m, n) &= p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}, \\ [m, n] &= p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}. \end{aligned}$$

S  $p$ -valuacemi je nyní snadné dokázat rovnosti, jako je tato:

**Příklad.** Dokaž, že

$$\frac{[a, b, c]^2}{[a, b] \cdot [b, c] \cdot [c, a]} = \frac{(a, b, c)^2}{(a, b) \cdot (b, c) \cdot (c, a)}.$$

(USAMO 1972)

*Řešení.* Abychom měli jistotu, že pracujeme s celými čísly, tak si nejdříve rovnost upravíme do tvaru

$$[a, b, c]^2 \cdot (a, b) \cdot (b, c) \cdot (c, a) = (a, b, c)^2 \cdot [a, b] \cdot [b, c] \cdot [c, a].$$

Vezměme si libovolné prvočíslo  $p$  a označme  $x = v_p(a), y = v_p(b), z = v_p(c)$ . Můžeme BÚNO předpokládat  $x \geq y \geq z$ . Označme  $L$  a  $P$  levou a pravou stranu rovnosti. Spočítáme jejich  $p$ -valuace

$$\begin{aligned} v_p(L) &= 2 \cdot \max(x, y, z) + \min(x, y) + \min(y, z) + \min(z, x) = 2x + y + 2z, \\ v_p(P) &= 2 \cdot \min(x, y, z) + \max(x, y) + \max(y, z) + \max(z, x) = 2x + y + 2z. \end{aligned}$$

<sup>14</sup>Jde vlastně o obvyklý pohled, který se učí ve škole. Většinou je ale naprosto nevhodný pro výpočet NSD (zkus se například zeptat své učitelky, jak by počítala NSD čísel  $2^{42} + 3^{42}$  a  $2^{42}$ ), na rozdíl od Euklidova algoritmu, který je rychlý i pro velká čísla. Velká čísla totiž neumíme rychle rozkládat na prvočísla.

Vidíme, že každým prvočíslem je levá i pravá strana dělitelná ve stejné mocnině, takže se obě strany rovnají.

Další využití  $p$ -valuací najdeme, pokud se v úloze na dělitelnost setkáme s faktoriály.<sup>15</sup> Uvedeme si základní tvrzení, které se v takových úlohách používá.

**Tvrzení.** (Legendreova formule)

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

*Důkaz.* Nejprve si uvědomme, že součet je vlastně jen konečný, protože od jistého členu bude  $n < p^k$ , a tak budou všechny následující členy už jen nulové. A proč vzoreček funguje? Vezmeme všechna čísla menší nebo rovná  $n$ . Nejprve započítáme jedničku za všechna čísla dělitelná  $p$ , kterých je  $\lfloor n/p \rfloor$ . Ale některá čísla jsou dělitelná dokonce  $p^2$ , za každé z nich tedy připočítáme další jedničku v dalším členu  $\lfloor n/p^2 \rfloor$ . Poté připočítáme další jedničku za čísla dělitelná  $p^3$ , atd.

**Cvičení.**

- (i) Rozlož 15! na prvočísla.
- (ii) Urči, kolika nulami končí 100!.
- (iii) Dokaž, že číslo  $N = 46! \cdot 47! \cdot 48! \cdot 49!$  není druhou mocninou celého čísla, a najdi jeho největší dělitel, který druhou mocninou celého čísla je.

*Návod.*

- (i) Stačí spočítat  $p$ -valuace pro prvočísla menší než 15.
- (ii) Stačí spočítat  $v_5(100!)$ .
- (iii) Zde je výhodnější nepočítat  $p$ -valuace všech prvočísel v součinu, ale jen se zamyslet, jestli je  $p$ -valuace sudá.

**Úloha.** (těžká) Dokaž, že číslo  $M_n = (2n)!/(n!)^2$  je celé a že pro každé prvočíslo  $p$  platí  $p^{v_p(M_n)} \leq 2n$ .

*Návod.* Spočti si  $p$ -valuaci čitatele a jmenovatele, odečti je od sebe a dokaž, že

$$0 \leq \left\lfloor \frac{2n}{x} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{x} \right\rfloor \leq 1.$$

Uvědom si, že  $v_p(M_n)$  je maximálně takové  $k$ , že  $p^k \leq 2n < p^{k+1}$ .

## Náročnější pasáž

Díky tomuto zdánlivě samoúčelnému cvičení dostaneme velmi dobrý odhad počtu prvočísel. Zatím víme jen to, že jich je nekonečně mnoho, ale nemáme žádnou představu o tom, jak „husté“ se mezi přirozenými čísly vyskytují. Označme tedy  $\pi(x)$  počet prvočísel menších než  $x$  a zkusme tuto funkci nějak odhadnout.

Dá se poměrně snadno indukci dokázat, že pro  $M_n$  z předchozí úlohy platí  $M_n \geq 2^n$ . Spolu s tím, že každé prvočíslo splňuje  $p^{v_p(M_n)} \leq 2n$ , dostaneme, že pro počet prvočísel  $\pi(2n)$ , která jsou menší než  $2n$  (žádné větší prvočíslo nedělí  $M_n$ ), platí  $(2n)^{\pi(2n)} \geq M_n \geq 2^n$ . Pokud označíme  $x = 2n$ , můžeme předchozí vztah upravit do tvaru

$$\pi(x) \geq \frac{1}{2} \cdot \frac{x}{\log_2 x}.$$

<sup>15</sup>Připomeňme si, že číslo  $n!$  je rovno  $1 \cdot 2 \cdot \dots \cdot n$  a čte se  $[n]$  faktoriál].

To jsme tedy dokázali pro sudá  $x$ . Pro  $x$  lichá máme

$$\pi(x) \geq \pi(x-1) \geq \frac{1}{2} \cdot \frac{x-1}{\log_2(x-1)}.$$

## Návrat do reality

Pokud nevíš, co je funkce  $\log_2 x$  nebo jak přesně jsme k výše uvedenému výsledku dospěli, nezoufej. Nebudeš to dále v seriálu potřebovat a jen věz, že jsme si ukázali, že je prvočísel opravdu hodně.

## Eulerova věta

Nejprve si zavedeme dva užitečné pojmy.

**Definice.** *Úplnou sadou zbytků* myslíme množinu  $\{0, 1, 2, \dots, n-1\}$  zbytků modulo  $n$ . Značíme ji  $\mathbb{Z}_n$ . Když v ní sčítáme nebo násobíme, tak myslíme automaticky sčítání a násobení modulo  $n$ . *Redukovaná sada zbytků* je podmnožina  $\mathbb{Z}_n$  obsahující všechna čísla nesoudělná s  $n$ . Značíme ji  $\mathbb{Z}_n^*$ .

Například pro  $n = 10$  je redukovaná sada zbytků  $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ . Pro prvočíslu  $p$  je  $\mathbb{Z}_p^*$  množina  $\{1, 2, \dots, p-1\}$ , tedy  $\mathbb{Z}_p$  bez nuly.

**Cvičení.** Rozmysli si, že součin dvou prvků ze  $\mathbb{Z}_n^*$  je opět v  $\mathbb{Z}_n^*$ . Jak je to s jejich součtem?

**Cvičení.** Uvědom si, jak se pojmy, které známe, dají převést do řeči sad zbytků. Například, že  $a \equiv b \pmod{n}$  říká totéž, co  $a = b + kn$  v  $\mathbb{Z}_n$ , nebo že Eulerova funkce<sup>16</sup> není nic jiného než počet prvků  $\mathbb{Z}_n^*$ . Tvzení z minulého dílu, že „zbytky lze dělit“ zase říká, že každý prvek ze  $\mathbb{Z}_n^*$  má v  $\mathbb{Z}_n^*$  inverzi.<sup>17</sup>

S těmito pojmy jsme již vlastně pracovali, jejich pořádné zavedení nám ale usnadní mnoho úvah.

V minulém díle jsme se seznámili s Malou Fermatovou větou. Nyní si ukážeme její zobecnění pro libovolné přirozené modulo  $m$ , které se přepisuje Eulerovi.

**Věta.** (Eulerova) *Nechť  $(a, m) = 1$ . Pak  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .*

Důkaz se dá provést stejně jako důkaz MFV v prvním díle, uvedeme si však ještě jiný (a překvapivě kratší) důkaz.

*Důkaz.* Vezměme redukovanou sadu zbytků  $\mathbb{Z}_m^*$ . Nechť  $a$  je pevně dané číslo nesoudělné s  $m$ . Pokud jím každý prvek ze  $\mathbb{Z}_m^*$  vynásobíme, dostaneme opět celou  $\mathbb{Z}_m^*$ , jen v jiném pořadí. Kdyby se totiž nějaké dva prvky  $ak$  a  $al$  rovnaly ( $k \neq l$ ), tedy

$$ak \equiv al \pmod{m},$$

tak díky tomu, že  $(a, m) = 1$ , to znamená i  $k \equiv l \pmod{m}$ , což je požadovaný spor.

Například pro  $m = 10$  a  $a = 3$  (víme, že 3 je v  $\mathbb{Z}_{10}^*$ ) máme

$$\{3 \cdot 1, 3 \cdot 3, 3 \cdot 7, 3 \cdot 9\} = \{3, 9, 1, 7\} = \{1, 3, 7, 9\}.$$

<sup>16</sup>Připomeneme, že Eulerova funkce  $\varphi(n)$  přiřazuje číslu  $n$  počet přirozených čísel menších nebo rovných  $n$  a nesoudělných s  $n$ .

<sup>17</sup>Inverzi čísla  $a$  ze  $\mathbb{Z}_n^*$  myslíme takové číslo  $a^{-1}$ , že  $a \cdot a^{-1} \equiv 1 \pmod{n}$ .

Nyní udělejme součin všech prvků ze  $\mathbb{Z}_m^*$ , čímž dostaneme nějaké číslo  $K$  nesoudělné s  $m$ . To je však stejné číslo, jako když vynásobíme všechny zbytky v jiném pořadí, takže platí

$$a^{\varphi(m)} \cdot K \equiv K \pmod{m}.$$

Protože číslo  $K$  je nesoudělné s  $m$ , můžeme jím obě strany vydělit a dostáváme požadovanou kongruenci. Pro náš případ  $n = 10$ ,  $a = 3$  to znamená

$$3^4 \cdot 1 \cdot 3 \cdot 7 \cdot 9 = (3 \cdot 1) \cdot (3 \cdot 3) \cdot (3 \cdot 7) \cdot (3 \cdot 9) \equiv 3 \cdot 9 \cdot 1 \cdot 7 = 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10},$$

takže  $3^{\varphi(10)} = 3^4 \equiv 1 \pmod{10}$ .

**Příklad.** Nechť  $p$  je prvočíslo a  $b$  je celé číslo. Dokaž, že  $b^{p^2-1} \equiv 1 \pmod{p^2}$ , právě když  $b^{p-1} \equiv 1 \pmod{p^2}$ . (MKS 28–9–4)

*Řešení.* Jak jsme si ukázali v minulém díle,<sup>18</sup>  $\varphi(p^k) = p^k - p^{k-1}$ , tedy speciálně  $\varphi(p^2) = p^2 - p$ . Z Eulerovy věty tedy víme  $b^{p^2-p} \equiv 1 \pmod{p^2}$ . Proto

$$b^{p-1} \equiv 1 \pmod{p^2}, \quad \text{právě když} \quad b^{p^2-p} \cdot b^{p-1} \equiv 1 \pmod{p^2},$$

což je ale po úpravě přesně  $b^{p^2-1} \equiv 1 \pmod{p^2}$ .

