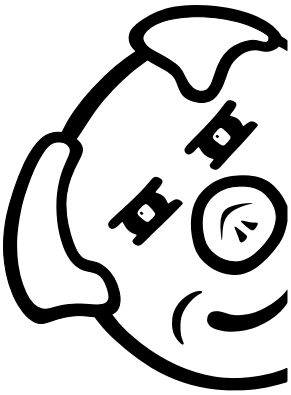
Matematický korespondenční seminář

Milý příteli!



Vánoční oslavy už jsou sice za námi, ale s novým rokem Ti posíláme trochu opožděný Vánoční dáreček v podobě komentářů! Nadílka pro naše šikovná PraSátka je bohatá, najdeš tady totiž hromadu věcí.

Ve 2. podzimní sérii jsme se prokousávali úložkami na téma **Prostory a roviny** a ve 3. podzimní sérii jsme se zabývali **Opakováním**. Kromě vzorových řešení k těmto sériím tady najdeš také vzorová řešení úloh z první seriálové série. Jak se Ti s řešením dařilo najdeš v průběžné výsledkovce na konci komentářů.

Už víš, jak správně vyřešit každý příklad z podzimních sérií? Tak to je štěstí, že Ti níže posíláme zbrusu nové zadání! Mrkni se na 1. jarní sérii o **Mocnění** nebo si pročti druhý díl seriálu **Polynomy 2 – Malé a velké věci nad** $\mathbb{Z}$ a s radostí se vrhni do řešení.

Podzimní sezóna se pomalu chýlí ke konci, nezapomeň proto na to, jak dobře se PraSátka mají na jaře. Můžou si zasoutěžit na zábavné soutěži jménem **Náboj** a hned další den si provětrat hlavu na PraSečím **jarním výletě**. Více informací k těmto akcím najdeš níže, moc rádi Tě tam a nebo jinde potkáme!

Do nového roku Ti přejeme všechno nejkrásnější a s tím i plno dobrých nápadů a kopu zábavy při řešení!

Za organizátory,

Lenka Poljaková

Co je dále v komentářích?

Náboj

Na jaře se uskuteční mezinárodní týmová matematická soutěž Náboj. Proběhne v pátek 14. března, letos už celkem v 15 různých zemích. Podrobnosti najdeš na stránkách Náboje[1]. Je to skvělá příležitost k porovnání sil nejen s českou, ale i zahraniční elitou. Registrace začíná 10. února a končí 5. března, tak si tuto úžasnou příležitost určitě nenech ujít!

Jarní výlet

Nesmíme zapomenout ani na tradiční jarní výlet po krásách naší vlasti. Je to možnost, jak poznat organizátory PraSátka i další řešitele. Tradičně se bude konat den po Náboji, v sobotu 15. března v okolí Prahy. Více informací se brzy dozvíš na našich stránkách. Těšíme se na Tebe!

[1] *https://math.naboj.org/*

Matematický korespondenční seminář
KAM MFF UK
Malostranské náměstí 25
118 00 Praha 1

matfyz

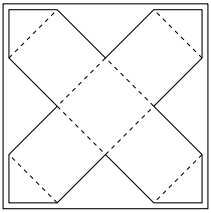
Prostory a roviny

2. podzimní série — Vzorové řešení

Úloha 1.

Ondra má papír ve tvaru čtverce o straně délky 3. Poraďte mu, jak z papíru vystřihnout souvislý útvar o obsahu 6, ze kterého pak bude moci složit krychli o hraně délky 1.

Řešení:
Pokud se pokusíme na papír dostat nějakou ze známých sítí sestávajících ze 6-ti čtverců, rychle zjistíme, že se Ondrovi na papír nevejde. Můžeme ale zachovat nějakou její část, v našem případě 5 čtverců, a poslední čtverec nějak šikovně rozdělit na více částí. Jeden příklad, jak může Ondra takový útvar vytvořit, je na obrázku.



Poznámky:
Někteří řešitelé se bohužel příliš upnuli na představu klasické sítě sestávající ze 6-ti čtverců, která se vskutku na Ondrův papír nevejde. Jiní řešitelé zvolili alternativní přístup, kdy papír rozdělili na 36 shodných čtverečků, ze kterých pak vytvořili méně či více divoký útvar, ze kterého lze krychli složit. *(Klárka Grinerová)*

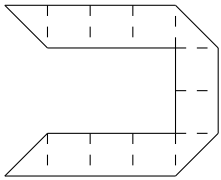
Úloha 2.

Alicka našla krychli o hraně délky 1 a obdélníkový proužek papíru 1×12*. Jak lze proužek obmotat kolem krychle tak, aby všechny její stěny byly v každém bodě pokryty dvěma vrstvami papíru? Proužek se smí přehýbat, ale ne stříhat.*

Řešení:
Jedno z možných řešení je níže. Nejprve si proužek rozdělíme na 12 čtverců, poté některé čtverce ohneme podél úhlopříčky (tím nám na nákresu vzniknou trojúhelníky) a nakonec každou čárkovanou hranu ohneme tak, aby spolu sousední stěny svíraly úhel 90°.

Rozmysleme si, že uvedené řešení skutečně splňuje zadání. Dvě spolu sousedící stěny krychle se pokryjí dvěma pravoúhlými trojúhelníky (které mají tloušťku dvou vrstev proužku). Z každé z těchto stěn pak vede úsek tří čtverců, který začíná v jednom z trojúhelníků dané stěny, obmotává se dokola kolem krychle a končí v druhém z trojúhelníků. Tyto dva úseky dohromady pokryjí další

dvě stěny krychle dvěma vrstvami proužku a zbylé dvě stěny jednou vrstvou. Tyto poslední dvě stěny jsou pak doobaleny úsekem dvou čtverců, který spojuje zmiňované stěny s trojúhelníky.



Poznámky:

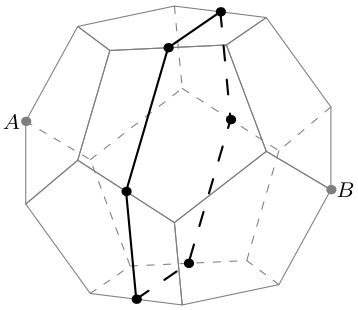
Uvedené řešení je cyklické, takže pokud bychom spolu spojili volné konce a přestřihli bychom libovolnou čárkovanou hranu, dostaneme rovněž validní řešení. *(Lukáš Trojan)*

Úloha 3.

Rozhodněte, zda existuje rovina, jejíž řez pravidelným dvanáctistěnem je pravidelný šestiúhelník.

Řešení:

Taková rovina existuje, jeden možný řez vypadá jako na obrázku, přičemž vrcholy šestiúhelníku leží vždy ve středu hrany dvanáctistěnu.



Protože dvanáctistěn je symetrický, je všech šest znázorněných vrcholů stejně vzdálených od vrcholů A a B – tedy znázorněné vrcholy skutečně leží v jedné rovině a jde o šestiúhelník. Protože strany šestiúhelníku tvoří stejně vytvořené úsečky ve stěnách pravidelného dvanáctistěnu, jsou stejně dlouhé. Tedy skutečně jde o pravidelný šestiúhelník.

Poznámky:

Většina řešitelů si s úlohou poradila a nějakým způsobem se jim podařilo řez zkonstruovat, v některých řešeních ale bohužel chybělo zdůvodnění, proč je zkonstruovaný řez skutečně pravidelným šestiúhelníkem. *(Jolana Štraitová)*

Úloha 4.

Planeta Čuník je dokonalá koule. Vědci z hlavního města Rypáček postavili supermoderní vesmírnou loď Ocásek s inovativním pohonem. Ocásek si každou vteřinu vybere nějakou přímku tečnou k Čuníku, na které se nachází, a popoletí po ní o libovolnou celočíselnou vzdálenost. Ocásek vyrazil na testovací misi, která začala v Rypáčku a skončila opět někde na povrchu Čuníka. Dokažte, že Ocásek na misi uletěl sudou celočíselnou vzdálenost.

Řešení:
Nechť je poloměr Čuníka roven r a nechť se Ocásek nachází právě ve vzdálenosti s od povrchu Čuníka. Nazvěme *tečnovou vzdáleností* vzdálenost Ocásku od bodu dotyku vybrané tečny k Čuníkovi. Ta je pak podle Pythagorovy věty vždy rovna $\sqrt{(r+s)^2 - r^2}$, takže její hodnota nezávisí na volbě tečny.

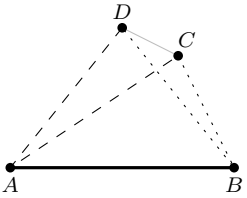
Jelikož se každé pohnutí Ocásku během jeho mise odehrává na nějaké tečně k Čuníkovi, vzdálenost uražená při daném pohnutí vždy odpovídá změně jeho tečnové vzdálenosti. Aby se přitom Ocásek mohl vrátit na povrch Čuníka (a jeho tečnová vzdálenost tedy byla rovna 0), musí se součet jeho nalétaných vzdáleností směrem od Čuníka rovnat součtu nalétaných vzdáleností směrem k Čuníkovi. Protože jsou oba tyto součty celočíselné, jejich součtem, tedy dvojnásobkem jednoho z nich, je sudé celé číslo, což jsme chtěli dokázat.

Poznámky:
S úlohou se dalo popasovat různými způsoby, ať už podobně jako ve vzoráku (kde se dívání na změny tečnové vzdálenosti dalo ekvivalentně převést na létání Ocásku po jedné tečně, čehož někteří řešitelé využili), nebo nějakým druhem zjednodušení trasy mise, dokazovalo se ale i indukcí. Mnoha řešitelům jsem bohužel musel strhávat body buď za opomenutí, nebo za nedostatečné okomentování klíčových kroků jejich řešení. *(Štěpán Varhaník)*

Úloha 5.

Rozhodněte, zda lze šest hran libovolného nedegenerovaného čtyřstěnu rozdělit na dvě trojice tak, aby z každé z nich šel poskládat nedegenerovaný trojúhelník.

Řešení:
Trojúhelník je nedegenerovaný, pokud pro něj platí všechny tři trojúhelníkové nerovnosti. Označme vrcholy čtyřstěnu $ABCD$ tak, že AB je jeho nejdelší hrana. Ukážeme, že lze vytvořit nedegenerovaný trojúhelník z hran AB, AC, AD nebo z hran AB, BC, BD.



Z trojúhelníkových nerovností pro trojúhelníky ABC a ABD víme, že

$$|AC| + |CB| > |AB|,$$
$$|AD| + |BD| > |AB|.$$

Sečtením získáme

$$|AC| + |CB| + |AD| + |BD| > 2 \cdot |AB|.$$

Z toho musí nutně platit $|AC| + |AD| > |AB|$ nebo $|BC| + |BD| > |AB|$, dále budeme předpokládat, že platí první možnost. Druhá možnost je symetrická.

Protože hrana AB je nejdelší, jsou zbylé dvě nerovnosti splněny triviálně, a tedy hrany AB, AC, AD tvoří nedegenerovaný trojúhelník. Druhý trojúhelník tvoří hrany BC, CD, BD, protože již tvoří jednu stěnu čtyřstěnu. Tímto jsme ukázali, že vždy umíme najít dvě trojice hran generující nedegenerovaný trojúhelník.

Poznámky:
Většina řešitelů použila řešení podobné tomu vzorovému, objevila se však i řešení, kde se rozebíraly možnosti umístění nejkratších či nejdelších hran, nebo řešení pomocí Heronova vzorce.

(Petr Hladík)

Úloha 6.

V PraSeploše stojí několik měst. Mezi každou dvojicí měst vede nanejvýš jedna silnice. Silnice se smí libovolně klikatit, ale nemohou se křížit (ani mimoúrovňově).[2] *Dokažte, že z nich lze udělat jednosměrné silnice tak, aby z každého města šlo vycestovat nanejvýš třemi silnicemi.*

Řešení:
Představme si PraSeplochu jako neorientovaný rovinný graf (města budou vrcholy a silnice hrany). Naší úlohou je pak zorientovat všechny hrany tak, aby z každého vrcholu vedly maximálně tři. Označme si E jako množinu hran a V jako množinu vrcholů. V řešení budeme používat známé tvrzení platící pro rovinné grafy, $|E| \leq 3|V| - 6$, které snadno vyplývá z Eulerovy věty[3]. Jako stupeň vrcholu v budeme označovat počet orientovaných hran, které vedou z v do jiného vrcholu.