## Primitivní prvek

Připomeňme si, že řád  $\text{ord}_m(a)$  čísla  $a$  modulo  $m$  je nejmenší přirozené číslo  $r$  takové, že  $a^r \equiv 1 \pmod{m}$ . Budeme se nyní zabývat otázkou, pro která  $m$  existuje  $a$ , jehož řád je maximální možný, tj.  $\text{ord}_m(a) = \varphi(m)$ . Z Eulerovy věty totiž víme, že řád libovolného prvku je maximálně  $\varphi(m)$ , neboť  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

**Definice.** Pokud  $\text{ord}_m(a) = \varphi(m)$ , nazveme  $a$  *primitivním prvkem* modulo  $m$ .

**Cvičení.** Primitivní prvek je tedy číslo, které „generuje“ celou  $\mathbb{Z}_m^*$ , neboli každé číslo ze  $\mathbb{Z}_m^*$  se dá zapsat jako jeho mocnina.

*Návod.* Co by se stalo, kdyby se dvě mocniny primitivního prvku rovnaly? Kolik je tedy různých mocnin primitivního prvku?

**Příklad.** Najdi primitivní prvek modulo 5 a dokaž, že neexistuje primitivní prvek modulo 8.

*Řešení.* Modulo 5 je primitivní prvek například číslo 2, protože čísla  $2^1, 2^2, 2^3, 2^4$  dávají zbytky po dělení pěti postupně 2, 4, 3, 1, takže opravdu  $\text{ord}_5(2) = 4$  (resp. číslo 2 skutečně generuje celou  $\mathbb{Z}_5^*$ ).

Primitivní prvek modulo 8 nemůže být sudý, protože pak bychom nemohli dostat jako jeho mocninu žádné liché číslo. Na druhou stranu  $1^1 \equiv 1, 3^2 \equiv 1, 5^2 \equiv 1, 7^2 \equiv 1 \pmod{8}$ , takže řád žádného lichého čísla není roven  $\varphi(8) = 4$ .

**Cvičení.** Najdi primitivní prvek modulo 13.

## Náročnější pasáž

K důkazu existence primitivního prvku modulo každé prvočíslo se ještě potřebujeme lehce seznámit s chováním polynomů<sup>19</sup> modulo  $p$ . Jak jsi asi slyšel, polynom stupně  $n$  s reálnými koeficienty

<sup>18</sup>Nebo jak si snadno rozmyslíš.

<sup>19</sup>Polynom s koeficienty ze  $\mathbb{Z}_p$  je funkce  $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$  taková, že  $P(x) = \sum_{i=0}^n a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , kde  $a_i \in \mathbb{Z}_p$  a  $n \in \mathbb{N}$ . Je-li  $a_n \neq 0$ , pak říkáme, že polynom má stupeň  $n$ . Polynom nazýváme nulový, pokud jsou všechny jeho koeficienty nulové.

má maximálně  $n$  kořenů v reálných číslech, a dokonce přesně  $n$  kořenů v oboru komplexních čísel. Pro sady zbytků máme tuto analogii:

**Věta.** (Lagrangeova<sup>20</sup>) *Nechť  $P$  je nenulový polynom stupně  $n$  s koeficienty ze  $\mathbb{Z}_p$ . Pak má rovnice  $P(x) \equiv 0 \pmod{p}$  maximálně  $n$  kořenů modulo  $p$ .*

*Důkaz.* Postupujeme indukcí podle  $n$ . Pro  $n = 0$  to platí triviálně. Předpokládejme, že tvrzení platí pro nějaké  $n$ , a dokažme, že platí i pro  $n + 1$ . Nechť je  $P(x) = \sum_{i=0}^{n+1} a_i x^i$  polynom stupně  $n + 1$ . Pokud má 0 kořenů, jsme hotovi, protože 0 je menší než  $n + 1$ . Jinak má nějaký kořen  $r$ , a protože pro každé  $i$  platí  $x - r \mid x^i - r^i$ , tak můžeme upravit  $P(x) = P(x) - P(r) = \sum_{i=0}^{n+1} a_i (x^i - r^i) = (x - r)Q(x)$ , kde  $Q$  je nějaký polynom stupně  $n$  a má tedy z indukčního předpokladu maximálně  $n$  kořenů.

Dosud jsme nijak nevyužili, že pracujeme modulo prvočíslo. Víme, že když  $p$  je prvočíslo, pak z  $ab \equiv 0 \pmod{p}$  plyne  $a \equiv 0 \pmod{p}$  nebo  $b \equiv 0 \pmod{p}$ . To znamená, že pokud  $x$  je kořen polynomu  $F(x)G(x)$  modulo  $p$ , pak musí být také kořenem jednoho z polynomů  $F$  nebo  $G$ . V našem případě víme, že  $F(x) = x - r$  má jeden kořen a  $G(x) = Q(x)$  má maximálně  $n$  kořenů, takže  $P(x) = F(x)G(x)$  má maximálně  $n + 1$  kořenů. Tím je indukční krok hotov.

Uvědom si, že věta neplatí pro složená modula! Například polynom  $x^2 - 1$  má 4 kořeny modulo 8, přestože je jeho stupeň jen 2.

Nyní jsme dostatečně vyzbrojeni pro důkaz existence primitivního prvku.

**Věta.** *Pro každé prvočíslo  $p$  existuje primitivní prvek modulo  $p$ .*

*Důkaz.* Využijeme Lagrangeovu větu a především poslední tvrzení z předchozího dílu, které říká, že

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

Označme  $\psi(d)$  počet zbytků ze  $\mathbb{Z}_p^*$ , které mají řád  $d$ . Již víme, že pokud existuje prvek řádu  $d$ , tak  $d \mid p - 1$ . Protože každý prvek má nějaký řád a žádný prvek nemá dva různé řády, dostáváme, že<sup>21</sup>

$$\sum_{d|p-1} \psi(d) = |\mathbb{Z}_p^*| = p - 1,$$

takže také

$$\sum_{d|p-1} \psi(d) = p - 1 = \sum_{d|p-1} \varphi(d). \quad (\heartsuit)$$

Mějme nějaké  $d \mid p - 1$ . Ukážeme, že  $\psi(d) \leq \varphi(d)$ . Pokud neexistuje žádné  $a$ , které má řád  $d$ , tak je zřejmě  $0 = \psi(d) \leq \varphi(d)$ . V opačném případě si takové  $a$  vezmeme. Pak jsou všechna čísla  $a^0, a^1, \dots, a^{d-1}$  různá (rozmysli si). Ale přitom pro  $i \in \{0, \dots, d - 1\}$  platí  $(a^i)^d - 1 \equiv 0 \pmod{p}$ . Navíc podle Lagrangeovy věty má polynom  $x^d - 1$  maximálně  $d$  kořenů, takže už jsme našli všechny. Vezmeme si  $i \in \{0, 1, \dots, d - 1\}$ , které je soudělné s  $d$ . Nechť  $(i, d) = k$  a  $i = mk$ ,  $d = nk$ . Potom

$$(a^i)^n \equiv (a^m)^d \equiv 1 \pmod{p},$$

takže  $a^i$  nemá řád  $d$ , nýbrž  $n$ . To znamená, že čísla, která mají řád  $d$ , jsou ta čísla  $a^i$ , která mají i nesoudělné s  $d$ , a je jich tedy maximálně  $\varphi(d)$ . Tudíž  $\psi(d) \leq \varphi(d)$ .

Kdyby nyní pro nějaké  $d \mid p - 1$  platilo  $\psi(d) < \varphi(d)$ , tak by neplatila rovnost  $(\heartsuit)$ , protože levá strana by byla menší než pravá. Takže speciálně  $\psi(p - 1) = \varphi(p - 1) > 0$ . Mimo jiné jsme tedy zjistili, kolik má prvočíslo primitivních prvků.

<sup>20</sup>Joseph-Louis Lagrange byl významný italsko-francouzský matematik a astronom (1736–1813).

<sup>21</sup>Symbol  $|\mathbb{Z}_p^*|$  značí počet prvků množiny  $\mathbb{Z}_p^*$ .

## Návrat do reality

V předchozí části jsme si dokázali existenci primitivního prvku modulo každé prvočíslo. Přestože je důkaz poměrně náročný, k samotnému řešení úloh ho znát nepotřebuješ. Existenci primitivního prvku můžeš využívat bez důkazu.<sup>22</sup> Tento fakt nyní zkusíme zužítkovat v úlohách:

**Příklad.** Nechť  $p$  je liché prvočíslo. Najdi všechna taková  $k$ , že  $1^k + 2^k + \dots + (p-1)^k$  je dělitelné  $p$ .  
(Hungary-Israel Math Competition 2009)

*Řešení.* Každé číslo  $a$  z množiny  $\mathbb{Z}_p^*$  se dá zapsat jako  $q^{i_a}$ , kde  $q$  je primitivní prvek. Čísla  $i_a$  jsou navzájem různá. Proto

$$\begin{aligned} 1^k + 2^k + \dots + (p-1)^k &\equiv (q^{i_1})^k + (q^{i_2})^k + \dots + (q^{i_{p-1}})^k \\ &\equiv (q^k)^{i_1} + (q^k)^{i_2} + \dots + (q^k)^{i_{p-1}} \\ &= (q^k)^1 + (q^k)^2 + \dots + (q^k)^{p-1} \pmod{p}, \end{aligned}$$

neboť čísla  $i_1, i_2, \dots, i_{p-1}$  jsou čísla  $1, 2, \dots, p-1$ , jen v jiném pořadí.

Tímto jsme se zbavili nepříjemného součtu a nahradili ho známou geometrickou posloupností, kterou už není problém sečíst. Musíme ale ještě rozehrát dva případy.

- (i)  $q^k \equiv 1 \pmod{p}$ , což je ekvivalentní s  $(p-1) = \text{ord}_p(q) \mid k$ , protože  $q$  je primitivní prvek. Potom  $(q^k)^1 + (q^k)^2 + \dots + (q^k)^{p-1} \equiv 1 + 1 + \dots + 1 = p-1 \pmod{p}$ , takže tato  $k$  nevyhovují.
- (ii)  $q^k \not\equiv 1 \pmod{p}$ . Poté můžeme sečíst geometrickou posloupnost pomocí známého vzorce<sup>23</sup> a dostaneme<sup>24</sup>

$$q^k \cdot \frac{(q^k)^{p-1} - 1}{q^k - 1} \equiv q^k \cdot \frac{1 - 1}{q^k - 1} = 0 \pmod{p}.$$

Vyhovují tedy všechna  $k$ , která nejsou dělitelná  $p-1$ .

**Cvičení.** (těžké) Ukaž, že 2 je primitivní prvek mod  $3^n$ .

*Návod.* Indukcí podle  $n$ . Musí platit  $\varphi(3^n) = \text{ord}_{3^n}(2) \mid \text{ord}_{3^{n+1}}(2) \mid \varphi(3^{n+1})$ . Další indukci vyluč případ  $\text{ord}_{3^{n+1}}(2) = 2 \cdot 3^{n-1}$ .

Primitivní prvek neexistuje jen pro prvočíselné moduly. Známý výsledek shrnuje následující věta, která popisuje všechna modula, pro která primitivní prvek existuje. Důkaz už není tak těžký jako pro případ, kdy  $n$  je prvočíslo, ale ani tolik zajímavý, takže ho zde neuvádíme.

**Věta.** *Primitivní prvek modulo  $n$  existuje právě tehdy, když  $n = 1, 2, 4, p^k$  nebo  $2p^k$ , kde  $p$  je liché prvočíslo a  $k$  je přirozené číslo.*

Zmíníme ještě slavnou Dirichletovu<sup>25</sup> větu. Důkaz této věty je bohužel nad rámec našeho seriálu. Někdy se však hodí i v olympiádě (typicky ji vzorové řešení nevyužívá, ale Dirichletova věta je opravdu „silná“).

<sup>22</sup>Jak v PraSeti, tak v olympiádě.

<sup>23</sup>Pokud ses s geometrickou posloupností ještě nesetkal, tak věz, že to je posloupnost tvaru  $a_n = k \cdot q^{n-1}$ , kde  $k \neq 0$  a  $q \neq 1$  jsou kladná reálná čísla. Dá se snadno odvodit, že součet prvních  $n$  členů je  $k \cdot \frac{q^n - 1}{q - 1}$ .

<sup>24</sup>To, že máme zlomek v kongruenci, je v pořádku. Zlomek  $\frac{a}{b}$  se totiž v kongruenci dá chápat jako  $a \cdot b^{-1}$ , tedy  $a$  vynásobeno inverzním prvkem  $b$ .

<sup>25</sup>(Johann Peter Gustav) Lejeune Dirichlet (1805–1859) byl německý matematik. Proslavil se hlavně výsledky v teorii čísel, matematické analýze a statistice. Vzal si nejmladší sestru slavného hudebního skladatele Mendelssohna-Bartholdyho, Rebeccu.



**Věta.** (Dirichletova) *Pro každá dvě nesoudělná přirozená čísla  $a, b$  existuje nekonečně mnoho prvočísel tvaru  $ak + b$ .*

V následující úloze ukážeme, jak se dá vhodně zkombinovat s úvahami o primitivním prvku.

**Příklad.** Ukaž, že existuje nekonečně mnoho přirozených  $n$  takových, že číslo  $n^4 + 1$  má prvočíselného dělitele většího než  $2n$ . (MKS 30–2–8)

*Řešení.* Nechť  $p$  je prvočíslo tvaru  $8k + 1$  a  $q$  primitivní prvek modulo  $p$ . Potom z MFV víme, že

$$1 \equiv q^{p-1} \equiv q^{8k} \equiv (q^{4k})^2 \pmod{p},$$

což se dá přepsat do tvaru

$$(q^{4k} + 1)(q^{4k} - 1) \equiv 0 \pmod{p}.$$

Protože  $p$  je prvočíslo, dělí alespoň jednu ze závorek. Ale  $q$  je primitivní prvek, takže  $p \nmid q^{4k} - 1$ . Proto kongruence  $n^4 + 1 \equiv 0 \pmod{p}$  má vždy řešení pro prvočíslo tvaru  $8k + 1$  (a to  $n = q^k$ ). Můžeme si vzít takové  $n$ , že  $1 \leq n \leq p - 1$  (protože  $p \nmid n$  a  $(n + kp)^4 + 1 \equiv n^4 + 1 \pmod{p}$ ). Ale zřejmě platí  $n^4 + 1 \equiv (p - n)^4 + 1$ , takže si můžeme vzít to z čísel  $n, p - n$  které je menší. Tím dostaneme nové  $n$ , pro které platí  $n < p/2$ .

Zbývá dokázat, že takovýchto  $n$  existuje nekonečno. Budeme postupovat sporem. Nechť je takových  $n$  jen konečně a  $n_1$  je největší z nich. Podle Dirichletovy věty existuje nekonečně mnoho prvočísel tvaru  $8k + 1$ , takže najdeme i takové, že  $p > n_1^4 + 1$ . Z předchozího odstavce plyne, že existuje  $n_2$  takové, že  $p \mid n_2^4 + 1$  a  $p > 2n_2$ . Navíc  $n_2^4 + 1 \geq p > n_1^4 + 1$ . Takže jsme našli vyhovující  $n$  větší než  $n_1$ , což je požadovaný spor.

**Úloha.** Urči počet všech posloupností reálných čísel  $\{a_n\}_{n=1}^{\infty}$  takových, že pro všechna přirozená čísla  $m, n$  platí  $a_m \cdot a_n = a_{m \cdot n}$  a zároveň  $a_n = a_{n+2011}$ . (MKS 30–6–8)

## Řády

V této kapitole si důkladně procvičíme práci s řády. Opravdu se totiž hodí mít je v malíčku.

**Příklad.** Najdi všechna kladná celá čísla nesoudělná se všemi členy nekonečné posloupnosti

$$a_n = 2^n + 3^n + 6^n - 1.$$

(IMO 2005)

*Řešení.* Číslo 1 to triviálně splňuje. Všechna další čísla tvaru  $2^k \cdot 3^l$  pro  $k, l \geq 0$  nevyhovují, protože jsou soudělná s  $a_2 = 48 = 2 \cdot 3 \cdot 8$ . Dokážeme, že ani žádné jiné přirozené číslo s výjimkou jedničky zadání nesplní. Vezmeme si prvočíslo  $p > 3$  a najdeme v posloupnosti člen, který je tímto prvočíslem dělitelný. Vzpomeneme si na malou Fermatovu větu, která nám pomáhá zbavovat se mocnin v kongruencích. Po chvíli zkoušení zjistíme, že viník je člen  $a_{p-2}$ .

$$\begin{aligned} 6 \cdot a_{p-2} &= 6 \cdot (2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \\ &\equiv 3 + 2 + 1 - 6 = 0 \pmod{p}, \end{aligned}$$

a jelikož  $p > 3$ , tak nutně  $p \mid a_{p-2}$ .

Podívejme se, co nám řeknou řády o dělitelích Mersennových<sup>26</sup> čísel. Připomeňme, že Mersennovo číslo je číslo ve tvaru  $2^n - 1$ .

<sup>26</sup>Marin Mersenne (1588–1648) byl francouzský matematik, filozof, teolog a hudební teoretik.

**Cvičení.** Necht  $p$  je prvočíslo a  $q$  je prvočíslo, které dělí  $2^p - 1$ . Dokaž, že pak  $p \mid q - 1$ .

*Návod.* Řád prvku 2 modulo  $q$  dělí všechna čísla  $k$ , pro která platí  $2^k \equiv 1 \pmod{q}$ . Díky MFV je mezi nimi i  $q - 1$ .

**Cvičení.** Pokud prvočíslo  $p$  dělí  $n$ -té Fermatovo číslo  $2^{2^n} + 1$ , pak  $2^{n+1} \mid p - 1$ .

*Návod.* Úlohu zabijeme podobnou myšlenkou jako minule. Zde je však třeba ještě použít trik „umocnění kongruence na druhou“, abychom si vyrobili z  $-1$  jedničku.

**Příklad.** Dokaž, že pro  $n > 1$  nemůže nastat  $n \mid 2^{n-1} + 1$ .

*Řešení.* Řešení je velmi trikové, ale pěkné. Budeme postupovat sporem, tedy předpokládejme, že takové  $n$  existuje. Zřejmě  $n$  nemůže být sudé. Rozložme si  $n$  na prvočísla:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}.$$

Vezměme si takové  $i$ , že  $v_2(p_i - 1)$  je nejmenší. Napišme  $p_i = 1 + m \cdot 2^r$ , kde  $m$  je nějaké liché číslo. Z výběru  $i$  víme, že pro každé prvočíslo  $p_j$  z rozkladu čísla  $n$  platí  $p_j^{\alpha_j} \equiv 1 \pmod{2^r}$ . Když tyto kongruence vynásobíme pro  $i = 1, \dots, k$ , tak dostaneme  $n \equiv 1 \pmod{2^r}$ , takže  $n - 1 = t \cdot 2^r$ . Z podmínky ze zadání víme  $2^{t \cdot 2^r} \equiv -1 \pmod{p_i}$ , takže po umocnění na liché číslo  $m$  dostáváme, že

$$-1 = (-1)^m \equiv (2^{t \cdot 2^r})^m \equiv 2^{t \cdot m \cdot 2^r} \equiv 2^{(p_i - 1) \cdot t} \equiv 1^t = 1 \pmod{p_i}.$$

Přitom poslední kongruence plyne z MFV. Ale potom  $p_i \mid 2$ , což je spor.

## Kvadratické zbytky a reciprocita

V minulém díle jsme se seznámili s kvadratickými zbytky. To jsou ta čísla  $k$  ze  $\mathbb{Z}_p^*$ , pro která existuje  $x$  takové, že platí  $x^2 \equiv k \pmod{p}$ . Ukážeme si další užitečná tvrzení o zbytcích. Představíme si také standardní metody, jak kvadratické zbytky využívat v úlohách. Připomeneme ještě, že Legendreovým symbolem  $\left(\frac{a}{p}\right)$  myslíme

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

Zabývejme se tedy vlastnostmi Legendreova symbolu. Je dobré si uvědomit, že Legendreův symbol není jen hezké značení vlastnosti „být kvadratickým zbytkem“. Je to chytře zvolená funkce z množiny zbytků do množiny  $\{-1, 0, 1\}$ , která má mnoho pěkných vlastností. Díky nim se nám například značně zjednoduší rozhodování, zda je daný zbytek kvadratický.

**Tvrzení.** (Základní vlastnosti Legendreova symbolu) *Necht  $p$  je liché prvočíslo,  $a, b, k$  jsou celá čísla, pak platí:*

- (i) Pokud  $a \equiv b \pmod{p}$ , pak  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ , neboli  $\left(\frac{a}{p}\right) = \left(\frac{a + kp}{p}\right)$ ,
- (ii) (Eulerovo kritérium)  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- (iii)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ .

*Návod.*

- (i) Pokud existuje číslo  $x$  takové, že  $x^2 \equiv a \pmod{p}$ , pak také platí  $x^2 \equiv b \pmod{p}$ . Pokud takové číslo neexistuje, nemůže existovat ani pro  $b$ .
- (ii) Viz minulý díl.
- (iii) Aplikuj Eulerovo kritérium.

Už pomocí těchto jednoduchých vlastností můžeme odvodit zajímavé výsledky. V následujícím tvrzení ještě o kvadratické zbytky nejde.

**Tvrzení.** *Mersennovo číslo  $2^n - 1$  je složené, pokud je  $n$  složené.*

*Důkaz.* Pokud  $n = ab$ , můžeme  $2^n - 1$  upravit pomocí známého vzorce<sup>27</sup>

$$2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \dots + (2^a)^1 + (2^a)^0),$$

přičemž oba členy v součinu napravo jsou větší než jedna. Číslo  $2^{ab} - 1$  má tedy dva netriviální dělitele, takže je složené.

S pomocí kvadratických zbytků se dá sestrojít případ, kdy podmínka prvočíselnosti  $n$  nestačí k prvočíselnosti čísla  $2^n - 1$ .<sup>28</sup>

**Úloha.** Necht čísla  $4n + 3$  a  $8n + 7$  jsou prvočísla. Pak číslo  $M_{4n+3} = 2^{4n+3} - 1$  je složené.

*Návod.* Například  $23 \mid M_{11}$ ,  $47 \mid M_{23}$  nebo  $503 \mid M_{251}$ .

Dostáváme se k hlavnímu výsledku teorie kvadratických zbytků – kvadratické reciprocitě. Ta nám říká, že pokud víme, zda je prvočíslo  $p$  kvadratický zbytek modulo jiné prvočíslo  $q$ , můžeme kongruenci „obrátit“ a dozvíme se, zda je  $q$  kvadratický zbytek modulo  $p$ . Všechno, co jsme dosud dělali, se (s trochou nadsázky) dá považovat za intuitivní. To však není případ kvadratické reciprocitě – důvody, proč tato věta platí, rozhodně elementární nejsou.