Úlohu dokážeme algoritmicky. Zorientujme hrany v grafu náhodně. Mějme množinu M, ve které jsou všechny vrcholy, z nichž vedou alespoň 4 hrany. Budeme postupně snižovat součet stupňů vrcholů v M (bude to náš monovariant). Pokusíme se najít orientovanou cestu z vrcholu v M do vrcholu se stupněm nanejvýš 2. Pokud takovou cestu najdeme, stačí obrátit orientace všech jejích hran. Tím o 1 zvětšíme stupeň koncového vrcholu, o 1 zmenšíme stupeň počátečního a zbylé stupně zachováme.

Tvrdím, že existuje alespoň 1 hrana, která vede z M do zbytku grafu. Nechť pro spor taková hrana neexistuje. Podgraf rovinného grafu je jistě stále rovinný graf, tedy množina vrcholů M spolu s množinou hran, které z těchto vrcholů vedou, tvoří rovinný graf. Jelikož ale z každého vrcholu vedou alespoň 3 hrany (dokonce alespoň 4), platí: $|E_M| \geq 3|V_M|$, jenže podle tvrzení zmíněného výše musí zároveň platit $3|E_M| \leq 3|V_M| - 6$, čímž získáme spor. Tudíž existuje alespoň 1 hrana, která vede ven z množiny M.

Označme si N množinu všech vrcholů stupně 3 dosažitelných z M (tedy takových, do kterých vede cesta z vrcholů M). Uvědomme si, že pro množinu vrcholů $M \cup N$ rovněž platí nutnost existence hrany vedoucí z ní (odhad, který jsme použili, byl natolik slabý, že platí i po přidání vrcholů se stupněm 3). Na konci této hrany jistě bude vrchol v se stupněm maximálně dva (jinak by byl v množině M nebo N). Tudíž víme, že buď přímo z nějakého vrcholu z M vede hrana do v, nebo do něj vede hrana z nějakého vrcholu z N, ten je ovšem dosažitelný z nějakého vrcholu z M, takže získáme kýženou cestu.

Po jejím přeorientování se nám buď stupeň vrcholu z M sníží na 3, a tedy jej z M vyřadíme, nebo bude stále větší než 3 a v M zůstane, ale součet stupňů v M o 1 klesne.

Jelikož jsme cestu našli pro libovolnou neprázdnou množinu M, můžeme takto pokračovat až do chvíle, kdy nějaká M existuje, zároveň jelikož součet stupňů vrcholů v M stále klesá, algoritmus skončí a graf po jeho skončení splňuje požadavek ze zadání.

Skutečně tedy lze takové jednosměrné silnice udělat.

---

[2] Formálně řečeno tedy města a silnice představují *nakreslení rovinného grafu*. O rovinných grafech se lze více dozvědět v seriálu Letem grafovým světem zde: *https://prase.cz/archive/34/serial.pdf*.

[3] Pokud toto tvrzení neznáš, podívej se do výše zmíněného seriálu.

Poznámky:

Pokud máme nějaký maximální rovinný graf, tak nejsme nutně schopni vytvořit každý možný rovinný graf pouze odebíráním hran. Například vždy jsme schopni udělat maximální rovinný graf, kde každý vrchol má stupeň maximálně 3 a z něj triviálně nejsme schopni udělat žádný graf s vrcholem stupně víc než 3 pouze odebíráním hran. *(Áďa Žáčková a Lukáš Trojan)*

Úloha 7.

V prostoru je dán konvexní mnohostěn M a uvnitř něj bod P, kterým prochází několik (alespoň jedna) přímek $\ell_1, \ldots, \ell_n$. Význačnou přímkou stěny mnohostěnu M nazveme tu z přímek $\ell_1, \ldots, \ell_n$, která s její rovinou svírá největší úhel. Svírá-li více přímek tentýž největší úhel, volíme za význačnou libovolnou z nich. Dokažte, že existuje stěna mnohostěnu M, která je protnuta svou význačnou přímkou.

Řešení:

Všimneme si, že máme-li dva body A, B na rovině H a nějaký bod P mimo rovinu H a $|AP| < |BP|$, pak AP svírá větší úhel s H než BP. Průsečík stěny, popřípadě roviny, na níž stěna leží, s její význačnou přímkou nazveme *význačný bod* dané stěny. Ukážeme, že nejbližší význačný bod k bodu P leží na stěně, ke které je význačný. Daný bod si nazveme A, stěnu S a přímku l.

Tvrzení dokážeme sporem. Tedy řekněme, že A neleží na S. Pak z konvexity existuje nějaká stěna S' taková, že ji l protíná mezi A a P, průsečík označme B. Všimněme si, že $|AP| > |BP|$. Nyní mohou nastat dva případy. Buď B je význačný bod a leží na S' a pak se dostáváme do sporu s minimalitou vzdálenosti $|AP|$. A nebo existuje nějaký jiný význačný bod K pro S'. Takový bod ale musí být blíže P než B, tedy $|AP| > |BP| > |KP|$, dle tvrzení na začátku důkazu, což je opět spor.

Poznámky:

Většina řešení byla správných. *(Vojta „Dláža“ Gaďurek)*

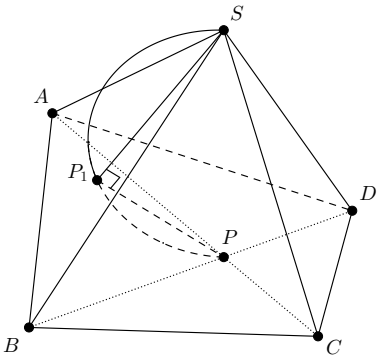
Úloha 8.

Úhlopříčky základny $ABCD$ čtyřbokého jehlanu $ABCDS$ jsou navzájem kolmé. Navíc je jejich průsečík P zároveň kolmým průmětem vrcholu S na základnu. Dokažte, že všechny čtyři kolmé průměty bodu P na roviny ABS, BCS, CDS a DAS leží na jedné kružnici.

Řešení:

Průměty bodu P do rovin ABS, BCS, CDS a DAS budeme označovat P_1, P_2, P_3, P_4.

Nejprve si všimněme, že $|\sphericalangle SP_iP| = 90°$ pro libovolné i. Potom bod P_i leží na oblouku *Thaletovy kružnice* nad úsečkou PS, tj. jeho vzdálenost od středu úsečky PS, který provizorně označíme T, je rovna $\frac{|PS|}{2}$. Vidíme, že každý z bodů P_1, P_2, P_3, P_4 má od bodu T stejnou vzdálenost $\frac{|PS|}{2}$. Proto všechny tyto body musí ležet na sféře (kterou bychom mohli nazvat „Thaletovou sférou“ nad úsečkou PS).



Nyní bychom chtěli ještě dokázat, že body P_1, P_2, P_3, P_4 leží zároveň v jedné rovině. V takovém případě by totiž musely ležet v průniku sféry a roviny, což je kružnice. Zde použijeme pomocné tvrzení.

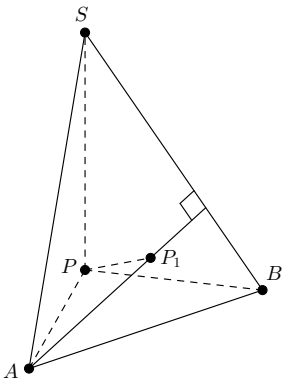
Tvrzení. *Průměty P_1, P_2, P_3, P_4 jsou ortocentry trojúhelníkových stěn jehlanu, ve kterých se nacházejí.*

Důkaz provedeme pro P_1, pro ostatní body se tvrzení dokáže analogicky.

Důkaz. Máme v prostoru body A, B, P, S, P_1, kde $AP \perp BP$ – úhlopříčky AC, BD podstavy jsou kolmé a $SP \perp AP$, $SP \perp BP$, protože P je kolmou projekcí S na podstavu $ABCD$. Potom P_1 vzniklo kolmým promítnutím P na rovinu ABS, takže $PP_1 \perp ABC$.

Protože je úsečka AP kolmá na BP a zároveň $AP \perp SP$, je AP kolmá na celou rovinu BSP. Potom každá úsečky této roviny, takže i BS, je kolmá na AP. Dále víme, že úsečka PP_1 je kolmá na ABS, tím pádem je kolmá i na $BS \subset ABS$. Z toho, že $AP \perp BS$ a $PP_1 \perp BS$, už nám ale plyne, že celá rovina APP_1 je kolmá na úsečku BS. A jelikož $AP_1 \subset APP_1$, je také $AP_1 \perp BS$. Zjistili jsme, že v trojúhelníkové stěně ABS je spojnice AP_1 kolmá na stranu BS, je to tedy výška z bodu A.

Úplně stejným způsobem lze dokázat (díky symetrii úlohy), že BP_1 je výška v ABS z bodu B. Díky tomu P_1 musí ležet na průsečíku výšek ABS a je to tedy ortocentrum.

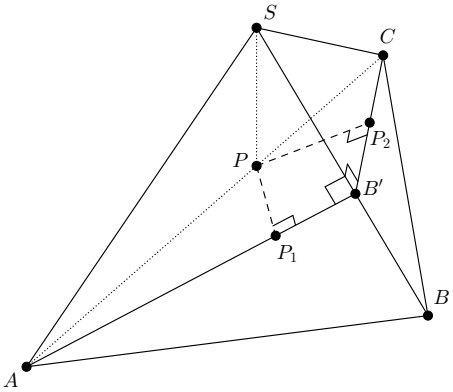


Označme si A_0 patu výšky z bodu A v trojúhelníku ABS a C_0 patu výšky z bodu C v trojúhelníku BCS. Dokážeme, že tyto paty jsou vlastně jeden bod $A_0 = C_0$. Použijme poznatek, že

$A_0 = BS \cap APP_1$ a obdobně $C_0 = BS \cap CPP_2$. Jelikož obě roviny APP_1 a CPP_2 jsou kolmé na jednu úsečku BS, musí být rovnoběžné $APP_1 \parallel CPP_2$.

Protože $P \in APP_1 \cap CPP_2$, tj. obě roviny procházejí bodem P, musí být totožné $APP_1 = CPP_2$. Potom je ale $A_0 = BS \cap APP_1 = BS \cap CPP_2 = C_0$, čili obě paty jsou stejné. Tento jeden bod od teď budeme značit B'.

To, že paty výšek ze dvou sousedních stěn leží v jednom bodě, se analogicky dokáže i pro zbylé tři hrany jehlanu AS, CS, DS. Paty budeme dále označovat A', C', D'.



Nyní už pojďme dokázat tvrzení.

Tvrzení. *Body P_1, P_2, P_3, P_4 leží v jedné rovině.*

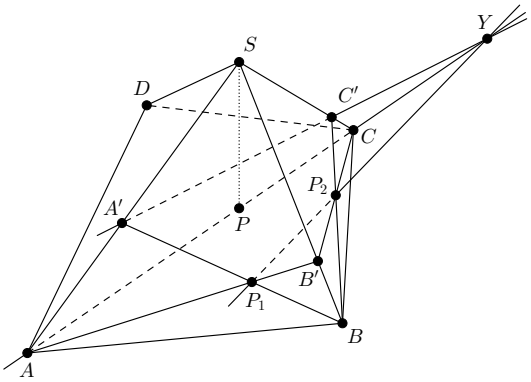
Důkaz. Nejprve vezměme přímku P_1P_2. Protože P_1 leží na výšce AB' a P_2 leží na výšce CB', leží přímka P_1P_2 v rovině $AB'C$. Zároveň protože $P_1 \in A'B$ a $P_2 \in C'B$, leží přímka P_1, P_2 také v rovině $A'BC'$. Proto P_1P_2 musí být průsečnicí rovin $P_1P_2 = AB'C \cap A'BC'$.

Úplně stejným způsobem dojdeme k tomu, že $P_3P_4 = AD'C \cap A'DC'$.

Nyní uvažme body A, A', C, C'. Ty leží všechny v jedné rovině ACS, proto přímky AC a $A'C'$ jsou buď rovnoběžné nebo různoběžné.

Pokud jsou různoběžné, můžeme vzít jejich průsečík $Y = AC \cap A'C'$, potom Y leží v obou rovinách $Y \in AC \subset AB'C$ a $Y \in A'C' \subset A'BC'$. Proto musí ležet na jejich průsečnici $Y \in AB'C \cap A'BC = P_1P_2$. Obdobně $Y \in AC \subset AD'C$ a $Y \in A'C' \subset A'DC'$ a z toho dostaneme, že $Y \in P_3P_4$. Nyní vidíme, že $Y \in P_1P_2 \cap P_3P_4$, tj. přímky P_1P_2, P_3P_4 se protínají v bodě Y. Jsou tedy nutně různoběžné a body P_1, P_2, P_3, P_4 leží v jedné rovině.