**Věta.** (Kvadratická reciprocita) *Necht  $p, q$  jsou lichá prvočísla. Pak platí*

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

Bohužel si nevedeme důkaz této věty, protože je obtížný a v seriálu nám na něj nezbyvá místo. Pokud Tě to zajímá, jistě najdeš rozmanité důkazy v pokročilejších učebnicích teorie čísel nebo na internetu (sám Gauss<sup>29</sup> byl prý kvadratickou reciprocitou natolik nadšen, že ji nazýval „zlatou větou“ a objevil několik různých důkazů).

Ještě si všimni, že kvadratická reciprocita nám říká, že existuje nějaké řešení  $x$  kongruencí typu  $x^2 \equiv p \pmod{q}$ , ale nedává nám žádný nástroj, jak toto řešení najít. Ještě než si ukážeme příklad na využití reciprocitě, přidáme dodatek, kterým počítáme kvadratické zbytky v případech, které reciprocita nezahrnuje, tedy pro  $-1$  a  $2$ .

**Tvrzení.** (Dodatek ke kvadratické reciprocitě) *Pro liché prvočíslo  $p$  platí*

- (i)  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ ,
- (ii)  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ .

<sup>27</sup>Jak si počtvá čtenářka snadno roznásobí.

<sup>28</sup>Neboli neplatí Mersennova hypotéza, která tvrdí opak.

<sup>29</sup>Carl Friedrich Gauss (1777–1855) byl slavný německý matematik a fyzik, který ovlivnil mnoho matematických disciplín včetně teorie čísel. Jeho mozek prý vážil 1492 gramů.

První tvrzení plyne jednoduše z Eulerova kritéria. Druhé tvrzení je opět těžké, jeho důkaz si tedy dovolíme zamlčet. Spolu s dodatkem se kvadratická reciprocita stává ultimátní zbraní, jak rozhodnout, jestli je něco kvadratický zbytek.

**Cvičení.** (uvědomovací) Mějme lichá prvočísla  $p, q$ . Uvědom si, že  $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right)$  je  $-1$ , právě když jsou obě prvočísla tvaru  $4k + 3$ .

Ukažme si tedy, jak se reciprocita používá.

**Příklad.** Zjisti, zda je 179 kvadratický zbytek modulo 463.

*Řešení.* Všimneme si, že příklad je zadán tak pěkně, že 179 a 463 jsou prvočísla. Počítejme tedy s využitím tvrzení (i) a (iii) z úvodu kapitoly a s pomocí kvadratické reciprocit:

$$\begin{aligned} \left(\frac{179}{463}\right) &= -\left(\frac{463}{179}\right) = -\left(\frac{105}{179}\right) = -\left(\frac{3 \cdot 5 \cdot 7}{179}\right) = -\left(\frac{3}{179}\right) \cdot \left(\frac{5}{179}\right) \cdot \left(\frac{7}{179}\right) \\ &= -\left(-\left(\frac{179}{3}\right)\right) \cdot \left(\frac{179}{5}\right) \cdot \left(-\left(\frac{179}{7}\right)\right) = -\left(\frac{2}{3}\right) \cdot \left(\frac{4}{5}\right) \cdot \left(\frac{4}{7}\right) = 1. \end{aligned}$$

Takto jsme dostali, že 179 je kvadratický zbytek modulo 463 (aniž bychom museli najít konkrétní řešení kongruence  $x^2 \equiv 179 \pmod{463}$ ).

**Cvičení.** Je 365 kvadratický zbytek modulo 1847?

## A co na to primitivní prvek?

Ukážeme si důležitou souvislost mezi kvadratickými zbytky a primitivním prvkem. Jak víme, primitivní prvek je takový, že jeho umocňováním dostaneme všechny různé zbytky. Které z nich jsou kvadratické? Odpověď je jednoduchá – jsou to ty, které vzniknou umocněním primitivního prvku  $q$  na sudou mocninu. Každá sudá mocnina  $q$  je totiž zřejmě kvadratický zbytek. Žádné další číslo už kvadratický zbytek nebude. Počet sudých mocnin mezi zbytky je totiž  $(p-1)/2$ , což je přesně počet kvadratických zbytků!

**Cvičení.** Dokaž, že kvadratický zbytek nemůže být (pro lichá prvočísla) primitivním prvkem.

**Cvičení.** Urči prvočísla  $p$ , pro která je  $q$  primitivní prvek, právě když je  $-q$  primitivní prvek.

**Úloha.** Mějme prvočísla  $p$ . Ukaž, že  $p$  je Fermatovo prvočísla (tedy tvaru  $2^{2^n} + 1$ ) právě tehdy, když je každý kvadratický nezbytek zároveň primitivním prvkem modulo  $p$ .

*Návod.* Uvědom si, kolik je nezbytků a kolik je primitivních prvků modulo  $p$ . Tím dokážeš, že Fermatovo prvočísla podmínku splňuje a že  $p$  je tvaru  $2^m + 1$ . Kdyby nějaké liché číslo dělilo  $m$ , vyuzij vzorečku

$$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - \dots - ab^{2k-1} + b^{2k})$$

a dostaneš spor s prvočíslností  $p$ . Proto je  $m$  tvaru  $2^n$ .

## 2. podzimní série – Podobnost a shodnost

VÝSLEDKOVÁ LISTINA

1.–3.	František	Couf	1	GZborovPH	3-355555	25	<b>25,00</b>
1.–3.	Martin	Raszyk	4	G Karviná	33355555	25	<b>25,00</b>
1.–3.	Miroslav	Stankovič	4	G PošKošice	---55555	25 + <i>i</i>	<b>25,00</b>
4.	Jakub	Svoboda	4	G KomHavíř	33155455	24 + <i>i</i>	<b>23,94</b>
5.	Filip	Bialas	1	G OpatovPH	-33554-5	22	<b>23,86</b>
6.	Vojtěch	Suchánek	3	G JarošeBO	33355445	23	<b>23,63</b>
7.	Radovan	Švarc	3	G ČTřebová	00355455	24	<b>23,02</b>
8.	Martin	Hora	4	GMikul23PL	3--55455	24	<b>22,77</b>
9.	Marián	Poppr	3	GJNerudyPH	1-355454	23	<b>22,57</b>
10.	Václav	Steinhauser	0	ZŠVranéNVl	333454--	19	<b>22,51</b>
11.	Tereza	Kislingerová	1	G Klatovy	33355---	19	<b>22,43</b>
12.	Martin	Surma	3	GJWolkraPV	2335545-	22 - <i>i</i>	<b>22,37</b>
13.	Anh Dung	Le	4	G Tachov	---55455	24	<b>22,33</b>
14.	Pavel	Turek	1	GTomkovaOL	33355---	19	<b>21,87</b>
15.–17.	Markéta	Horová	2	GMikul23PL	33355---	19	<b>21,52</b>
15.–17.	Minh Thao	Nguyen	2	GEbenešeKL	33355---	19	<b>21,52</b>
15.–17.	Marian	Poljak	2	GJŠkodyPŘ	33355---	19	<b>21,52</b>
18.	Jakub	Löwit	2	GČeskolIPH	333554--	20	<b>21,45</b>
19.–20.	Ondřej	Darmovzal	3	GJarošeBO	033554--	20	<b>21,41</b>
19.–20.	Václav	Rozhoň	3	GJirsikaČB	333554--	20	<b>21,41</b>
21.	Katarína	Krajčiová	3	GAlejKošic	--35545-	22	<b>21,35</b>
22.	Mikuláš	Zindulka	3	GMikul23PL	33-55-4-	20 - <i>i</i>	<b>21,21</b>
23.	Jan	Šorm	2	GJarošeBO	33355---	19	<b>20,77</b>
24.	Antonín	Češík	4	SPŠElek PA	33-555-	21 + <i>i</i>	<b>20,33</b>
25.	Anh	Le Hoang	2	GJarošeBO	13355---	17	<b>20,12</b>
26.	Lukáš	Sadlek	3	G Čadca	333524--	18	<b>19,83</b>
27.	Marko	Puza	4	G PošKošice	-305545-	22 - <i>i</i>	<b>19,51</b>
28.	Kristýna	Šmidová	4	GMensaPH	333554--	20 + <i>i</i>	<b>19,43</b>
29.	Martin	Kopřiva	2	GMikul23PL	33352---	16	<b>19,28</b>
30.	Jan	Soukup	3	G Klatovy	33-5544-	21	<b>19,14</b>
31.	Miroslav	Psota	4	GHlinŽilina	-2355--5	20 + 2 <i>i</i>	<b>19,07</b>
32.	Eduard	Batmendijn	3	CGStLubovňa	33-5---5	16 + 2 <i>i</i>	<b>18,45</b>
33.	Zuzana	Svobodová	2	G FrýdlINOs	31255---	16	<b>18,43</b>
34.	Jakub	Šebek	4	GKepleraPH	33355---	19	<b>18,35</b>
35.	Karolína	Kuchyňová	3	GMLerchaBO	23355---	18	<b>18,31</b>
36.–37.	Mihály	Kotiers	2	GHSelyhoKM	01355---	14	<b>17,77</b>
36.–37.	Tomáš	Kuzma	2	GAB Senec	03352110	14	<b>17,77</b>
38.	Jiří	Zeman	4	GLesníZlín	3335-44-	19 - <i>i</i>	<b>17,52</b>
39.	Petr	Lukeš	4	GNeumannŽR	33355---	19	<b>17,44</b>

40.	Vojtěch	Lanz	0	GZborovPH	3 2 3 2 - - - -	10	<b>17,36</b>
41.	Daniel	Pišťák	2	GZborovPH	3 2 3 3 5 - - - -	16	<b>17,30</b>
42.	Martin	Špilar	3	G Vyškov	2 2 3 3 5 - - - -	15	<b>17,27</b>
43.	Jakub	Dargaj	4	G PošKošice	- 3 3 5 5 4 - - -	20	<b>17,23</b>
44.	Barbora	Hudcová	4	PORG PH	3 3 2 5 5 - - - -	18	<b>17,22</b>
45.	Miroslav	Krabec	4	G KomHavíř	3 3 3 5 5 - - - -	19 - <i>i</i>	<b>16,95</b>
46.-50.	Jiřina	Duspivová	2	G Kralupy	2 3 3 5 - - - -	13	<b>16,90</b>
46.-50.	Vít	Kalisz	2	FSG Pirna	1 2 - 5 5 - - - -	13	<b>16,90</b>
46.-50.	Patricie	Klosse	2	G ČKrumlov	2 3 3 5 - - - -	13	<b>16,90</b>
46.-50.	Andrea	Kučerová	2	G ČKrumlov	3 3 3 4 - - - -	13	<b>16,90</b>
46.-50.	Jan	Václavek	2	G Ústí n O	3 3 2 5 0 - - - -	13	<b>16,90</b>
51.	Jiří	Česka	1	CMGProstěj	0 3 3 5 - - - -	11	<b>16,83</b>
52.-53.	Jaromír	Mielec	1	GVolgogrOS	3 3 2 5 - - - -	13	<b>16,56</b>
52.-53.	Anna	Steinhauserová	4	G Dačice	3 3 3 5 5 4 - - -	20	<b>16,56</b>
54.	Petr	Jakubčík	0	PORG PH	3 1 - 5 - - - -	9	<b>16,42</b>
55.	Matěj	Konečný	3	G Jírov ČB	3 3 3 5 - 2 - - -	16	<b>16,25</b>
56.	Michaela	Brezinová	2	G KomTřebiš	3 - 3 1 5 - - - -	12	<b>16,00</b>
57.	Minh Tri	Pham	2	NPorg	1 3 3 5 - - - -	12	<b>15,52</b>
58.	Jan	Jurka	3	G MLerchaBO	3 2 3 5 - - - -	13 - <i>i</i>	<b>15,04</b>
59.	Jakub	Sláma	3	G OpatovPH	3 3 1 5 - - - -	12	<b>14,47</b>
60.	Dominik	Krasula	1	G Krnov	3 2 1 3 - 1 - - -	10	<b>14,33</b>
61.-63.	Michaela	Brabcová	2	G Jírov ČB	3 1 - 5 - - - -	10	<b>14,05</b>
61.-63.	Vojtěch	Lukeš	2	G LPika PL	3 2 - 5 - - - -	10	<b>14,05</b>
61.-63.	Peter Kulcsár	Szabó	2	GHselyhoKM	- - - 5 - - - -	10	<b>14,05</b>
64.	Kateřina	Nová	1	G Vimperk	3 3 1 1 - - - -	8	<b>13,81</b>
65.	Daniela	Šindelářová	2	GaSOŠ Telč	1 2 0 3 1 0 - 2 9		<b>13,00</b>
66.	Tomáš	Fiala	3	GLedečNSáz	3 2 1 5 - - - -	11	<b>12,82</b>
67.	Kristýna	Ilievová	3	G Milevsko	2 3 3 - 5 - - - -	13	<b>12,70</b>
68.	Lenka	Kopfová	0	CZŠSL HnM	0 3 3 - - - - -	6 - <i>i</i>	<b>12,68</b>
69.	Marek	Vicha	3	MendelG OP	1 3 - 5 - 1 - - -	10	<b>12,45</b>
70.	Zuzana	Vlasáková	4	G Rumburk	3 3 3 5 - - - -	14	<b>12,22</b>
71.	Henrieta	Michelová	2	GAlejKošic	3 3 3 - - - - -	9	<b>12,02</b>
72.	Michael	Bucha	3	G Zábřeh	3 1 - 4 - - 1 - 9		<b>11,39</b>
73.	Jan	Krejčí	4	G Bilovec	3 1 3 - 5 - - - -	12	<b>10,27</b>
74.	Ludmila	Šimková	4	GPároNitra	- 3 3 5 - - - -	11	<b>10,11</b>
75.	Jan	Kadlec	3	G Klatovy	1 3 - 2 5 - - - -	11	<b>9,49</b>
76.	Pavel	Souček	2	G Nymburk	0 2 3 1 - - - -	6	<b>9,48</b>
77.	Michaela	Bieliková	4	G Sereď	3 3 - 5 - - - -	11	<b>9,32</b>
78.	Viktor	Němeček	3	GJMasar JI	1 2 2 5 - - - -	10	<b>8,90</b>
79.	Hana	Daňiková	1	G Vimperk	3 1 - - 0 - - - -	4	<b>8,48</b>
80.-81.	Lukáš	Honsa	2	G Jírov ČB	- 3 - 2 - - - -	5	<b>8,17</b>
80.-81.	David	Peňáz	2	GNeumannŽR	3 2 0 0 0 - 0 - 5		<b>8,17</b>
82.	Tereza	Koberová	3	G Chrudim	3 3 - - 0 0 - - -	6	<b>8,00</b>
83.	Tran Vi Thanh	Pham	4	GNeumannŽR	3 3 3 - - - - -	9	<b>7,49</b>
84.	Lukáš	Kubacki	1	GNadKavaPH	0 3 - - - - - -	3	<b>6,79</b>
85.-87.	Lucie	Roškotová	2	G Turnov	- - 1 2 0 0 1 0 4		<b>6,76</b>
85.-87.	Adam	Řiha	2	G ČesLípa	3 0 0 - 1 - - 0 4		<b>6,76</b>
85.-87.	Šimon	Tabačko	2	EvG Košice	3 0 1 - - - - 0 - 4		<b>6,76</b>
88.	Markéta	Calábková	3	GJŠkodyPŘ	3 3 - - - - - -	6	<b>6,58</b>
89.	Přemysl	Šťastný	0	G Žamberk	1 1 - - - - - -	2	<b>6,25</b>
90.	Otto	Hollmann	4	GUBalvanJN	3 - - 3 - - - -	6	<b>6,00</b>

91.–93.	Tomáš	Flaschka	2	G Hlučín	3	-----	3	<b>5,27</b>
91.–93.	Jaroslav	Stránský	2	G Tišnov	2	1----	0-3	<b>5,27</b>
91.–93.	Tomáš	Šacha	2	SPŠEB Břeclav	3	00----	0-3	<b>5,27</b>
94.	Irena	Bačinská	4	ŠPMNDAg BA	2	3-----	5	<b>5,00</b>
95.–96.	Jan	Lukáč	3	G ČKrumlov	-	3-----	3	<b>4,23</b>
95.–96.	Emese	Szabó	3	GZKMJ Gal	3	-----	3	<b>4,23</b>
97.	Jakub	Hledík	3	GSŘMRskuteč	-	3-----	3	<b>3,74</b>
98.–102.	Martin	Konečný	2	GStrážnice	0	2-----	2	<b>3,65</b>
98.–102.	Jakub	Marták	2	G GolNitra	0	0100100	2	<b>3,65</b>
98.–102.	Štefan	Ráčák	2	GTajBanBys	-	1-10000	2	<b>3,65</b>
98.–102.	Adéla	Šedová	2	GJungmanLT	0	1100-0-	2	<b>3,65</b>
98.–102.	Jana	Vráblíková	2	GLesníZlín	-	1010-0-	2	<b>3,65</b>
103.	Kristýna	Šudomová	2	GValašKlob	1	--1-000	2	<b>3,30</b>
104.	Nicholas	Čapek	4	GBNěmcovHK	0	3-1----	4	<b>3,26</b>
105.	Veronika	Holubová	3	PORG PH	0	1-1-----	2	<b>2,88</b>
106.–108.	Markéta	Ospálková	1	G Uničov	1	-----	1	<b>2,67</b>
106.–108.	David	Ucháč	1	VOŠDoprPH	0	1--0---	1	<b>2,67</b>
106.–108.	Marie	Vonzino	1	GTomkovaOL	-	-1-----	01	<b>2,67</b>
109.	Jana	Lepšová	4	G Dobruška	-	3-----	3	<b>2,58</b>
110.	Tomáš	Valovič	4	GAHŠ VKrtiš	0	0-1-10-	2	<b>2,00</b>
111.–113.	Tomáš	Beneš	2	GVráLevice	0	100----	1	<b>1,91</b>
111.–113.	Martin	Chabada	2	G Bardejov	0	0-001--	1	<b>1,91</b>
111.–113.	Tomáš	Velich	2	GJHroncaBA	0	100000-	1	<b>1,91</b>
114.	Adam	Gálik	4	GOlivuPopr	0	1000000	1	<b>1,00</b>
115.–128.	Daniel	Backov	2	G Ružomb	0	-----	0-0	<b>0,00</b>
115.–128.	Katarína	Behinská	2	G GolNitra	-	-----	00	<b>0,00</b>
115.–128.	Jaroslav	Cerman	2	GJilemnice	0	-----	0	<b>0,00</b>
115.–128.	Petr	Gintar	3	MendelG OP	0	-0000--	0	<b>0,00</b>
115.–128.	Jakub	Hrubý	2	G Chrudim	0	--0---0	0	<b>0,00</b>
115.–128.	Matěj	Kosma	2	SOŠDoprOS	-	-00000	0	<b>0,00</b>
115.–128.	Alena	Košáková	2	G Strakon	-	-000000	0	<b>0,00</b>
115.–128.	Stanislav	Kruml	3	G Chotěboř	0	-0-----	0	<b>0,00</b>
115.–128.	Jozef	Mišť	2	GAHŠ VKrtiš	-	-00----	0	<b>0,00</b>
115.–128.	Marina	Pogarčenko	2	GJungmanLT	0	000-00-	00	<b>0,00</b>
115.–128.	Tereza	Rašková	3	GTomkovaOL	-	-0--0-	0	<b>0,00</b>
115.–128.	Jáchym	Solecký	1	PORG PH	0	-----	0	<b>0,00</b>
115.–128.	Jiří	Štrincl	3	GSRandyJN	0	-----	0	<b>0,00</b>
115.–128.	Věra	Tesařová	1	MasG Plzeň	-	-0-----	0	<b>0,00</b>

### 3. podzimní série – Funkce

VÝSLEDKOVÁ LISTINA

1.–3.	František	Couf	1	GZborovPH	3 2 – 5 5 5 5 5	25 + <i>i</i>	<b>25,00</b>
1.–3.	Martin	Hora	4	GMikul23PL	3 – – 5 5 5 5 5	25	<b>25,00</b>
1.–3.	Radovan	Švarc	3	G ČTřebová	0 0 3 5 5 5 5 5	25	<b>25,00</b>
4.	Pavel	Turek	1	GTomkovaOL	3 2 2 5 4 5 5 5	24	<b>24,55</b>
5.	Martin	Surma	3	GJWolkraPV	3 3 3 5 5 5 5 0	23	<b>23,41</b>
6.	Ondřej	Darmovzal	3	GJarošeBO	3 3 – 5 4 – 5 5	22 + <i>i</i>	<b>23,10</b>
7.	Filip	Bialas	1	GOpatoVPH	3 3 3 5 4 5 – –	20	<b>22,94</b>
8.	Martin	Raszyk	4	G Karviná	3 3 3 5 4 5 5 5	24	<b>22,58</b>
9.	Lukáš	Sadlek	3	G Čadca	3 0 3 5 5 4 2 –	20	<b>21,41</b>
10.	Jan	Jurka	3	GMLerchaBO	3 3 3 5 4 – 5 –	20	<b>21,34</b>
11.	Jakub	Svoboda	4	G KomHavíř	3 3 2 5 4 5 5 1	22	<b>20,83</b>
12.	Eduard	Batmendijn	3	CGStLubovňa	3 3 3 5 – – – 5	19 + <i>i</i>	<b>20,73</b>
13.–14.	Václav	Rozhoň	3	GJirsíkaČB	3 3 – 5 4 4 – –	19	<b>20,63</b>
13.–14.	Vojtěch	Suchánek	3	GJarošeBO	3 1 3 5 3 5 – 1	19	<b>20,63</b>
15.	Jan	Soukup	3	G Klatovy	3 3 3 5 5 4 5 –	22	<b>20,50</b>
16.	Katarína	Krajčiová	3	GAlejKošic	3 3 – 5 5 5 – –	21	<b>20,18</b>
17.	Matěj	Konečný	3	G Jírov ČB	3 3 2 5 3 4 5 1	20	<b>20,17</b>
18.	Jakub	Löwit	2	GČeskoliPH	3 3 3 5 3 4 2 –	18	<b>19,87</b>
19.	Miroslav	Psota	4	GHlinŽilina	3 – – 5 4 4 5 –	21	<b>19,65</b>
20.	Karolína	Kuchyňová	3	GMLerchaBO	3 3 3 5 5 – – –	19	<b>19,28</b>
21.	Jan	Šorm	2	GJarošeBO	3 3 3 5 3 – – –	17	<b>19,17</b>
22.	Daniel	Pišťák	2	GZborovPH	3 2 2 5 1 5 3 –	18	<b>19,12</b>
23.	Antonín	Češík	4	SPŠElek PA	3 3 3 5 2 4 5 –	20	<b>18,84</b>
24.	Václav	Steinlhauser	0	ZŠVranéNVI	3 3 1 5 1 – – –	13	<b>18,66</b>
25.–26.	Vojtěch	Lukeš	2	G LPika PL	3 3 3 – 3 – 3 –	15	<b>18,59</b>
25.–26.	Minh Thao	Nguyen	2	GEbenešeKL	3 – 1 5 2 4 – –	15	<b>18,59</b>
27.	Tereza	Kislingerová	1	G Klatovy	3 3 3 – 2 – 2 –	13	<b>18,52</b>
28.	Jan	Alfery	2	GNPražačPH	2 1 3 5 – 4 – –	15	<b>18,39</b>
29.	Miroslav	Stankovič	4	GPošKošice	3 – – 5 4 4 5 –	21	<b>18,24</b>
30.	Marian	Poljak	2	GJŠkodyPŘ	3 – – 5 2 3 1 –	14	<b>17,77</b>
31.	Mikuláš	Zindulka	3	GMikul23PL	3 3 – 5 2 – 2 –	15	<b>17,27</b>
32.	Miroslav	Krabec	4	G KomHavíř	3 3 3 5 – – 5 –	19	<b>17,26</b>
33.	Marko	Puza	4	GPošKošice	3 – – 5 4 3 5 –	20	<b>17,06</b>
34.	Martin	Kopřiva	2	GMikul23PL	2 0 3 5 3 – – –	13	<b>16,79</b>
35.	Zuzana	Svobodová	2	G FrýdlNOs	3 3 3 5 – – – –	14	<b>16,69</b>
36.	Jan	Krejčí	4	G Bílovec	3 2 2 5 3 – 5 –	18	<b>16,50</b>
37.	Michael	Bucha	3	G Zábřeh	3 3 2 1 – 3 3 0	14	<b>16,36</b>
38.	Marián	Poppr	3	GJNerudyPH	3 3 – 5 – 4 2 –	17	<b>15,79</b>
39.	Markéta	Calábková	3	GJŠkodyPŘ	3 3 2 5 – 2 2 –	15	<b>15,73</b>