Druhou možností je, že přímky AC a $A'C'$ jsou rovnoběžné $AC \parallel A'C'$. Víme, že $BDS \perp AC$, díky rovnoběžnosti je potom také $BDS \perp A'C'$. Když je $AC \perp BDS$, je i rovina $AB'C \perp BDS$ a stejně tak když $A'C' \perp BDS$, je i $A'BC' \perp BDS$. Pokud jsou ale obě roviny $AB'C$, $A'BC'$ kolmé na BDS, musí být i jejich průsečnice $AB'C \cap A'BC' = P_1P_2$ kolmá na BDS. Tím, že $P_1P_2 \perp BDS \perp AC$, musí být $P_1P_2 \parallel AC$. Pokud bychom celý tento postup zopakovali pro body P_3, P_4 a roviny $AD'C$ a $A'DC'$, došli bychom k $P_3P_4 \parallel AC$. Zjišťujeme tedy, že $P_1P_2 \parallel P_3P_4$, a to už stačí, aby P_1, P_2, P_3 a P_4 ležely v jedné rovině.



Ukázali jsme, že průměty P_1, P_2, P_3, P_4 leží v rovině a zároveň na povrchu sféry. Průnikem sféry s rovinou je kružnice, takže body leží na kružnici.

Poznámky:
Mnoho řešitelů řešilo úlohu pouze pro jehlan s kosočtvercovou podstavou. Toto ovšem důkaz výrazně zjednodušilo, takže jsem za něj (pokud byl správný) udílel pouze 1 bod. Nemalá část lidí se rozhodla použít analytiku. U této úlohy to celkem fungovalo, každopádně to určitě není preferovaný způsob řešení. Například úlohy v reálných soutěžích bývají často vybírány speciálně tak, aby nešly analyticky upočítat. *(Ondra Trinkewitz)*

Opakování

3. PODZIMNÍ SÉRIE — VZOROVÉ ŘEŠENÍ

Úloha 1.

Pro kladné celé číslo n definujme

$$f(n) = 1 + 11 + 111 + \cdots + \underbrace{11\ldots1}_{n\text{-krát}},$$

kde sčítáme n sčítanců. Určete nejmenší n takové, že $f(n)$ je násobkem 45.

ŘEŠENÍ:
Označme si

$$\varphi(n) := \underbrace{11\ldots1}_{n\text{-krát}}.$$

Potom $f(n)$ můžeme zapsat jako $f(n) = \sum_{k=1}^{n} \varphi(k)$. Všimněme si, že $f(n)$ je násobkem 45 právě tehdy[4], když je násobkem 5 a zároveň 9. Rozeberme nejprve dělitelnost pěti. Nejprve si všimněme, že dekadický zápis $\varphi(k)$ končí jedničkou pro libovolné $k \in \mathbb{N}$, čili $\varphi(k) \equiv 1 \pmod{10}$. Potom je také $\varphi(k) \equiv 1 \pmod 5$. Protože $f(n)$ je součet n čísel, která dávají zbytek 1 modulo 5, bude výsledek dávat zbytek n:

$$f(n) = \sum_{k=1}^{n} \varphi(k) \equiv \sum_{k=1}^{n} 1 = n \pmod 5.$$

Vidíme, že aby mohlo $5 \mid f(n)$, musí $5 \mid n$.

Nyní se podívejme na dělitelnost devíti. Vyřešíme nejprve, kolik je $\varphi(n)$ modulo 9. Platí, že zbytek po dělení číslem 9 je stejný jako zbytek jeho ciferného součtu po dělení 9. Proto $\varphi(n) \equiv n \pmod 9$. Můžeme tedy spočítat zbytek

$$f(n) = \sum_{k=1}^{n} \varphi(k) \equiv \sum_{k=1}^{n} n = \frac{n(n+1)}{2} \pmod 9.$$

Proto aby platilo $9 \mid f(n)$, musí $9 \mid f(n) = \frac{n(n+1)}{2}$, tedy $9 \mid n(n+1)$. Trojka nemůže zároveň dělit dvě po sobě jdoucí čísla, takže musí buď $9 \mid n$, nebo $9 \mid n+1$.

Dejme nyní vše dohromady. Zjistili jsme, že $5 \mid n$ a zároveň $9 \mid n$, nebo $9 \mid n+1$. Vyřešme tedy dva případy. Uvažme nejprve $5 \mid n$ a $9 \mid n$. To platí právě tehdy, když $45 \mid n$, takže n je nějaký násobek 45. Nejmenší takový násobek je $n = 45$. Pro druhý případ $5 \mid n$ a $9 \mid n+1$ vyzkoušejme několik možností. Aby $9 \mid n+1$, musí $n = 9k - 1$ pro nějaké $k \in \mathbb{N}$. Dostáváme postupně čísla 8, 17, 26, 35. Nejmenší, které je dělitelné 5, je 35.

Protože $35 < 45$, nejmenší řešení je $n = 35$.

[4] Ekvivalence platí, protože 5 a 9 jsou nesoudělná

Poznámky:
Většina řešitelů vyřešila úlohu správně. Nejčastější chybou bylo tvrdit, že ciferný součet $f(n)$ se rovná $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. Toto neplatí pro větší n. (Zkus si dosadit $n = 10$.) Čísla pouze dávají stejný zbytek modulo 9. *(Ondra Trinkewitz)*

Úloha 2.

Označme $f(x) = \frac{1}{1-x}$. Určete $f^{2025}(2024)$.

Řešení:
Podíváme se, co se stane, pokud $f(x)$ několikrát opakujeme.

$$f^1(x) = \frac{1}{1-x}$$
$$f^2(x) = \frac{1}{1-f^1(x)} = \frac{1}{1-\frac{1}{1-x}} = \frac{1}{\frac{-x}{1-x}} = \frac{1-x}{-x}$$
$$f^3(x) = \frac{1}{1-f^2(x)} = \frac{1}{1-\frac{1-x}{-x}} = \frac{1}{\frac{-1}{-x}} = x$$

Vidíme, že $f^3(x) = x$, a tak platí $f^{3k}(x) = x$ pro každé přirozené k. Jelikož $2025 = 3 \cdot 675$, tak $f^{2025}(x) = f^3(x) = x$, tedy $f^{2025}(2024) = 2024$.

Poznámky:
Všichni řešitelé si s úlohou velmi dobře poradili, jen někteří trochu válčili s úpravami výrazů nebo se zbytky po dělení číslem 3, jelikož $f(x) = f^1(x)$ nikoliv $f^0(x)$. *(Klárka Grinerová)*

Úloha 3.

Johy na tabuli napsala čísla 5, 7 a 11. *Poté v každém kroku vybrala z tabule dvě čísla a, b a připsala tam také číslo $5a - 4b$. Mohlo se na tabuli po konečném počtu kroků objevit číslo* 2024*?*

Řešení:
Všimnime si, že na tabuli sú iba nepárne (liché) čísla. Ak sú na tabuli iba nepárne čísla, vieme v jednom kroku pripísať iba ďalšie nepárne číslo. Prečo? Zoberme si dve čísla z tabule, keďže sú nepárne, vieme ich zapísať napríklad ako $a = 2k + 1$ a $b = 2m + 1$, kde k a m sú celé. Potom pripíšeme číslo

$$5\,(2k + 1) - 4\,(2m + 1) = 10k + 5 - 8m - 4 = 2\,(5k - 4m) + 1,$$

čo je vždy nepárne.

To znamená, že na to, aby sme na tabuľu dopísali párne (sudé) číslo, musí už nejaké párne číslo na tabuli byť. V našom príklade tam na začiatku nie je, a tak sa nikdy nedostaneme do stavu, že pripíšeme prvé párne číslo. Nikdy sa tak na tabuli neobjaví žiadne párne číslo, teda ani 2024.

Poznámky:
Väčšina riešiteľov riešila úlohu pomocou parity. Dá sa to ale napríklad aj cez zvyšky po delení 4 alebo 5, môžeš si to vyskúšať. *(Alica Dományová)*

Úloha 4.

Označme $\mathbb{P}$ množinu všech prvočísel. Nalezněte všechny funkce $f : \mathbb{P} \to \mathbb{P}$ takové, že pro libovolná $p, q \in \mathbb{P}$ platí

$$\mathrm{NSD}(p, q) = \mathrm{NSD}(f^p(q), f^q(p)).$$

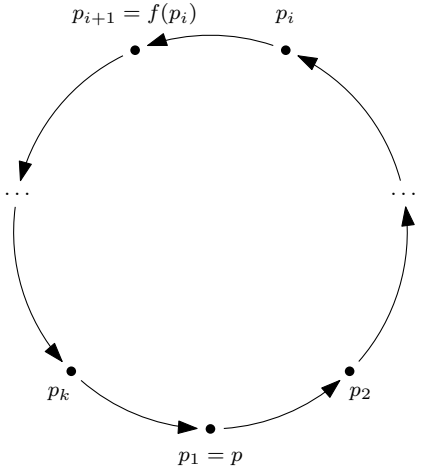
Řešení:
Všimněme si, že $f(x) = x$ rovnost splňuje. Dále ukážeme, že žádná jiná funkce rovnost nesplňuje.

Uvažme vyhovující funkci, která není identita. Pak jistě existují nějaká prvočísla $p \neq q$ taková, že $f(p) = q$. Ze vztahu ze zadání pro dvojici prvočísel p, p platí: $p = \mathrm{NSD}(p, p) = \mathrm{NSD}\left(f^p(p), f^p(p)\right) = f^p(p)$. Co to vlastně znamená? Pokud máme prvočíslo p, vrátíme se po p aplikacích funkce f zpět na hodnotu p, pro každé prvočíslo tak funkce vytvoří cyklus.

Mějme cyklus C_p prvočísel $p_1, \ldots, p_k$ takový, že $k \mid p$ (neboť víme, že po p krocích se opět dostaneme na začátek cyklu), $p_1 = p$, $p_2 = q$, pro $i < k$ platí $f(p_i) = p_{i+1}$ a $f(p_k) = p_1$. Protože p je prvočíslo, může být k pouze 1 nebo p. Jelikož p a $f(p) = q$ jsou dva různé prvky cyklu, nemůže k být rovno 1, musí být tedy rovno p.

Analogicky získáme i cyklus C_q délky q obsahující q. Cykly C_q a C_p oba obsahují prvočíslo q, tedy platí $C_q = C_p$. To je ale spor, protože mají rozdílné délky.

Jediná funkce, která splňuje rovnici je opravdu $f(p) = p$.



Poznámky:
Spousta řešení byla správných. Ovšem hodně jich máchalo rukama, nohama, za což jsem bohužel musel strhávat body. :(*(Vojta „Dláža“ Gaďurek)*

Úloha 5.

Nechť $f : \mathbb{N} \to \mathbb{N}$ je funkce daná předpisem

$$f(n) = \begin{cases} \frac{n}{2}, & \text{pokud je } n \text{ sudé,} \\ 3n + 1, & \text{pokud je } n \text{ liché.} \end{cases}$$

Dokažte, že pro libovolné $n \in \mathbb{N}$ lze zvolit $k \in \mathbb{N}$ takové, že v nekonečné posloupnosti

$$kn, \quad f(kn), \quad f(f(kn)), \quad f(f(f(kn))), \quad \ldots$$

se vyskytne číslo 1.

Řešení:
Nejprve si uvědomme, že jakmile se dostaneme k číslu 2^i pro libovolné nezáporné i, po i iteracích naší funkce se dostaneme na 1. Naším cílem bude tedy pro dané n najít takové k, které by argument funkce eventuálně přetvořilo na mocninu dvou.

Vyjádřeme si naše dané n jako $2^\ell x$, kde x je liché a $\ell \geq 0$. Jistě takto můžeme vyjádřit libovolné n (uvědomme si, že pro lichá n bude $\ell = 0$). Zřejmě při prvních ℓ iteracích budeme argument funkce pouze dělit dvěma. Předpokládejme, že naše k je liché (pokud by bylo sudé, pouze bychom přidali iterace, které by argument dělily dvěma, až bychom se eventuálně dostali k nějakému lichému k'). Po nějakém počtu iterací tedy budeme mít číslo kx, které je liché, po další iteraci bude $3kx + 1$.

Ukážeme, že existují k, j, pro něž platí $3kx + 1 = 2^j$, tedy, že výše zmíněný výraz je mocninou dvou. Vyjádřeme si $k = \frac{2^j-1}{3x}$. Jelikož k musí být přirozené, musí $3x$ dělit $2^j - 1$, chceme tedy vybrat takové j, že $2^j \equiv 1 \pmod{3x}$.