40.	Jaromír	Mielec	1	GVolgogrOS	3 - 3 5 1 - - -	12	<b>15,64</b>
41.	Vojtěch	Lanz	0	GZborovPH	3 - - - 2 3 - -	8	<b>15,39</b>
42.	Minh Tri	Pham	2	NPorg	3 3 1 2 - - 2 -	11 + <i>i</i>	<b>14,82</b>
43.	Jan	Kadlec	3	G Klatovy	3 3 - 5 3 2 - -	16	<b>14,52</b>
44.-45.	Jakub	Sláma	3	G OpatovPH	3 - 3 1 4 1 - -	12	<b>14,47</b>
44.-45.	Martin	Špilar	3	G Vyškov	3 2 2 1 2 - 3 1	12	<b>14,47</b>
46.	Markéta	Horová	2	GMikul23PL	3 - - 5 2 - - -	10	<b>14,05</b>
47.	Anh Dung	Le	4	G Tachov	- - - 5 4 5 0 5	19	<b>13,62</b>
48.	Vít	Kalisz	2	FSG Pirna	3 2 0 2 2 - - -	9 + <i>i</i>	<b>13,29</b>
49.	Dominik	Krasula	1	G Krnov	3 - 1 1 3 1 - -	9	<b>13,28</b>
50.	Anh	Le Hoang	2	GJarošeBO	3 2 1 2 1 - 1 0	9	<b>13,00</b>
51.	Jiří	Zeman	4	GLesníZlín	3 3 - 5 3 - - -	14	<b>12,49</b>
52.	Jakub	Dargaj	4	G PošKošice	3 3 3 5 2 - - -	16	<b>12,45</b>
53.	Petr	Lukeš	4	G NeumannŽR	3 3 - - 2 4 2 -	14	<b>12,04</b>
54.	Michaela	Brabcová	2	G Jírov ČB	3 3 1 - 1 - 0 -	8	<b>11,89</b>
55.	Tomáš	Fiala	3	GLEdečNSáz	3 3 1 0 3 - - -	10	<b>11,79</b>
56.	Petr	Jakubčík	0	PORG PH	3 - - - 2 - - -	5	<b>11,66</b>
57.-58.	Lukáš	Honsa	2	G Jírov ČB	3 3 1 - - - - -	7	<b>10,72</b>
57.-58.	Jan	Václavek	2	G Ústí n O	3 - 1 1 1 - 1 1	7	<b>10,72</b>
59.-60.	Jiří	Čech	3	G Strakon	3 - - 5 - - - -	8	<b>10,30</b>
59.-60.	Vít	Fojtik	3	G ÚstavníPH	3 - 2 1 - - 1 1	8	<b>10,30</b>
61.	Kateřina	Nová	1	G Vimperk	3 - - - 2 - - -	5	<b>10,00</b>
62.	Anna	Steinhauserová	4	G Dačice	3 2 2 5 2 1 - -	14	<b>9,66</b>
63.	Jakub	Hlédík	3	GSŘMRSkuteč	3 - 2 1 2 - - -	8	<b>9,43</b>
64.	Zuzana	Vlasáková	4	G Rumburk	3 3 3 2 - - - -	11	<b>9,28</b>
65.	Lukáš	Kubacki	1	GNadKavaPH	3 - - 1 - - - -	4	<b>8,48</b>
66.-67.	Jaroslav	Stránský	2	G Tišnov	3 - 1 - 1 - - -	5	<b>8,17</b>
66.-67.	Daniela	Šindelářová	2	GaSOŠ Telč	3 - - - 2 - - -	5	<b>8,17</b>
68.-70.	Markéta	Ospálková	1	G Uničov	3 - - - - - - -	3	<b>6,79</b>
68.-70.	David	Ucháč	1	VOŠDoprPH	3 - 0 - - - - -	3	<b>6,79</b>
68.-70.	Marie	Vonzino	1	GTomkovaOL	3 - - - - - - -	3	<b>6,79</b>
71.-73.	Tomáš	Kuzma	2	GAB Senec	3 - 0 - 1 - - -	4	<b>6,76</b>
71.-73.	Anežka	Michálková	2	GaSOŠ Telč	3 - 1 - 0 - - -	4	<b>6,76</b>
71.-73.	Štefan	Račák	2	GTajBanBys	3 1 0 - 0 - 0 -	4	<b>6,76</b>
74.	Adam	Gáli	4	G OlivuPopr	3 1 0 0 1 0 1 0	6	<b>6,00</b>
75.-76.	Tereza	Koberová	3	G Chrudim	3 - - - 1 - - -	4	<b>5,53</b>
75.-76.	Jiří	Štrincl	3	GS RandyJN	3 - - - 1 - - -	4	<b>5,53</b>
77.-84.	Daniel	Backov	2	G Ružomb	3 - - - - - - -	3	<b>5,27</b>
77.-84.	Jiřina	Duspívová	2	G Kralupy	3 - - - - - - -	3	<b>5,27</b>
77.-84.	Patricie	Klosse	2	G ČKrumlov	3 - - - - - - -	3	<b>5,27</b>
77.-84.	Kryštof	Kolář	2	GJarošeBO	3 - - - - - - -	3	<b>5,27</b>
77.-84.	Andrea	Mučerová	2	G ČKrumlov	3 - - - - - - -	3	<b>5,27</b>
77.-84.	Jakub	Marták	2	G GolNitra	- - 0 0 1 2 - -	3	<b>5,27</b>
77.-84.	Adam	Říha	2	G ČesLípa	3 - - - - - - -	3	<b>5,27</b>
77.-84.	Pavel	Souček	2	G Nymburk	3 - - - - - - -	3	<b>5,27</b>
85.-87.	Michaela	Biová	3	MendelG OP	3 - - 0 - - - -	3	<b>4,23</b>
85.-87.	Emese	Szabó	3	GZKMJ Gal	3 - - - - - - -	3	<b>4,23</b>
85.-87.	Kristýna	Šmidová	4	GMensaPH	2 3 - - - - - -	5	<b>4,23</b>
88.	Tomáš	Flaschka	2	G Hlučín	2 - - - - - - -	2	<b>3,65</b>
89.	Kristýna	Šudomová	2	GValašKlob	2 - - - - 0 - -	2	<b>3,30</b>
90.	Marek	Vícha	3	MendelG OP	2 - - - - - - -	2	<b>2,88</b>

<b>91.</b>	<i>Kristýna</i>	<i>Ilievová</i>	3	G Milevsko	3	-----	0	3	<b>2,87</b>
<b>92.</b>	<i>Otto</i>	<i>Hollmann</i>	4	GUBalvanJN	2	-----		2	<b>2,00</b>
<b>93.-94.</b>	<i>Petr</i>	<i>Gintar</i>	3	MendelG OP		-----	0	0	<b>0,00</b>
<b>93.-94.</b>	<i>Tomáš</i>	<i>Velich</i>	2	GJHroncaBA	0	0	-----	0	<b>0,00</b>

# 1. seriálová série – Teorie čísel

VÝSLEDKOVÁ LISTINA

1.–10.	Eduard	Batmendijn	3	CGStLubovňa	5 5 5	15	<b>15,00</b>
1.–10.	Filip	Bialas	1	GOpatoVPH	5 5 5	15	<b>15,00</b>
1.–10.	František	Couf	1	GZborovPH	5 5 5	15 + <i>i</i>	<b>15,00</b>
1.–10.	Martin	Hora	4	GMikul23PL	5 5 5	15 + <i>i</i>	<b>15,00</b>
1.–10.	Matěj	Konečný	3	G Jírov ČB	5 5 5	15	<b>15,00</b>
1.–10.	Anh Dung	Le	4	G Tachov	5 5 5	15	<b>15,00</b>
1.–10.	Martin	Raszyk	4	G Karviná	5 5 5	15 + <i>i</i>	<b>15,00</b>
1.–10.	Jan	Soukup	3	G Klatovy	5 5 5	15 + <i>i</i>	<b>15,00</b>
1.–10.	Radovan	Švarc	3	G ČTřebová	5 5 5	15	<b>15,00</b>
1.–10.	Pavel	Turek	1	GTomkovaOL	5 5 5	15	<b>15,00</b>
11.	Jakub	Löwit	2	GČeskolíPH	5 5 4	14	<b>14,32</b>
12.	Jakub	Svoboda	4	G KomHavíř	4 5 5	14	<b>13,57</b>
13.	Ondrej	Bínovský	3	GAnMeTr	5 5 –	10 + <i>i</i>	<b>11,46</b>
14.	Jan	Jurka	3	GMLerchaBO	5 – 5	10 + <i>i</i>	<b>11,39</b>
15.	Lukáš	Sadlek	3	G Čadca	3 4 2	9	<b>10,36</b>
16.	Martin	Kopřiva	2	GMikul23PL	5 3 –	8	<b>10,25</b>
17.	Markéta	Horová	2	GMikul23PL	4 3 –	7 + <i>i</i>	<b>9,66</b>
18.	Jan	Šorm	2	GJarošeBO	5 3 –	8	<b>9,58</b>
19.	Václav	Steinhauser	0	ZŠVranéNVI	2 3 –	5	<b>8,61</b>
20.	Anh	Le Hoang	2	GJarošeBO	1 2 3	6	<b>8,43</b>
21.	Miroslav	Stankovič	4	GPošKošice	5 – 5	10 + <i>i</i>	<b>7,94</b>
22.	Mikuláš	Zindulka	3	GMikul23PL	3 3 –	6	<b>7,47</b>
23.	Jan	Krejčí	4	G Bílovec	– 3 5	8	<b>6,95</b>
24.	Marko	Puza	4	GPošKošice	1 3 5	9	<b>6,72</b>
25.	Václav	Rozhoň	3	GJirsíkaČB	5 – –	5 + <i>i</i>	<b>6,69</b>
26.	Markéta	Calábková	3	GJŠkodyPŘ	5 – –	5 + <i>i</i>	<b>5,70</b>
27.	Karolína	Kuchyňová	3	GMLerchaBO	5 – –	5 + <i>i</i>	<b>5,49</b>
28.	Marián	Poppr	3	GJNerudyPH	5 0 1	6	<b>5,25</b>
29.	Petr	Lukeš	4	GNeumannŽR	1 – 5	6	<b>4,91</b>
30.	Antonín	Češík	4	SPŠElek PA	5 – –	5 + <i>i</i>	<b>4,39</b>
31.	Katarína	Krajčiová	3	GAlejKošic	5 – –	5	<b>4,28</b>
32.	Jan	Kadlec	3	G Klatovy	1 2 2	5	<b>4,20</b>
33.–34.	Dominik	Krasula	1	G Krnov	1 – 1	2	<b>3,60</b>
33.–34.	Daniel	Pišťák	2	GZborovPH	1 – 2	3	<b>3,60</b>
35.–36.	Minh Thao	Nguyen	2	GEBenešKL	2 – –	2	<b>3,47</b>
35.–36.	Jan	Václavek	2	G Ústí n O	0 2 –	2	<b>3,47</b>
37.	Jakub	Dargaj	4	GPošKošice	1 4 –	5	<b>3,26</b>
38.	Miroslav	Psota	4	GHlinŽilina	– 4 –	4	<b>3,04</b>
39.	Anna	Steinhauserová	4	G Dačice	2 3 –	5	<b>2,95</b>