Nyní můžeme být hrozně fancy a vzpomenout si, že existuje Eulerova věta. Ta nám říká, že pro každé přirozené n a každé přirozené a nesoudělné s m platí, že $a^{\varphi(m)} \equiv 1 \pmod{m}$. Pokud tedy do Eulerovy věty za m dosadíme $3x$ a za a dosadíme 2 (což je jistě s lichým číslem $3x$ nesoudělné), dostaneme $2^{\varphi(3x)} \equiv 1 \pmod{3x}$. Získáme tak, že nějaké takové vyhovující j bude například $\varphi(3x)$.

Pokud si náhodou na Eulerovu větu nevzpomeneme, můžeme si uvědomit, že mezi prvními $3x+1$ mocninami 2 budou z Dirichletova principu určitě dvě se stejným zbytkem modulo $3x$. Nechť to jsou 2^a a 2^b, kde BÚNO $a \geq b$. Pak platí $2^a \equiv 2^b \pmod{3x}$. Jelikož 2^b a $3x$ jsou nesoudělné, můžeme kongruenci vydělit 2^b. Tím získáme $2^{a-b} \equiv 1 \pmod{3x}$. Pokud tedy zvolíme $j = a - b$, máme příslušný vyhovující exponent, který lze jednoduše získat spočtením prvních několika mocnin 2 a jejich zbytků modulo $3x$.

Dokázali jsme, že takové j lze zvolit, tedy lze zvolit i příslušné k. Tím pádem bude i nějaký člen naší posloupnosti mocninou 2 a opravdu se v posloupnosti eventuálně vyskytne číslo 1.

Poznámky:
Naprostá většina řešitelů postupovala stejným směrem, jako vzorové řešení. Někteří řešitelé byli odvážní a vydali se jinudy. Některým to vyšlo, jiní se bohužel ztratili v nefungujících argumentech. Byla jsem přísná a za neocitování vět/nedovysvětlené věci jsem strhávala bod. Za řešení, kterým chybělo si uvědomit, že existuje něco jako Eulerova věta, jsem dávala 3 body.

(Adéla Karolína „Áďa“ Žáčková)

Úloha 6.

Štěpán si nakreslil svůj oblíbený nedegenerovaný trojúhelník. Poté v každém kroku opakoval následující: změřil délky stran a, b, c svého současného trojúhelníku, smazal jej a pokusil se nakreslit nový trojúhelník s délkami stran $a + b - c$, $a + c - b$, $b + c - a$. Pokud z úseček s těmito délkami nešel sestrojit nedegenerovaný trojúhelník, Štěpán kreslení zanechal. Určete všechny možné délky stran prvního trojúhelníku, pokud víte, že Štěpán kreslil nové a nové trojúhelníky do nekonečna.

Řešení:
Ukažme, že jestli se Štěpánovi podařilo kreslit trojúhelníky do nekonečna, jistě začal s rovnostranným trojúhelníkem.

Bez újmy na obecnosti pro spor předpokládejme, že máme nerovnostranný trojúhelník se stranami a, b, c, kde $a \geq b \geq c > 0$, takový, že by mohl Štěpán kreslit trojúhelníky do nekonečna. Označme si $S = a + b + c$. Po prvním kroku se nám délky stran změní na $a + b - c$, $b + c - a$, $c + a - b$. Všimněme si, že tyto délky umíme zapsat jako $a + b - c = S - 2c$, $b + c - a = S - 2a$, $c + a - b = S - 2b$. Vzhledem k předpokladu $a \geq b \geq c > 0$ budou délky stran nového trojúhelníku seřazeny následovně: $S - 2c \geq S - 2b \geq S - 2a$.

Podívejme se nyní na rozdíl nejdelší a nejkratší strany. Na začátku to byly po řadě strany a a c, jejich rozdíl byl tedy roven $a - c$. V dalším kroku to pak je rozdíl stran $S - 2c$ a $S - 2a$, tedy $S - 2c - S + 2a = 2(a - c)$. To ovšem znamená, že se rozdíl nejdelší a nejkratší strany v každém kroku zdvojnásobí. Pokud tedy na začátku Štěpán dostal trojúhelník, kde je tento rozdíl větší než

0, a víme, že v každém kroku 2x vzroste, po nějakém kroku zmíněný rozdíl jistě přesáhne i hodnotu S.

Také ale platí, že se součet stran trojúhelníku na začátku a po prvním kroku nezmění, jelikož $a+b+c=S$ a zároveň

$$S-2a+S-2b+S-2c=3S-2(a+b+c)=3S-2S=S.$$

Tím pádem zůstává obvod trojúhelníku stejný a zároveň, jak už víme, rozdíl nejdelší a nejkratší strany v nějakém kroku přesáhne hodnotu S. Označme si délky stran takového trojúhelníku jako $c \le b \le a > c+S$. Jelikož je nutně každá strana trojúhelníku menší než jeho obvod, platí $S > a > c+S$, tedy strana c by musela být záporná. Dostáváme tak spor s předpokladem, že rozdíl nejdelší a nejkratší strany je na začátku nenulový (že je trojúhelník nerovnostranný), tudíž tento rozdíl musí být roven 0. Pak ovšem na začátku platilo $a \ge b \ge c = a \implies a=b=c$.

Pro rovnostranný trojúhelník s délkami stran a, a, a dostaneme v dalším kroku trojúhelník o délce každé strany $a+a-a$, tedy opět a. Vidíme, že trojúhelník vůbec nezměníme, takže ho opravdu můžeme (ne)obměňovat do nekonečna.

Závěrem je, že se Štěpánovi mohlo povést kreslit trojúhelníky do nekonečna právě tehdy, když začal s rovnostranným trojúhelníkem.

Poznámky:
Na tuto úložku nám dorazila spousta různých řešení! Každý řešitel k zadání přistupoval trošku jinak – některé postupy byly o dost pracnější než postup, který jsem použila ve vzoráku. To v některých případech vedlo k menším chybkám nebo k nepořádným důkazům a v takových případech jsem strhávala bodíky. I techničtější cestou se ale většině řešitelů podařilo dojít ke správnému závěru a všichni se s úložkou náležitě poprali! *(Lenka Poljaková)*

Úloha 7.

Najděte všechny funkce $f : \mathbb{N} \to \mathbb{N}$ takové, že pro každé $n \in \mathbb{N}$ existuje právě jedno $k \in \mathbb{N}$ splňující $f^k(n) \le n+k+1$.

Řešení:
Nechť f je libovolná funkce vyhovující zadání. Sporem o ní dokážeme, že pro všechna $n \in \mathbb{N}$ splňuje $f(n) > n+1$. Pro spor tedy předpokládejme, že existuje $n_1 \in \mathbb{N}$ takové, že $f(n_1) \le n_1+1$. Označme $n_2 = f(n_1)$. Pro n_2 ze zadání existuje k_2 takové, že $f^{k_2}(n_2) \le n_2+k_2+1$. Dosazením za n_2 dostáváme:

$$f^{k_2}(f(n_1)) \le f(n_1)+k_2+1,$$
$$f^{k_2+1}(n_1) \le f(n_1)+k_2+1 \le (n_1+1)+k_2+1 = n_1+(k_2+1)+1,$$

kde druhá nerovnost plyne z $f(n_1) \le n_1+1$. Pro n_1 je tedy hodnota k, která splňuje nerovnost ze zadání, k_2+1. To je ale spor, protože platí $f^1(n_1) \le n_1+1+1$ a nerovnost je tedy splněna i pro $k=1$, což je nutně jiná hodnota ($k_2 \neq 0$). Dostali jsme spor a pro každé n tedy platí $f(n) > n+1$. Tedy $f(n) \ge n+2$, z čehož plyne $f^k(n) \ge n+2k$ pro všechna $k \in \mathbb{N}$.

Zvolme si nyní konkrétní n'. Pro něj existuje unikátní k', pro které je splněna nerovnost ze zadání $f^{k'}(n') \le n'+k'+1$ a zároveň platí nerovnost $f^{k'}(n') \ge n'+2k'$. Musí proto platit:

$$n'+k'+1 \ge n'+2k',$$
$$1 \ge k'.$$

A jelikož $k' \in \mathbb{N}$, tak z toho již $k'=1$. Právě jsme tedy dokázali, že aby funkce vyhovovala zadání, tak pro všechna n musí být hodnota k splňující nerovnost v zadání rovna jedné. Tedy $f(n) \le n+2$ pro všechna n. Máme však i opačnou nerovnost a dohromady tedy $f(n) = n+2$ pro všechna $n \in \mathbb{N}$. Taková funkce je již jednoznačně určena a stačí ukázat, že skutečně vyhovuje zadání. To je však již jednoduché, protože zřejmě pro libovolné n a $k=1$ je nerovnost splněna, ale pro $k \ge 2$ dostáváme $f^k(n) = n+2k \ge n+k+2$. Jediná funkce vyhovující zadání je tedy $f(n) = n+2$.

Poznámky:
Nejtěžší na řešení bylo ukázat, že je funkce pro všechna n rostoucí, což došlá řešení dělala rozmanitými způsoby. Vždy však bylo nejdůležitější neztratit se v nerovnostech. Některá řešení si nedala pozor, ke které hodnotě n patří dané k a pak například odečítala k, která vůbec nebyla stejná.

Důležité také bylo nepředpokládat o funkci nic, co nemusí platit - funkce například nemusí mít žádný předpis polynomem a může se pro různé hodnoty chovat velmi odlišně. No a pak je také důležité nezapomínat, že když člověk dojde ke konci důkazu a správně určí, že funkce vyhovující zadání nemůže mít jiný předpis než $f(n) = n + 2$, tak je ještě důležité alespoň zmínit, že tento předpis již zadání splňuje. *(Martin „Fofík“ Fof)*

Úloha 8.

Lukáš na tabuli napsal konečně mnoho racionálních čísel. Poté přišla Bára, z tabule zvolila dvě čísla x, y (ne nutně různá) taková, že $xy \neq 1$, a připsala na tabuli také číslo $\frac{x+y}{1-xy}$. Toto mohla libovolně mnohokrát zopakovat. Dokažte, že ať napsal Lukáš na tabuli jakákoliv čísla, vždy existovalo nějaké $q \in \mathbb{Q}$, které Bára na tabuli nemohla dostat, ať se snažila sebevíc.

Řešení:
Když si zkusíme dosadit za racionální čísla $x = \frac{a}{b}$ a $y = \frac{c}{d}$, zjistíme, že $\frac{x+y}{1-xy} = \frac{ad+bc}{bd-ac}$. Toto nám začne připomínat násobení komplexních čísel: $(b + ai)(d + ci) = (bd - ac) + (ad + bc)i$; případně Brahmaguptovu identitu: $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ad + bc)^2 + (bd - ac)^2$. Pro libovolné $x \in \mathbb{Q}$ v základním zlomkovém tvaru $x = \frac{a}{b}$ tedy označme a zkoumejme $\widehat{x} = a^2 + b^2$. Všimněme si, že $\widehat{x} \in \mathbb{N}$. Pokud vezmeme nějaké Bárou vytvořené číslo $z = \frac{x+y}{1-xy} = \frac{ad+bc}{bd-ac}$ a převedeme zlomek do základního tvaru vydělením čitatele i jmenovatele číslem D, kde $D = \mathrm{NSD}(ad + bc, bd - ac)$, pak pro $\widehat{x}$, $\widehat{y}$ a $\widehat{z}$ definovaná stejně jako výše bude platit:

$$\widehat{z} = \frac{(ad+bc)^2}{D^2} + \frac{(bd-ac)^2}{D^2} \mid (ad+bc)^2 + (bd-ac)^2 = \left(a^2+b^2\right)\left(c^2+d^2\right) = \widehat{x} \cdot \widehat{y}.$$

Označme $X = \{x_1, x_2, \ldots, x_n\}$ množinu čísel, která Lukáš na začátku napsal. Kdykoliv Bára na tabuli přidala nějaké číslo $z = \frac{x+y}{1-xy}$, víme, že $\widehat{z} \mid \widehat{x} \cdot \widehat{y}$. Potom ale platí, že množina prvočísel, která dělí $\widehat{z}$, musí nutně být podmnožinou prvočísel, která dělí $\widehat{x} \cdot \widehat{y}$. To ale znamená, že pro každé z, které kdy Bára na tabuli vytvoří, může být $\widehat{z}$ dělitelné pouze prvočísly (tedy mít ve svém rozkladu pouze prvočísla), která dělila $\widehat{x}_i$ pro některé z počátečních čísel $x_i \in X$. Volně řečeno, pomocí Bářiny operace nemůže v rozkladu $\widehat{z}$ vzniknout žádné „nové“ prvočíslo.

Nyní tedy vezměme nějaké prvočíslo $p \equiv 1 \pmod 4$ (k čemu bude tato vlastnost potřeba, uvidíme později) takové, že $p \nmid \widehat{x}_i$ pro každé $x_i \in X$. To jde vždycky, protože prvočísel kongruentních 1 modulo 4 je nekonečně mnoho.

Tudíž p nemůže dělit $\widehat{z}$ pro žádné z, které kdy Bára umí na tabuli vytvořit. Kdybychom tedy našli nějaké $w \in \mathbb{Q}$ takové, že $p \mid \widehat{w}$, máme vyhráno, protože je Bára určitě nevyrobí.

Nyní si vzpomeneme na známé tvrzení, že pro každé prvočíslo p kongruentní 1 modulo 4 je -1 kvadratický zbytek, tedy že existuje $k \in \mathbb{N}$ takové, že $k^2 \equiv -1 \pmod p$. Potom ale platí $p \mid k^2 + 1^2$, kde si můžeme všimnout, že $k^2 + 1^2 = \widehat{\left(\frac{1}{k}\right)}$. Takže když zvolíme naše $w = \frac{1}{k}$, platí $p \mid \widehat{w}$ a máme vyhráno.

Našli jsme $w \in \mathbb{Q}$, které Bára nikdy nemůže na tabuli dostat.

Poznámky:
Na úloze bylo nejdůležitější získat náhled, že se Bářina funkce chová pěkně k výrazu $\widehat{x} = a^2 + b^2$. Zbytek úlohy se dal dořešit různě, osobně se mi líbilo elegantní řešení od *Dominika Rigasze* pomocí Gaussových prvočísel[5]. *(Ondra Trinkewitz)*

[5] O Gaussových prvočíslech si můžeš pěkně počíst například tady: *https://prase.cz//library/s_AlgebraickaTC_1/s_AlgebraickaTC_1.pdf*, nebo trochu obsáhleji od strany 29 zde: *https://prase.cz//library/KomplexniCislaJHJO/KomplexniCislaJHJO.pdf*.

Polynomy 1

1. seriálová série — Vzorové řešení

Úloha 1.

Nalezněte všechna reálná čísla q, pro které má polynom $x^4 - 40x^2 + q$ čtyři reálné kořeny, jež tvoří aritmetickou posloupnost.

Řešení:

Mějme nějaké q vyhovující zadání. Ukážeme, že pak již nutně $q = 144$.

Označme kořeny našeho polynomu r_1, r_2, r_3, r_4. Tyto kořeny jsou reálné a tvoří aritmetickou posloupnost, existují tedy[6] $s, d \in \mathbb{R}$ taková, že $r_1 = 3s$, $r_2 = 3s + d$, $r_3 = 3s + 2d$, $r_4 = 3s + 3d$. Z Viètova vztahu pro koeficient u x^3 dostáváme

$$12s + 6d = r_1 + r_2 + r_3 + r_4 = 0,$$

aneb $d = -2s$. Můžeme tedy psát $r_1 = 3s$, $r_2 = s$, $r_3 = -s$, $r_4 = -3s$. Nyní ze vztahu pro koeficient u x^2 obdržíme

$$-10s^2 = r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 = -40,$$

neboli $s = \pm 2$. V obou případech dosazením do vzorce pro absolutní člen dostáváme

$$q = r_1r_2r_3r_4 = 9s^4 = 9 \cdot 16 = 144.$$

Jediným kandidátem na řešení je tudíž $q = 144$. Musíme však ještě ověřit, že q skutečně vyhovuje(!), tedy že pro toto q má polynom čtyři reálné kořeny tvořící aritmetickou posloupnost. To uděláme snadno, neboť dosazením $s = \pm 2$ do výše odvozených vztahů získáme $d = -4$ a $r_1 = 6$, $r_2 = 2$, $r_3 = -2$, $r_4 = -6$ (resp. $d = 4$ a $r_1 = -6$, $r_2 = -2$, $r_3 = 2$, $r_4 = 6$) a jejich „kořenovost“ ověříme přímým výpočtem.

Poznámky:

Přibližně polovina došlých řešení postupovala jako vzorové, leč bohužel často zapomínala získaného kandidáta $q = 144$ ověřit. To šlo buď přímým dosazením, jako je uvedeno výše, nebo ověřením, že nalezené kořeny (a diference) splňují i třetí Viètův vztah (pak to již kořeny být musí). Druhý častý postup byl substituování $t = x^2$ a řešení výsledné kvadratické rovnice. *(Josef „José“ Soural)*

[6] Zde schválně bereme $3s$, abychom se později vyhnuli zlomkům ;).

Úloha 2.

Najděte všechny dvojice polynomů $P, Q \in \mathbb{C}[x]$, jež splňují $Q(x^2) = (x+1)^4 - xP(x)^2$ pro všechny komplexní hodnoty x.

Řešení:
Všimněme si, že $\deg\left((x+1)^4\right) = 4$ a $\deg\left(xP(x)^2\right) = 2\deg(P) + 1$. Pokud $\deg(P) \geq 2$, pak $\deg\left(xP(x)^2\right) \geq 5$. Nemůže se tedy rovnat stupni $(x+1)^4$, takže

$$\deg\left((x+1)^4 - xP(x)^2\right) = \max\left\{4, \deg\left(xP(x)^2\right)\right\} = 2\deg(P) + 1$$

je kladný a lichý. Zároveň ale $\deg\left(Q\left(x^2\right)\right) = 2\deg(Q(x))$, takže se nikdy nerovná kladnému lichému číslu. Musí tedy platit $\deg(P) \leq 1$.

Díky tomu $P(x) = ax + b$ pro nějaká $a, b \in \mathbb{C}$ a

$$(x+1)^4 - xP(x)^2 = x^4 + \left(4 - a^2\right)x^3 + (6 - 2ab)x^2 + \left(4 - b^2\right)x + 1.$$

Tento polynom se rovná $Q\left(x^2\right)$ pro nějaké $Q \in \mathbb{C}[x]$, právě když jsou koeficienty u lichých mocnin x nulové, tedy právě když $a = \pm 2$ a $b = \pm 2$. Z $Q\left(x^2\right)$ je možné jednoznačně určit Q, takže pro každou volbu a, b vyhovuje právě jedna dvojice P, Q:

$$\begin{aligned}
a = 2, \quad b = 2 \quad &\Longrightarrow \quad P(x) = 2x + 2, \quad Q(x) = x^2 - 2x + 1, \\
a = 2, \quad b = -2 \quad &\Longrightarrow \quad P(x) = 2x - 2, \quad Q(x) = x^2 + 14x + 1, \\
a = -2, \quad b = 2 \quad &\Longrightarrow \quad P(x) = -2x + 2, \quad Q(x) = x^2 + 14x + 1, \\
a = -2, \quad b = -2 \quad &\Longrightarrow \quad P(x) = -2x - 2, \quad Q(x) = x^2 - 2x + 1.
\end{aligned}$$

Poznámky:
Mnoho důkazů toho, že $\deg(P) \leq 1$ nebylo úplně přesvědčivých: několik řešitelů si například neuvědomilo, že pro polynomy $R, S \in \mathbb{C}[x]$ rovnost v $\deg(R+S) \leq \max\{\deg(R), \deg(S)\}$ nemusí platit pokud $\deg(R) = \deg(S)$. *(Tomáš Flídr)*

Úloha 3.

Buď $P(x) \in \mathbb{R}[x]$ polynom, který má stupeň 2024, *vedoucí koeficient* 1 *a pro každé celé číslo n takové, že $1 \leq |n| \leq 1012$, splňuje $P\left(\frac{1}{n}\right) = n^2$. Najděte všechna další reálná čísla r, jež splňují $P\left(\frac{1}{r}\right) = r^2$.*

Řešení:
Uvažujme polynom $Q(x) = x^2P(x) - 1$. Platí, že $P\left(\frac{1}{r}\right) = r^2$ právě tehdy, když je $\frac{1}{r}$ kořenem $Q(x)$. Známe tedy již 2024 kořenů Q, a to $\frac{1}{n}$ pro celá čísla n taková, že $1 \leq n \leq 1012$. Stupeň Q je 2026, ze základní věty algebry má tedy ještě další dva kořeny (které můžou být komplexní). Označme tyto dva kořeny r_1 a r_2. Potom je odpovědí $\frac{1}{r_1}$ a $\frac{1}{r_2}$.

Zbývá určit r_1 a r_2, což uděláme pomocí Viètových vztahů pro konstantní a lineární člen Q. Označme S součin všech kořenů Q. Vedoucí koeficient Q je 1, neboť vedoucí koeficient P je 1. Protože konstantní člen Q je -1 a lineární je 0, platí

$$-1 = (-1)^{2026}S = S = r_1r_2 \cdot \prod_{n=1}^{1012} \frac{1}{n} \cdot \frac{1}{-n} = (-1)^{1012} \cdot r_1r_2 \cdot \frac{1}{(1012!)^2} = r_1r_2 \cdot \frac{1}{(1012!)^2},$$

$$0 = (-1)^{2025} \cdot \left(\frac{S}{r_1} + \frac{S}{r_2} + \sum_{n=1}^{1012}\left(\frac{S}{n} + \frac{S}{-n}\right)\right) = -S \cdot \left(\frac{1}{r_1} + \frac{1}{r_2}\right).$$

Jelikož nula zjevně není kořenem Q, můžeme druhou rovnost upravit na $r_2 = -r_1$. Z první rovnosti potom dostáváme $r_1^2 = (1012!)^2$. Tudíž $r_{1,2} = \pm 1012!$.

Odpověď je tedy $\pm\frac{1}{1012!}$.

Poznámky:
Jak si povšimla *Svatava Šimečková*, není na první pohled jasné, že polynom P je jednoznačně daný. To lze buď vyřešit tím, že ukážeme jednoznačnost P, nebo stejně jako ve vzorovém řešení pracujeme s nějakým takovým polynomem P a protože Q se ukáže být jednoznačně daný, je jednoznačný i P.

Většina došlých řešení se vydala stejnou cestu jako to vzorové. Největším oříškem se ukázalo uvědomění si, že kořen Q je převrácená hodnota čísla splňujícího podmínku v zadání. V hodně řešeních mi také chyběla zmínka, že používáme základní větu algebry. Jinak bychom totiž ani nevěděli, že nalezená r_1 a r_2 vskutku jsou kořeny Q. *(Magdaléna Mišinová)*

Polynomy 2 – Malé a velké věci nad $\mathbb{Z}$

Milý příteli,

minule jsme se s polynomy seznámili ve velmi obecné rovině[7]. V tomto díle naproti tomu sestoupíme ke konkrétním záležitostem – naším cílem bude co nejlépe porozumět polynomům nad celými čísly. Prozkoumáme, jak polynomy interagují s pojmy z teorie čísel jako jsou dělitelnosti, kongruence či prvočísla. Za tímto účelem si příslušné pojmy taky pořádně zavedeme.

V první polovině tohoto dílu se budeme věnovat budování základních vlastností a nástrojů, které se hodí v úlohách olympiádního typu – dělitelnostem tvaru $a-b \mid P(a)-P(b)$ a větě o racionálním kořeni. V druhé části si ukážeme dva větší výsledky, které už sice lavírují na pomezí vysokoškolské teorie a v olympiádě tolik užití nenaleznou, ale přesto nám přijdou zajímavé samy o sobě – Schurovu větu a Henselovo lemma.

Opakování: jak rychle rostou reálné polynomy?

Ačkoliv v tomto díle budeme povětšinou pracovat s polynomy nad celými čísly za pomoci jemných celočíselných nástrojů, občas se nám bude hodit mít i hrubé ponětí o tom, jak rychle jejich hodnoty rostou. Poněvadž to už není nic specifického pro celá čísla, můžeme tyto vlastnosti shrnout rovnou nad reálnými čísly. Základem je tvrzení, které jsme dokázali v prvním díle v rámci řešení Cvičení 4:

Úmluva. Když řekneme, že nějaká vlastnost platí „pro dostatečně velká a“, myslíme tím, že existuje nějaké $A \in \mathbb{R}$ takové, že pro všechna $a \geq A$ uvedená vlastnost platí.

Tvrzení. *Ať je $P \in \mathbb{R}[x]$ nekonstantní polynom s kladným vedoucím koeficientem. Potom pro dostatečně velká a platí $P(a) > 0$.*

Jistě si snadno dovedeš rozmyslet, jak bychom tvrzení upravili pro záporný vedoucí koeficient. Také bychom mohli uvažovat o tom, co se bude dít, když místo hodně velkých kladných a budeme uvažovat a hluboko v záporných číslech – zde bude záležet na tom, zda má P sudý, či lichý stupeň.