40.–41.	Lukáš	Kubacki	1	GNadKavaPH	1	–	–	1	<b>2,51</b>
40.–41.	Kateřina	Nová	1	G Vimperk	1	–	–	1	<b>2,51</b>
42.	Anežka	Michálková	2	GaSOŠ Telč	1	–	–	1	<b>1,85</b>
43.	Jaromír	Mielec	1	GVolgogrOS	1	–	–	1	<b>1,74</b>
44.	Zuzana	Svobodová	2	G FrýdlNOs	1	–	–	1	<b>1,53</b>
45.	Jakub	Sláma	3	GOpatoVPH	1	–	–	1	<b>1,45</b>
46.	Tomáš	Fiala	3	GLedečNSáz	1	–	–	1	<b>1,31</b>
47.	Jakub	Hledík	3	GSŘMRSkuteč	1	–	–	1	<b>1,27</b>
48.–53.	Petr	Gintar	3	MendelG OP	0	–	–	0	<b>0,00</b>
48.–53.	Petr	Jakubčík	0	PORG PH	–	0	–	0	<b>0,00</b>
48.–53.	Jakub	Marták	2	G GolNitra	0	0	–	0	<b>0,00</b>
48.–53.	Jozef	Mišť	2	GAHŠ VKrtiš	0	–	–	0	<b>0,00</b>
48.–53.	Markéta	Ospálková	1	G Uničov	0	–	0	0	<b>0,00</b>
48.–53.	Kristýna	Šudomová	2	GValašKlob	0	–	–	0	<b>0,00</b>

## Pořadí po 3. podzimní sérii

1.	František	Couf	1	GZborovPH	25 25 25 15	<b>89,62</b>	325
2.	Radovan	Švarc	3	G ČTřebová	25 23 25 15	<b>88,02</b>	792
3.	Martin	Hora	4	GMikul23PL	25 23 25 15	<b>87,77</b>	659
4.	Filip	Bialas	1	G OpatovPH	25 24 23 15	<b>86,80</b>	87
5.	Pavel	Turek	1	G TomkovaOL	24 22 25 15	<b>85,49</b>	215
6.	Jakub	Svoboda	4	G KomHavíř	22 24 21 14	<b>80,51</b>	293
7.	Eduard	Batmendijn	3	CGStLubovňa	25 18 21 15	<b>79,18</b>	104
8.	Jakub	Löwit	2	GČeskoliPH	23 21 20 14	<b>78,57</b>	296
9.	Martin	Raszyk	4	G Karviná	16 25 23 15	<b>78,11</b>	701
10.	Jan	Soukup	3	G Klatovy	22 19 21 15	<b>76,56</b>	587
11.	Václav	Rozhoň	3	G JirsíkaČB	25 21 21 7	<b>73,73</b>	74
12.	Anh Dung	Le	4	G Tachov	22 22 14 15	<b>73,28</b>	1016
13.	Václav	Steinhauser	0	ZŠVranéNVI	23 23 19 9	<b>73,25</b>	170
14.	Miroslav	Stankovič	4	G PošKošice	22 25 18 8	<b>72,98</b>	523
15.	Katarína	Krajčiová	3	GAlejKošic	25 21 20 4	<b>70,81</b>	402
16.	Lukáš	Sadlek	3	G Čadca	18 20 21 10	<b>69,75</b>	70
17.	Martin	Surma	3	G JWolkraPV	23 22 23 -	<b>68,37</b>	175
18.	Martin	Kopřiva	2	GMikul23PL	21 19 17 10	<b>67,77</b>	87
19.	Ondřej	Darmovzal	3	G JarošeBO	23 21 23 -	<b>67,42</b>	67
20.	Markéta	Horová	2	GMikul23PL	22 22 14 10	<b>66,75</b>	67
21.	Mikuláš	Zindulka	3	GMikul23PL	21 21 17 7	<b>66,58</b>	67
22.	Marko	Puza	4	G PošKošice	23 20 17 7	<b>66,46</b>	480
23.	Karolína	Kuchyňová	3	G MLerchaBO	23 18 19 5	<b>66,45</b>	266
24.	Jan	Šorm	2	G JarošeBO	17 21 19 10	<b>66,09</b>	261
25.	Matěj	Konečný	3	G Jírov ČB	14 16 20 15	<b>65,69</b>	274
26.	Vojtěch	Suchánek	3	G JarošeBO	20 24 21 -	<b>64,09</b>	64
27.	Antonín	Češík	4	SPŠElek PA	20 20 19 4	<b>63,57</b>	196
28.	Miroslav	Psota	4	GHlinŽilina	21 19 20 3	<b>63,02</b>	256
29.	Jan	Jurka	3	G MLerchaBO	13 15 21 11	<b>61,10</b>	79
30.	Minh Thao	Nguyen	2	GEbenešKL	17 22 19 3	<b>60,48</b>	60
31.	Tereza	Kislingerová	1	G Klatovy	18 22 19 -	<b>58,65</b>	59
32.	Marián	Poppr	3	G JNerudyPH	14 23 16 5	<b>57,30</b>	382
33.	Marian	Poljak	2	G JŠkodyPŘ	17 22 18 -	<b>56,19</b>	56
34.	Zuzana	Svobodová	2	G FrýdlNOs	18 18 17 2	<b>55,08</b>	233
35.	Jan	Krejčí	4	G Bílovec	21 10 17 7	<b>54,89</b>	196
36.	Martin	Špilar	3	G Vyškov	22 17 14 -	<b>53,91</b>	54
37.	Anh	Le Hoang	2	G JarošeBO	11 20 13 8	<b>52,27</b>	52
38.	Vojtěch	Lanz	0	G ZborovPH	19 17 15 -	<b>51,77</b>	52
39.	Jakub	Dargaj	4	G PošKošice	19 17 12 3	<b>51,54</b>	438
40.	Anna	Steinhauserová	4	G Dačice	21 17 10 3	<b>50,35</b>	542

41.	Miroslav	Krabec	4	G KomHavíř	16 17 17	–	<b>50,32</b>	238	
42.	Daniel	Pišťák	2	GZborovPH	8 17 19	4	<b>48,25</b>	387	
43.	Minh Tri	Pham	2	NPorg	17 16 15	–	<b>47,68</b>	121	
44.	Dominik	Krasula	1	G Krnov	15 14 13	4	<b>46,53</b>	233	
45.	Petr	Jakubčík	0	PORG PH	18 16 12	0	<b>46,31</b>	46	
46.	Jan	Kadlec	3	G Klatovy	18 9 15	4	<b>46,00</b>	392	
47.	Vojtěch	Lukeš	2	G LPika PL	13 14 19	–	<b>45,64</b>	46	
48.	Kateřina	Nová	1	G Vimperk	19 14 10	3	<b>45,60</b>	46	
49.	Tomáš	Fiala	3	GLedečNSáz	19 13 12	1	<b>45,06</b>	122	
50.	Petr	Lukeš	4	GNeumannŽR	10 17 12	5	<b>44,45</b>	208	
51.	Jan	Václavek	2	G Ústí n O	13 17 11	3	<b>44,09</b>	44	
52.	Jakub	Sláma	3	GOpátovPH	12 14 14	1	<b>42,84</b>	43	
53.	Vít	Kalisz	2	FSG Pirna	12 17 13	–	<b>42,08</b>	42	
54.	Daniela	Šindelářová	2	GaSOŠ Telč	21 13 8	–	<b>42,01</b>	42	
55.	Michaela	Brabcová	2	G Jírov ČB	16 14 12	–	<b>41,94</b>	42	
56.	Kristýna	Šmídová	4	GMensaPH	18 19 4	–	<b>41,68</b>	136	
57.	Andrea	Kučerová	2	G ČKrumlov	19 17 5	–	<b>41,54</b>	42	
58.	Jaromír	Mielec	1	GVolgogrOS	6 17 16	2	<b>40,39</b>	321	
59.	Markéta	Calábková	3	GJŠkodyPŘ	12 7 16	6	<b>39,77</b>	213	
60.	Jakub	Šebek	4	GKepleraPH	21 18	–	<b>38,87</b>	98	
61.	Patricie	Klosse	2	G ČKrumlov	16 17 5	–	<b>38,17</b>	38	
62.	Michael	Bucha	3	G Zábřeh	10 11 16	–	<b>38,05</b>	38	
63.	Tomáš	Kuzma	2	GAB Senec	13 18 7	–	<b>37,53</b>	38	
64.	Jiří	Česka	1	CMGProstěj	19 17	–	<b>35,35</b>	35	
65.	Jiřina	Duspívová	2	G Kralupy	11 17 5	–	<b>32,89</b>	33	
66.	Jakub	Hledík	3	GSŘMRSkuteč	17 4 9	1	<b>31,84</b>	134	
67.	Mihály	Kotiers	2	GHSelyhoKM	13 18	–	<b>30,77</b>	31	
68.	Jiří	Zeman	4	GLesníZlín	– 18 12	–	<b>30,01</b>	147	
69.	Lukáš	Kubacki	1	GNadKavaPH	11 7 8	3	<b>29,16</b>	29	
70.	Lenka	Kopfová	0	CZSSL HnM	16 13	–	<b>29,10</b>	29	
71.	Lukáš	Honsa	2	G Jírov ČB	9 8 11	–	<b>28,37</b>	28	
72.	Štefan	Račák	2	GTajBanBys	18 4 7	–	<b>28,18</b>	28	
73.	Viktor	Němeček	3	GJMasar JI	19 9	–	<b>28,11</b>	338	
74.	Michaela	Brezinová	2	GKomTřebiš	12 16	–	<b>27,89</b>	28	
75.	Jan	Alfery	2	GNPražacPH	9	– 18	–	<b>27,63</b>	64
76.	Barbora	Hudcová	4	PORG PH	10 17	–	–	<b>27,31</b>	92
77.	Anežka	Michálková	2	GaSOŠ Telč	19	– 7	2	<b>27,20</b>	27
78.	Marek	Vícha	3	MendelG OP	11 12	3	–	<b>26,72</b>	27
79.	Zuzana	Vlasáková	4	G Rumburk	4 12 9	–	<b>25,45</b>	169	
80.	Marie	Vonzino	1	GTomkovaOL	16 3 7	–	<b>25,35</b>	25	
81.	Markéta	Ospálková	1	G Uničov	15 3 7	0	<b>24,35</b>	24	
82.	Jaroslav	Stránský	2	G Tišnov	11 5 8	–	<b>24,16</b>	24	
83.	Adam	Říha	2	G ČesLípa	12 7 5	–	<b>23,92</b>	24	
84.	Peter Kulcsár	Szabó	2	GHSelyhoKM	9 14	–	–	<b>23,53</b>	24
85.	David	Ucháč	1	VOŠDoprPH	14 3 7	–	<b>23,27</b>	23	
86.	Henrieta	Michelová	2	GAlejKošic	11 12	–	–	<b>22,94</b>	163
87.	Tereza	Koberová	3	G Chrudim	9 8 6	–	<b>22,70</b>	23	
88.	Emese	Szabó	3	GZKMJ Gal	13 4 4	–	<b>21,93</b>	22	
89.	Kristýna	Ilievová	3	G Milevsko	6 13 3	–	<b>21,35</b>	265	
90.	Daniel	Backov	2	G Ružomb	16 0 5	–	<b>21,27</b>	21	
91.	Kristýna	Šudomová	2	GValašKlob	14 3 3	0	<b>20,98</b>	120	