Důsledek. *Jsou-li $P, Q \in \mathbb{R}[x]$ nenulové polynomy s $\deg P > \deg Q$ a P má kladný vedoucí koeficient, pak pro dostatečně velká a platí $P(a) > Q(a)$.*

Důkaz. Určitě $\deg P > \deg Q \geq 0$, takže P je nekonstantní. Protože Q nemá členy stupně $\deg P$, určitě bude mít rozdíl $P - Q$ stále stupeň $\deg P$ a kladný vedoucí koeficient, podle předchozího tvrzení proto bude od nějaké meze nabývat jen kladných hodnot, což odpovídá $P(a) > Q(a)$. □

Bez důkazu též zmiňme, jak se polynomy porovnávají s jinými známými funkcemi.

Tvrzení. *Ať je $c > 1$ reálné číslo, $P \in \mathbb{R}[x]$ nekonstantní polynom s kladným vedoucím koeficientem a* log *přirozený logaritmus.*

(i) *Pro dostatečně velká a platí $c^a > P(a)$.*
(ii) *Pro dostatečně velká a platí $P(a) > \log a$.*

Neformálně: jakákoliv rostoucí exponenciála nakonec porazí jakýkoliv polynom a jakýkoliv nekonstantní polynom s kladným vedoucím koeficientem nakonec porazí logaritmus.

[7] A taky v komplexní rovině.

Dělitelnost

Nyní už se pusťme do vlastností specifických pro celá čísla. Na chvilku odložíme polynomy, abychom si zavedli dělitelnost a pojmy od ní odvozené. Některé z nich už možná znáš, chceme si ale sjednotit naši startovní pozici.

Definice. Ať jsou a, b celá čísla. Říkáme, že a *dělí* b (nebo též že b *je násobkem* a nebo a *je dělitelem* b), pokud existuje celé číslo c splňující $b = ac$. Značíme $a \mid b$.

Všimni si, že s touto definicí není problém mluvit o dělitelnosti nulou – nevadí, že *dělení* nulou není definované, *dělitelnost* nulou stále dává smysl (a platí $0 \mid a \iff a = 0$).

Cvičení 1. Pokud $a \neq 0$, pak je $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$.

Tvrzení. (vlastnosti dělitelnosti) *Pro libovolná celá čísla a, b, c, d platí:*

(i) $1 \mid a$, $a \mid a$ *i* $a \mid 0$,
(ii) $a \mid b$ *a zároveň* $b \mid c \implies a \mid c$,
(iii) $a \mid b$ *a zároveň* $a \mid c \implies a \mid b + c$,
(iv) $a \mid b$ *a zároveň* $c \mid d \implies ac \mid bd$,
(v) $a \mid b$ *a zároveň* $b \neq 0 \implies |a| \leq |b|$.

Důkaz. V (i) až (iv) jde vždy jen o správnou volbu násobku. Jako příklad si ukažme (iii): z definice dělitelnosti máme $b = ka$ a $c = \ell a$ pro nějaká celá čísla k, ℓ. Potom však $b + c = ka + \ell a = (k + \ell)a$, čímž je naplněna definice $a \mid b + c$, protože $k + \ell$ je opět celé číslo.

Pro (v) si jen stačí uvědomit, že nenulové celé číslo je v absolutní hodnotě alespoň 1. Pokud tedy $b = ac$, kde c je celé číslo, pak $b \neq 0$ implikuje taky $c \neq 0$, čímž už dostaneme $|b| = |a| \cdot |c| \geq |a| \cdot 1$. □

Cvičení 2. Dorozmysli si důkazy bodů (i), (ii) a (iv).

Cvičení 3. (důležité) Jediné celé číslo, jež má nekonečně mnoho dělitelů, je 0.

Jakmile máme pojem dělitelnosti, jsme připraveni přesunout se k prvočíslům:

Definice. *Prvočíslem* rozumíme celé číslo $p > 1$, jehož kladnými děliteli jsou pouze 1 a p samo.

Význam prvočísel pro olympiádní úlohy tkví především v rozkladu na prvočísla. Důkaz jeho jednoznačnosti není úplně jednoduchý, proto se mu zde nebudeme věnovat a pouze bez důkazu zformulujeme:[8]

Věta. (základní věta aritmetiky) *Každé kladné celé číslo n lze zapsat jako součin několika prvočísel $p_1 \cdots p_r$, přičemž tento rozklad je jednoznačný až na záměnu pořadí prvočísel.*

K tomuto se sluší několik vysvětlivek. Zaprvé by se mohlo zdát, že tvrzení nefunguje pro $n = 1$, v tomto případě se ale budeme tvářit, že 1 je „součin žádných prvočísel“. Zadruhé, tvrzení bychom snadno rozšířili i na záporná celá čísla, pak bychom řekli, že každé $n \neq 0$ se (až na pořadí jednoznačně) rozkládá na součin několika prvočísel a jednoho „znaménka“ 1 či -1. Zatřetí, v rozkladu většinou bývá užitečné seskupit kopie toho samého prvočísla do jedné mocniny a následně psát, že n má prvočíselný rozklad

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

kde $p_1, \ldots, p_k$ jsou navzájem různá prvočísla a $e_1, \ldots, e_k$ jsou kladná celá čísla.

Cvičení 4. Mějme (kladná) celá čísla s prvočíselnými rozklady $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, v nichž $p_1, \ldots, p_k$ jsou navzájem různá prvočísla a v případě potřeby jsme doplnili triviální mocniny p_i^0, abychom oba rozklady zapsali stejnou sadou prvočísel. Potom

$$a \mid b \quad \iff \quad \alpha_i \leq \beta_i \text{ pro všechna } i.$$

[8] Pokud by Tě důkaz přece jenom zajímal, můžeme Tě odkázat na první díl seriálu o teorii čísel z 33. ročníku PraSete: *https://prase.cz/archive/33/uvod1s.pdf*.

Definice. Říkáme, že celá čísla a, b jsou *nesoudělná*, pokud neexistuje prvočíslo, které by je obě dělilo. V opačném případě říkáme, že jsou *soudělná*.

Tvrzení. (dělitelnost a nesoudělnost) *Ať jsou a, b, c celá čísla a ať jsou a, b nesoudělná. Potom:*

(i) $a \mid bc \implies a \mid c$,
(ii) $a \mid c$ a zároveň $b \mid c \implies ab \mid c$.

Důkaz. (i) $a \mid bc$ říká, že bc má od každého prvočísla ve svém rozkladu alespoň tolik kopií, co a. Přitom se samozřejmě stačí dívat na ta prvočísla, která dělí a, protože od ostatních má jen 0 kopií. Z nesoudělnosti a, b ale víme, že b do bc nepřispívá žádnými prvočísly, která se vyskytují v a. Všechna tato prvočísla, jež zařídila dělitelnost $a \mid bc$, už proto musela být přítomna v samotném c, takže také $a \mid c$.

(ii) $a \mid c$ říká, že c má alespoň všechna ta prvočísla, co a. Podobně $b \mid c$ říká, že c alespoň ta prvočísla, co b. Jenže z nesoudělnosti a, b se jedná o dvě zcela disjunktní sady prvočísel. Pokud tedy c obsahuje každou zvlášť, obsahuje je i dohromady, takže $ab \mid c$. □

Trochu nepohodlné je na dělitelnosti to, že nám dává jen binární informaci, zda a dělí b, nebo nedělí. Často je pohodlnější o něco jemněji rozlišit, jaký zbytek b dává po dělení a. K tomu si zaveďme pojem *kongruence*:

Definice. Ať jsou a, b, m celá čísla. Říkáme, že a *je kongruentní* b *modulo* m, pokud $m \mid a - b$. Značíme $a \equiv b \pmod m$.

Abychom si osvojili některé vztahy, které kongruence splňují, stačí je přeložit z vlastností dělitelnosti:

Tvrzení. (vlastnosti kongruence) *Uvažujme celá čísla a, b, c, d, m. Potom:*

(i) $a \equiv b \pmod m$ a zároveň $c \equiv d \pmod m \implies a + c \equiv b + d \pmod m$,
(ii) $a \equiv b \pmod m$ a zároveň $c \equiv d \pmod m \implies ac \equiv bd \pmod m$,
(iii) $ac \equiv bc \pmod m$ a zároveň *jsou* c, m *nesoudělná* $\implies a \equiv b \pmod m$.

Důkaz. (i) Máme $m \mid a - b$ i $m \mid c - d$, takže určitě i $m \mid (a - b) + (c - d) = (a + c) - (b + d)$.

(ii) Máme $m \mid a - b$ i $m \mid c - d$ a opět se z těchto násobků pokusíme vyrobit $ac - bd$. Na první pohled není zřejmé, jak to udělat, k úspěchu ale povede přidání nulového výrazu $bc - bc$ skrze

$$m \mid (a - b)c + b(c - d) = ac - bc + bc - bd = ac - bd.$$

(iii) Máme $m \mid ac - bc = (a - b)c$, přičemž c je nesoudělné s m. Víme proto už, že jej můžeme z dělitelnosti odebrat, tudíž $m \mid a - b$. □

Vlastnosti (i) a (ii) dohromady říkají, že pokud nás zajímá zbytek po dělení nějakého výrazu sestávajícího ze sčítání a násobení, pak nám stačí znát jen zbytky vstupních hodnot. „Výraz sestávající ze sčítání a násobení“ je ale jen květnatý popis polynomu, takže už tyto základní vlastnosti kongruencí jsou předzvěstí toho, že polynomy (alespoň nad $\mathbb{Z}$) se budou k počítání modulo m chovat dobře.

Úloha 1. Dokaž, že rovnice $x^2 + y^2 + z^2 = 2023$ nemá celočíselné řešení.

Věta. (malá Fermatova) *Ať celé číslo a není násobkem prvočísla p. Potom* $a^{p-1} \equiv 1 \pmod p$.

Ekvivalentně lze též větu zformulovat jako $a^p \equiv a \pmod p$ pro jakékoliv a (tedy i násobky p).

Důkaz. Podívejme se na množiny $S = \{1, 2, \ldots, p - 1\}$ a $S_a = \{a, 2a, \ldots, (p - 1)a\}$. Zjevně prvky S dávají navzájem různé a nenulové zbytky modulo p. Dokažme, že totéž platí o S_a. Zaprvé, kdyby se přihodilo $ai \equiv aj \pmod p$ pro některá $i, j \in S$, pak můžeme a v kongruenci zkrátit, neboť je nesoudělné s p, takže by to značilo $i \equiv j \pmod p$. Tedy, v násobení číslem a se z různých zbytků nemůže stát ten samý zbytek. Zadruhé, v $ai \equiv 0 \pmod p$ bychom opět mohli zkrátit a a získat $i \equiv 0 \pmod p$, takže také víme, že v násobení číslem a se z nenulového zbytku nemůže stát nulový.

Dohromady tak víme, že z hlediska zbytků modulo p je S_a jen „zamícháním“ S: v obou množinách jsou modulo p zastoupeny všechny nenulové zbytky, každý právě jednou. Pokud tedy u obou vezmeme součin všech prvků, měli bychom modulo p dostat totéž:

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

Každý z činitelů $1, 2, \ldots, p-1$ je ale nesoudělný s p, takže je můžeme zkrátit, čímž nám zbude $1 \equiv a^{p-1} \pmod{p}$, což jsme chtěli dokázat. □

Cvičení 5. Ať je p prvočíslo a $a \not\equiv 0 \pmod{p}$. Rozmysli si, že existuje b takové, že $ab \equiv 1 \pmod{p}$.

Polynomy a dělitelnost

S dělitelností pevně v rukou můžeme do situace vrátit polynomy. Hlavním nástrojem nám bude tvrzení, jehož předzvěst už se objevila u vlastností kongruencí:

Tvrzení. (rozdíl argumentů dělí rozdíl hodnot) *Pro $P \in \mathbb{Z}[x]$ a libovolná celá čísla a, b platí $a - b \mid P(a) - P(b)$.*

Důkaz. Rozepišme $P(x) = \sum_{k=0}^{n} c_k x^k$, potom můžeme zapsat

$$P(a) - P(b) = \sum_{k=0}^{n} c_k \left(a^k - b^k\right).$$

Díky vzorečkům $a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}\right)$ máme $a - b \mid a^k - b^k$. Když tyto rozličné dělence vynásobíme jednotlivými celými čísly c_k a vše sečteme, dělitelnost zůstane zachována, a tedy $a - b \mid P(a) - P(b)$. □

Jinou formulací podobné myšlenky je, že pro $a \equiv b \pmod{m}$ je taktéž $P(a) \equiv P(b) \pmod{m}$. Pozor na to, že tvrzení funguje skutečně jen na polynomy ze $\mathbb{Z}[x]$. Např. takový $Q(x) = \frac{x(x+1)}{2} \in \mathbb{Q}[x]$ sice nabývá ve všech celých číslech celočíselných hodnot, přesto ale $2 - 0 \nmid Q(2) - Q(0)$.

Cvičení 6. Máme-li polynom $P = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ a $r \in \mathbb{Z}$ je jeho kořenem, dokaž, že $r \mid a_0$.

Ukažme si použití získané dělitelnosti na příkladu:

Příklad. Je dán polynom $P \in \mathbb{Z}[x]$. Rozhodni, zda mohou existovat tři navzájem různá $a, b, c \in \mathbb{Z}$ taková, že

$$P(a) = b, \qquad P(b) = c, \qquad P(c) = a.$$

(USAMO 1974)

Řešení. Ukážeme, že nemohou – pro spor ať tedy existují. Aplikací tvrzení potom máme $a - b \mid P(a) - P(b) = b - c$. Analogicky získáme také $b - c \mid c - a$ a konečně $c - a \mid a - b$. Z předpokladu různosti a, b, c jsou tyto rozdíly nenulové, takže

$$|a - b| \leq |b - c| \leq |c - a| \leq |a - b|.$$

Když v sérii (neostrých) nerovností narazíme na stejné číslo na obou koncích, znamená to, že všechny výrazy, které jsme porovnávali, si ve skutečnosti musí být navzájem rovny.

Takže $|a - b| = |b - c| = |c - a|$, jinými slovy (různá) čísla a, b, c se na číselné ose vyskytují tak, že libovolná dvě mají stejnou (nenulovou) vzdálenost. To ale snadno odhalíme jako nemožné: kdyby BÚNO $a < b < c$, pak $|c - a| = |a - b| + |b - c| > |a - b|$, což je spor. Dohromady jsme tak dokázali, že žádaná a, b, c nemohla existovat.

Úloha 2. Najdi všechny polynomy $P \in \mathbb{Z}[x]$, jež splňují: jsou-li $a, b \in \mathbb{Z}$ nesoudělná, pak jsou i $P(a)$, $P(b)$ nesoudělná.

Úloha 3. Najdi všechny polynomy $P \in \mathbb{Z}[x]$ takové, že pro každé kladné celé číslo n platí $P(n) \mid n! + 2$. (PraSe 41–4p–7)

Úloha 4. Najdi všechny polynomy $P \in \mathbb{Z}[x]$ takové, že pro každé kladné celé n platí $n \mid P(2^n)$.

Úloha 5. Královské vojsko táhne krajinou po křivce, která má tvar grafu polynomu P s celočíselnými koeficienty. Boleslav si cestu zkrátil po úsečce mezi body $[a, P(a)]$ a $[b, P(b)]$, kde $a, b \in \mathbb{Z}$, $a \neq b$. Všiml si navíc, že délka této úsečky byla celé číslo. Dokaž, že Boleslav táhl ve směru rovnoběžném s osou x. (Mecz 2021L)

Úloha 6. (těžší) Je dán polynom $P \in \mathbb{Z}[x]$ a dvě různá celá čísla a, b splňující $P(a)P(b) = -(a-b)^2$. Dokaž, že $P(a) + P(b) = 0$.

Úloha 7. (těžší) Polynom $P \in \mathbb{Z}[x]$ splňuje $a^{2^{2024}} - b^{2^{2024}} \mid P(a) - P(b)$ pro všechna $a, b \in \mathbb{Z}$. Dokaž, že $P(x) = Q\left(x^{2^{2024}}\right)$ pro nějaký polynom $Q \in \mathbb{Z}[x]$.

Racionální kořeny

Polynom ze $\mathbb{Z}[x]$ obecně vůbec nemusí mít racionální, či dokonce celočíselný kořen. Víme, že je-li nekonstantní, určitě bude mít nějaké komplexní kořeny, ale dopředu o nich nedovedeme garantovat skoro nic. Kupříkladu $x^2 - 2$ je polynom nad $\mathbb{Z}$, oba jeho kořeny $\pm\sqrt{2}$ jsou ale iracionální reálná čísla. Když už se nám však poštěstí míti racionální kořen, rázem dovedeme znatelně zúžit možnosti, jaké racionální číslo by jím mohlo být:

Úmluva. Jsou-li u, v celá čísla, pak říkáme, že zlomek $\frac{u}{v}$ je *v základním tvaru*, pokud jsou u, v nesoudělná.

Věta. (o racionálním kořeni) *Je-li $\frac{u}{v} \in \mathbb{Q}$ zlomek v základním tvaru, který je zároveň kořenem polynomu $P(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$, $a_n \neq 0$, pak platí $u \mid a_0$ a $v \mid a_n$.*

Důkaz. Máme rovnost $a_n \left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \cdots + a_1 \frac{u}{v} + a_0 = 0$, vynásobení obou stran výrazem v^n pak dá

$$a_n u^n + a_{n-1} u^{n-1} v + \cdots + a_1 u v^{n-1} + a_0 v^n = 0.$$

Zde je pravá strana násobkem u, zatímco na levé straně jsou násobky u všechny členy až na poslední. Nutně tak i tento poslední člen musí být násobkem u, tedy $u \mid a_0 v^n$. Víme, že $\frac{u}{v}$ byl v základním tvaru, tedy u a v jsou nesoudělná. Mocninu v tedy v dělitelnosti můžeme zahodit, a získat tak $u \mid a_0$.

Analogicky jsou všechny členy na levé straně rovnice vyjma prvního násobky v, takže $v \mid a_n u^n$, načež $v \mid a_n$. □

Cvičení 7. Nechť má polynom $P \in \mathbb{Z}[x]$ vedoucí koeficient 1. Jakýkoliv jeho racionální kořen už potom musí být celočíselný.

Příklad. Má-li pro celá čísla a, b, c rovnice $ax^2 + bx + c = 0$ racionální řešení, pak je alespoň jedno z a, b, c sudé.

Řešení. Buď $\frac{u}{v}$ racionální řešení v základním tvaru a předpokládejme pro spor, že a, b i c je liché. Podle věty o racionálním kořeni $u \mid c$, $v \mid a$, což speciálně zaručuje, že u i v jsou lichá. Roznásobením rovnosti $a\left(\frac{u}{v}\right)^2 + b\frac{u}{v} + c = 0$ pomocí v^2 dostaneme $au^2 + buv + cv^2 = 0$. To ale znamená, že tři lichá čísla se sečetla na sudé číslo, což je spor. Alespoň jedno z a, b či c tak muselo být sudé.

Úloha 8. Jsou-li m, n lichá celá čísla, dokaž, že $x^2 + 2mx + 2n$ nemá racionální kořen.

Úloha 9. Jsou dána nenulová $a, b, c \in \mathbb{Z}$ taková, že $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ i $\frac{b}{a} + \frac{c}{b} + \frac{a}{c}$ jsou celá čísla. Dokaž, že $|a| = |b| = |c|$.

Polynomy a prvočísla

Pojďme se nyní přesunout ke slibovaným velkým větám. První z nich pojednává o prvočíselných dělitelích, jež se vyskytnou v hodnotách polynomu ze $\mathbb{Z}[x]$.

Věta. (Schurova) *Budiž $P \in \mathbb{Z}[x]$ nekonstantní. Pak existuje nekonečně mnoho prvočísel p, jež dělí některou hodnotu $P(n)$ pro kladná celá n.*

Schurovu větu lze nahlížet jako zobecnění věty o existenci nekonečně mnoha prvočísel – ta odpovídá tomu, že hodnoty polynomu $P(x) = x$ mají nekonečně mnoho prvočíselných dělitelů. Volbou jiných polynomů lze spoustu prvočísel vyloučit, např. je známo, že žádná hodnota $P(x) = x^2 + 1$ nebude dělitelná kterýmkoliv prvočíslem $p \equiv 3 \pmod 4$, tedy $p = 3, 7, 11, 19, \ldots$, nicméně Schurova věta garantuje, že ať už takto vyšachujeme ze hry sebevíc prvočísel, pořád jich nekonečně mnoho zbude. Pojďme ji dokázat:

Důkaz. BÚNO předpokládejme, že vedoucí koeficient P je kladný, kdyby tomu tak nebylo, budeme se místo P dívat na $-P$. Induktivně zkonstruujeme dvě nekonečné posloupnosti $a_1, a_2, \ldots$ (kladná celá čísla) a $p_1, p_2, \ldots$ (prvočísla) tak, aby jednotlivá p_k byla navzájem různá, a navíc pro každé k platily dělitelnosti

$$p_1 \mid P(a_k), \qquad p_2 \mid P(a_k), \qquad \ldots, \qquad p_k \mid P(a_k).$$

Tím bude věta dokázána, protože každé z prvočísel $p_1, p_2, \ldots$ bude dělit některou hodnotu polynomu P.

Konstrukci začneme následovně: zvolíme si nějaké celé číslo a_1, v němž je hodnota $P(a_1)$ větší než 1 (to lze, protože P je nekonstantní s kladným vedoucím koeficientem, takže dříve či později přeroste jakoukoliv mez). Potom musí $P(a_1)$ mít nějaké prvočíselné dělitele, zvolme si libovolný z nich a označme jej p_1. Tím je hotov základní případ.

Popišme nyní indukční krok, předpokládejme, že už jsme zkonstruovali $a_1, \ldots, a_k$ a $p_1, \ldots, p_k$. Máme celé číslo $P(a_k)$, jež je násobkem všech $p_1, \ldots, p_k$. Podívejme se o něco jemněji na jeho prvočíselný rozklad – nechť

$$P(a_k) = p_1^{e_1} \cdots p_k^{e_k} \cdot m,$$

kde m je nesoudělné s $p_1, \ldots, p_k$. Jinými slovy, exponent mocniny p_i v rozkladu jsme si označili jako e_i a jako m jsme označili „to, co zbylo“ po vytknutí mocnin všech $p_1, \ldots, p_k$.

Naše nové a_{k+1} nyní budeme hledat ve tvaru $a_{k+1} = a_k + t \cdot p_1^{e_1+1} \cdots p_k^{e_k+1}$, přičemž t je celé číslo, které teprve zvolíme. Všimněme si, že nehledě na volbu t toto zaručí následující: pro každé i bude platit $a_{k+1} \equiv a_k \pmod{p_i^{e_i+1}}$, takže též $P(a_{k+1}) \equiv P(a_k) \pmod{p_i^{e_i+1}}$. To speciálně znamená, že jelikož $p_i^{e_i+1} \nmid P(a_k)$, tak ani $p_i^{e_i+1} \nmid P(a_{k+1})$. Naopak ale $p_i^{e_i} \mid P(a_k)$, takže i $p_i^{e_i} \mid P(a_{k+1})$. Vyvodili jsme tedy, že mocnina p_i v prvočíselném rozkladu $P(a_{k+1})$ bude přesně $p_i^{e_i}$.

S tímto pozorováním nyní zvolme t tak, aby platilo

$$P(a_{k+1}) > p_1^{e_1} \cdots p_k^{e_k}.$$

To lze, protože P roste nade všechny meze, takže když zvolíme t dostatečně velké, bude i a_{k+1} dostatečně velké na to, aby $P(a_{k+1})$ přerostlo zvolenou mez $p_1^{e_1} \cdots p_k^{e_k}$. Podobně jako pro $P(a_k)$ se nyní podívejme na prvočíselný rozklad $P(a_{k+1})$. Už víme přesně, jaké očekávat mocniny prvočísel $p_1, \ldots, p_k$, takže zapíšeme

$$P(a_{k+1}) = p_1^{e_1} \cdots p_k^{e_k} \cdot M$$

pro nějaké celé číslo M, které je nesoudělné s $p_1, \ldots, p_k$. Přitom ale $P(a_{k+1}) > p_1^{e_1} \cdots p_k^{e_k}$ znamená $M > 1$, takže M má nějaké prvočíselné dělitele. Zvolme si libovolný z nich a říkejme mu p_{k+1}. Z nesoudělnosti to nemůže být žádné z $p_1, \ldots, p_k$, a přitom $p_{k+1} \mid P(a_{k+1})$, takže jsou jím naplněny požadavky, podle kterých naše posloupnosti konstruujeme. Tím je hotov indukční krok, a tedy i důkaz věty. □

Často můžeš Schurovu větu potkat také ve formulaci, jež říká, že nekonečně mnoho prvočísel dělí některou *nenulovou* hodnotu $P(n)$. Tato verze z té naší snadno vyplývá: pokud by náhodou P měl nějaké celočíselné kořeny, označíme největší z nich jako c. Pro $n > 0$ jsou pak hodnoty $P(n+c)$ nenulové, a přitom aplikováním naší Schurovy věty na polynom $P(x + c)$ musí nekonečně mnoho prvočísel dělit některou z nich.