92.–93.	Jakub	Marták	2	G GolNitra	12	4	5	0	<b>20,81</b>	21
92.–93.	Tomáš	Flaschka	2	G Hlučín	12	5	4	–	<b>20,81</b>	21
94.	Michaela	Bielíková	4	G Sereď	11	9	–	–	<b>20,58</b>	161
95.	Přemysl	Šťastný	0	G Žamberk	14	6	–	–	<b>20,52</b>	21
96.	David	Peňáz	2	GNeumannŽR	12	8	–	–	<b>20,06</b>	20
97.	Victoria María	Nájares Romero	0	GZborovPH	20	–	–	–	<b>19,76</b>	20
98.	Vojtěch	Linhart	3	SlovanG OL	18	–	–	–	<b>18,15</b>	18
99.	Martin	Minasjan	4	GKepleraPH	18	–	–	–	<b>17,82</b>	135
100.	Jana	Vráblíková	2	GLesníZlín	14	4	–	–	<b>17,70</b>	18
101.	Jiří	ŠtrincI	3	GSRandyJN	11	0	6	–	<b>16,92</b>	17
102.	Martin	Konečný	2	GStrážnice	13	4	–	–	<b>16,65</b>	17
103.	Lucie	Roškotová	2	G Turnov	9	7	–	–	<b>16,24</b>	16
104.	Ludmila	Šimková	4	GPároNitra	5	10	–	–	<b>15,47</b>	78
105.	Tereza	Rašková	3	GTomkovaOL	15	0	–	–	<b>15,43</b>	15
106.	Otto	Hollmann	4	GUBalvanJN	7	6	2	–	<b>15,00</b>	15
107.	Pavel	Souček	2	G Nymburk	–	9	5	–	<b>14,75</b>	15
108.–109.	Radim	Bárta	3	GJarošeBO	14	–	–	–	<b>14,47</b>	14
108.–109.	Jan	Knížek	3	G Strakon	14	–	–	–	<b>14,47</b>	14
110.	Tran Vi Thanh	Pham	4	GNeumannŽR	7	7	–	–	<b>14,08</b>	150
111.–114.	Petr	Červenka	2	GNadKavaPH	14	–	–	–	<b>14,05</b>	14
111.–114.	Jozef	Mišť	2	GAHŠ VKrtiš	14	0	–	0	<b>14,05</b>	14
111.–114.	Jakub	Starý	2	VOŠKutHora	14	–	–	–	<b>14,05</b>	14
111.–114.	Jakub	Ševčík	2	GKukučPopr	14	–	–	–	<b>14,05</b>	14
115.	Adam	Gálik	4	GOlivuPopr	7	1	6	–	<b>14,00</b>	14
116.	Tomáš	Velich	2	GJHroncaBA	12	2	0	–	<b>13,80</b>	14
117.	Nicholas	Čapek	4	GBNěmcovHK	11	3	–	–	<b>13,78</b>	129
118.	Barbora	Pešlová	3	G Vimperk	13	–	–	–	<b>13,41</b>	131
119.–121.	Matyáš	Medek	4	G MozartovaPA	13	–	–	–	<b>13,00</b>	13
119.–121.	Jakub	Šinko	2	GNadKavaPH	13	–	–	–	<b>13,00</b>	13
119.–121.	Lukáš	Zib	2	GPisnickPH	13	–	–	–	<b>13,00</b>	13
122.–123.	Jakub Josef	Slavík	1	BiskG Brno	13	–	–	–	<b>12,64</b>	13
122.–123.	Jáchym	Solecký	1	PORG PH	13	0	–	–	<b>12,64</b>	13
124.	Martin	Šourek	3	GCoubTábor	12	–	–	–	<b>12,45</b>	12
125.–126.	Jakub	Hrubý	2	G Chrudim	12	0	–	–	<b>11,89</b>	12
125.–126.	Martin	Kutiš	2	G Humpolec	12	–	–	–	<b>11,89</b>	12
127.	Adéla	Šedová	2	GJungmanLT	8	4	–	–	<b>11,82</b>	12
128.	Pavčina	Hartmanová	2	G Broumov	12	–	–	–	<b>11,76</b>	30
129.	Vojtěch	Juříček	2	G Kralupy	12	–	–	–	<b>11,70</b>	39
130.	Borek	Požár	0	G Rakovník	12	–	–	–	<b>11,66</b>	12
131.	Ondrej	Bínovský	3	GAnMeTr	–	–	–	11	<b>11,46</b>	11
132.–133.	Tomáš	Beneš	2	GVráLevice	9	2	–	–	<b>11,39</b>	11
132.–133.	Martin	Chabada	2	G Bardejov	9	2	–	–	<b>11,39</b>	11
134.	Zuzana	Trégllová	1	G Žatec	11	–	–	–	<b>11,38</b>	11
135.	Michaela	Biová	3	MendelG OP	7	–	4	–	<b>11,02</b>	11
136.	Veronika	Holubová	3	PORG PH	8	3	–	–	<b>10,88</b>	11
137.–138.	Petra	Kratochvílová	2	GHustopeče	11	–	–	–	<b>10,72</b>	11
137.–138.	Daniel	Krejbych	2	G Litomyšl	11	–	–	–	<b>10,72</b>	11
139.	Kryštof	Kolář	2	GJarošeBO	5	–	5	–	<b>10,54</b>	11
140.–142.	Jiří	Čech	3	G Strakon	–	–	10	–	<b>10,30</b>	10
140.–142.	Vít	Fojtík	3	GÚstavníPH	–	–	10	–	<b>10,30</b>	10
140.–142.	Marek	Štěpán	3	SPŠE Fren	10	–	–	–	<b>10,30</b>	10

143.–147.	Dominik	Hodan	1	GNadAlejPH	10	–	–	–	<b>10,00</b>	10
143.–147.	Věra	Tesařová	1	MasG Plzeň	10	0	–	–	<b>10,00</b>	10
143.–147.	The Minh	Tran	1	PČGKarVary	10	–	–	–	<b>10,00</b>	10
143.–147.	Tomáš	Valovič	4	GAHŠ VKrtíš	8	2	–	–	<b>10,00</b>	10
143.–147.	Kateřina	Volková	1	MG Vsetín	10	–	–	–	<b>10,00</b>	10
148.	Jan	Erhart	3	GFXŠaldyLI	9	–	–	–	<b>9,45</b>	203
149.–153.	Cedrik	Horčíčka	3	G ČesLípa	9	–	–	–	<b>9,17</b>	9
149.–153.	Denisa	Kolenčíková	3	GNámostovo	9	–	–	–	<b>9,17</b>	9
149.–153.	Jan	Kříža	3	GVPavlovic	9	–	–	–	<b>9,17</b>	9
149.–153.	Tomáš	Vaniček	3	G Jírov ČB	9	–	–	–	<b>9,17</b>	9
149.–153.	Peter	Vook	3	GPOšKošice	9	–	–	–	<b>9,17</b>	9
154.	Daniel	Kočik	4	GŠroKošice	9	–	–	–	<b>9,00</b>	9
155.	Hana	Daňková	1	G Vimperk	–	8	–	–	<b>8,48</b>	8
156.	Jan	Lukáč	3	G ČKrumlov	4	4	–	–	<b>8,46</b>	8
157.	Lenka	Vincenová	0	GTomkovaOL	8	–	–	–	<b>8,34</b>	8
158.–160.	Katarína	Behinská	2	G GolNitra	8	0	–	–	<b>8,17</b>	8
158.–160.	Matěj	Kosma	2	SOŠDoprOS	8	0	–	–	<b>8,17</b>	8
158.–160.	Dennis	Ryšánek	2	SPŠÚžlabPH	8	–	–	–	<b>8,17</b>	8
161.–163.	Antonie	Brožová	4		8	–	–	–	<b>8,00</b>	8
161.–163.	Jakub	Kříž	4	SPŠ PB	8	–	–	–	<b>8,00</b>	8
161.–163.	Matěj	Sháněl	4	G VysMýto	8	–	–	–	<b>8,00</b>	8
164.	Vendula	Kotyzová	4	WichtG OS	8	–	–	–	<b>7,76</b>	113
165.	Ivona	Hřivová	4	GOKrŽilina	7	–	–	–	<b>7,38</b>	157
166.	Marie	Koutná	4	GTNovákBO	7	–	–	–	<b>7,00</b>	7
167.–170.	Levente	Berky	3	GZKMJ Gal	7	–	–	–	<b>6,79</b>	7
167.–170.	Kristýna	Davídková	1	OA Liberec	7	–	–	–	<b>6,79</b>	7
167.–170.	Anna	Filipová	3	G Kolín	7	–	–	–	<b>6,79</b>	7
167.–170.	Jana	Menšíková	1	G Frýdlant	7	–	–	–	<b>6,79</b>	7
171.–173.	Alena	Košáková	2	G Strakon	7	0	–	–	<b>6,76</b>	7
171.–173.	Ronald	Luc	2	GJarošeBO	7	–	–	–	<b>6,76</b>	7
171.–173.	Šimon	Tabačko	2	EvG Košice	–	7	–	–	<b>6,76</b>	7
174.	Tomáš	Konečný	1	GJirsíkaČB	6	–	–	–	<b>5,75</b>	143
175.–177.	Stanislav	Kruml	3	G Chotěboř	6	0	–	–	<b>5,53</b>	6
175.–177.	Barbora	Kubicová	3	PORG PH	6	–	–	–	<b>5,53</b>	6
175.–177.	Vít	Maroščík	3	G Bohumín	6	–	–	–	<b>5,53</b>	6
178.	Valentína	Straková	4	G Sereď	5	–	–	–	<b>5,36</b>	68
179.–181.	Matej	Kašťák	2	G Hlohovec	5	–	–	–	<b>5,27</b>	5
179.–181.	Marina	Pogarčenko	2	GJungmanLT	5	0	–	–	<b>5,27</b>	5
179.–181.	Tomáš	Šácha	2	SPŠEB Břeclav	–	5	–	–	<b>5,27</b>	5
182.–194.	Nevešli se.									

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](mailto:mks@mff.cuni.cz)