Zdvihání modulo prvočíselné mocniny

Poslední zastávkou v tomto díle naší jízdy bude následující problém: je dáno $n \in \mathbb{Z}$ a polynom $Q \in \mathbb{Z}[x]$, načež chceme nalézt nějaké $a \in \mathbb{Z}$, v němž je hodnota $Q(a)$ násobkem n. Pro jednoduchost uvažujme, že n je třeba nějaká prvočíselná mocnina[9] $n = p^e$. Pokud má platit $p^e \mid Q(a)$, pak určitě taky $p \mid Q(a)$.

Rozumnou strategií by proto mohlo být nejprve najít a, pro něž je $Q(a)$ násobkem p, a poté se jej snažit „posouvat“ o násobky p – už víme, že tím nezměníme $Q(a) \pmod p$ – tak, aby se stalo i násobkem vyšších mocnin p. Strategie tohoto typu se vyplácí i v některých praktických aplikacích – zkusme to v hrubých obrysech namotivovat na tzv. *Berlekampově–Zassenhausově algoritmu* pro faktorizaci polynomu ze $\mathbb{Z}[x]$. Ten funguje následovně[10]:

(1) Zmodulí koeficienty polynomu prvočíslem p,
(2) nalezne rozklad na součin modulo p,
(3) postupně tento rozklad zlepšuje na rozklad modulo p^2, modulo p^3, ...
(4) až nakonec z rozkladu modulo p^e pro dost velké e „přečte“ rozklad nad $\mathbb{Z}$.

Toto funguje, protože pokud se polynom rozkládá na součin nad $\mathbb{Z}$, pak se bude rozkládat i po zmodulení libovolným p^e, a pokud bude p^e větší než absolutní hodnoty všech koeficientů, jež se vyskytnou v rozkladu, pak bude celočíselný rozklad zřetelný z toho zmoduleného. Navíc se tento krkolomný postup z algoritmického hlediska vyplatí, protože rozkládání polynomů na součin modulo p je mnohem snazší než nad $\mathbb{Z}$ (existují pro to specializované algoritmy) a postupné zdvihání na modulo p^e je (výpočetně) dost levná operace na to, aby celý proces seběhl v rozumném čase.

Toliko k motivaci, proč je tohle vůbec rozumný problém, kterému má smysl se věnovat. Prvním zádrhelem v jeho zkoumání je to, že pro některé volby Q a p posouvací zdvihání selže:

Cvičení 8. Je dáno prvočíslo p. Sestroj polynom $Q \in \mathbb{Z}[x]$ takový, aby kongruence $Q(a) \equiv 0 \pmod p$ měla řešení, ale $Q(a) \equiv 0 \pmod{p^2}$ už nikoliv.

Hodila by se proto nějaká charakterizace, kdy má zdvihání šanci na úspěch. Dobrou představu nám o tom dá *Henselovo lemma*, které si brzy dokážeme. K jeho zavedení si potřebujeme rozšířit slovník o heslo, jež rutinně rozsévá hrůzu v řadách novopečených vysokoškoláků:

Definice. Buď $P(x) = \sum_{k=0}^{n} a_k x^k$ polynom nad komplexními čísly. Jeho *formální derivací* (nebo jen krátce *derivací*) rozumíme polynom $P' \in R[x]$ definovaný předpisem

$$P'(x) = \sum_{k=1}^{n} k a_k x^{k-1}.$$

(Pro konstantní P máme jen $P' = 0$.)

Pokud slovíčko „derivace“ potkáváš v matematice poprvé, gratulujeme, můžeš tento krátký odstaveček přeskočit :-). Pokud jsi jej už potkal(a) a právě Ti z něj běhá mráz po zádech, nezoufej

[9] To se může zdát jako tragicky nahodilá volba, nicméně často to dává smysl v kombinaci s *Čínskou zbytkovou větou* – ta v mnoha situacích ospravedlňuje, že pokud nás zajímá nějaká situace modulo n, jež má prvočíselný rozklad $p_1^{e_1} \cdots p_k^{e_k}$, pak stačí situaci porozumět modulo jednotlivé mocniny $p_i^{e_i}$. Tento seriál ale není o Čínské zbytkové větě – pokud by ses o ní chtěl(a) dozvědět víc, odkážeme Tě na tento sborníkový příspěvek: *https://prase.cz//library/CinskaZbytkovkaMD/CinskaZbytkovkaMD.pdf*.

[10] Schválně tu zamlčujeme některé technické detaily :-). Prosíme, odpusť nám to.

– naše formální derivace souvisí s pojmem derivace v kontextu matematické analýzy jen vzdáleně, shoda názvů je motivovaná tím, že „vypadají stejně“. Zde v seriálu budeme s derivací pracovat čistě jako s velice konkrétním vzorečkem pro koeficienty („přenásob exponentem a posuň“), na žádné limity či jinou analýznickou mašinerii nedojde.

Cvičení 9. (vlastnosti formální derivace) Mějme polynomy $P, Q \in R[x]$ a $c \in R$. Rozmysli si:

(i) Je-li P nekonstantní, pak $\deg(P') = \deg(P) - 1$,
(ii) $(c \cdot P)' = c \cdot P'$,
(iii) $(P + Q)' = P' + Q'$,
(iv) $(P \cdot Q)' = P' \cdot Q + P \cdot Q'$,
(v) (těžší) $(P(Q(x)))' = P'(Q(x)) \cdot Q'(x)$.

Povšimnout si lze také toho, že pro $P \in \mathbb{Z}[x]$ bude opět $P' \in \mathbb{Z}[x]$. Díky tomu dává smysl na takové P' následně znovu vrhnout všechnu teorii čísel, kterou jsme dosud v tomto díle vybudovali. Toho hned využijeme:

Věta. (Henselovo lemma) *Buď $Q \in \mathbb{Z}[x]$ polynom, p prvočíslo, r_1 celé číslo a $e \geq 1$ kladné celé číslo. Pokud $Q(r_1) \equiv 0 \pmod{p}$ a zároveň $Q'(r_1) \not\equiv 0 \pmod{p}$, potom existuje $r \in \mathbb{Z}$ takové, že $r \equiv r_1 \pmod{p}$ a zároveň $Q(r) \equiv 0 \pmod{p^e}$. Všechna taková r jsou si navíc navzájem kongruentní modulo p^e.*

Velice neformálně řečeno: pokud je r_1 „modulo p kořenem“ Q, ale nikoliv Q', pak už jej lze pro libovolné e zdvihnout na kořen Q modulo p^e.

Důkaz. Postupujme indukcí vzhledem ke e, pro $e = 1$ tvrzení platí triviálně. Předpokládejme, že už máme $r = r_e$ splňující tvrzení modulo p^e, a pojďme najít nové $r = r_{e+1}$, které jej splní modulo p^{e+1}. Pojďme toto zatím neznámé r_{e+1} hledat ve tvaru $r_e + tp^e$ pro zatím neznámé t. Rozmysleme si, co se pak stane s $Q(r_{e+1}) \pmod{p^{e+1}}$.

K tomu rozepišme v koeficientech $Q(x) = \sum_{k=0}^{n} a_k x^k$. Co se stane s x^k modulo p^{e+1} při dosazení r_{e+1}? Pro $k = 0$ se nestane nic, pořád budeme mít jen 1, zatímco pro $k \geq 1$ roznásobením z binomické věty dostaneme

$$(r_e + tp^e)^k = r_e^k + kr_e^{k-1}tp^e + \binom{k}{2} r_e^{k-2}t^2p^{2e} + \cdots,$$

přičemž další členy budou obsahovat jen větší a větší mocniny p. Díky $e \geq 1$ je ale $2e \geq e+1$, takže všechny členy kromě prvních dvou modulo p^{e+1} zmizí. Tedy

$$(r_e + tp^e)^k \equiv r_e^k + tp^e \cdot kr_e^{k-1} \pmod{p^{e+1}}.$$

Když toto posbíráme přes všechna k, dostaneme

$$\begin{aligned} Q(r_e + tp^e) = a_0 + \sum_{k=1}^{n} a_k (r_e + tp^e)^k \equiv a_0 + \sum_{k=1}^{n} a_k r_e^k + tp^e \cdot \sum_{k=1}^{n} k a_k r_e^{k-1} \equiv \\ \equiv Q(r_e) + tp^e Q'(r_e) \pmod{p^{e+1}}. \end{aligned}$$

Nyní už je skoro hotovo. $Q(r_e)$ už má správný zbytek, tedy nula, modulo p^e, znamená to tedy, že $Q(r_e) \equiv \ell p^e \pmod{p^{e+1}}$ pro nějaké $\ell \in \{0, 1, \ldots, p-1\}$. Potom přičítáme t-násobek $p^e Q'(r_e)$, to nás určitě bude posouvat jen mezi násobky p^e, takže nás pro výsledek modulo p^{e+1} zajímá jen to, jaký zbytek dává $tQ'(r_e)$ modulo p: vidíme, že $Q(r_{e+1}) \equiv 0 \pmod{p^{e+1}}$ nastane právě tehdy, když

$$\ell + tQ'(r_e) \equiv 0 \pmod{p}. \qquad (*)$$

Z předpokladu zadání díky $r_e \equiv r_1 \pmod{p}$ máme $Q'(r_e) \equiv Q'(r_1) \not\equiv 0 \pmod{p}$, takže k němu můžeme najít b takové, že $Q'(r_e)b \equiv 1 \pmod{p}$ (viz Cvičení 5). Když v kongruenci $(*)$ převedeme ℓ na pravou stranu a vynásobíme b, zjistíme, že $(*)$ je ekvivalentní

$$t \equiv t \cdot Q'(r_e)b \equiv -\ell b \pmod{p}.$$

S touto volbou pak tedy skutečně dostaneme $Q(r_{e+1}) \equiv 0 \pmod{p^{e+1}}$, jak jsme chtěli.

Z toho, jak jsme r_{e+1} zkonstruovali, okamžitě plyne $r_{e+1} \equiv r_e \equiv r_1 \pmod{p}$. Zbývá už jen dokázat, že pro každé jiné $\tilde{r}$, které by splňovalo $\tilde{r} \equiv r_1 \pmod{p}$ a zároveň $Q(\tilde{r}) \equiv 0 \pmod{p^{e+1}}$, už musí platit $\tilde{r} \equiv r_{e+1} \pmod{p^{e+1}}$. Takové $\tilde{r}$ by vzhledem k $Q(\tilde{r}) \equiv 0 \pmod{p^{e+1}}$ určitě splňovalo i $Q(\tilde{r}) \equiv 0 \pmod{p^e}$, tudíž bychom z indukčního předpokladu hned dostali $\tilde{r} \equiv r_e \pmod{p^e}$. Takže $\tilde{r}$ je tvaru $r_e + tp^e$, stejně jako když jsme v konstrukci výše vybírali r_{e+1}. Tam jsme ale viděli, že ke splnění $Q(r_e + tp^e) \equiv 0 \pmod{p^{e+1}}$ bylo ekvivalentně nutné $t \equiv -\ell b \pmod{p}$. Je celkem jedno, že to byl tento konkrétní zbytek, důležité je, že t bylo jednoznačně určeno modulo p. Protože se t posléze v $r_e + tp^e$ násobí s p^e, je pak celé $r_e + tp^e$ jednoznačně určeno modulo p^{e+1}, tedy $\tilde{r} \equiv r_e + (-\ell b)p^e \equiv r_{e+1} \pmod{p^{e+1}}$, jak jsme chtěli.

Důkaz indukcí je tak dokončen. □

Cvičení 10. Dokaž, že existuje celé číslo r takové, že r^2 dává zbytek -1 modulo 5^{2025}.

Úloha 10. Pro kladné celé číslo n říkejme, že polynom $Q \in \mathbb{Z}[x]$ je *bijekce modulo n*, pokud $Q(0), Q(1), \ldots, Q(n-1)$ dávají navzájem různé zbytky modulo n. Je-li p prvočíslo a Q je bijekce modulo p^2, dokaž, že je taky bijekce modulo p^3.

Závěr

Dobrá práce, dočetl(a) jsi už druhý díl letošního seriálu! Na co se můžeš těšit ve třetím a posledním díle? Podíváme se na polynomy z dalšího úhlu, totiž toho kombinatorického. Ukážeme si, jak zakódovat do světa algebry různé kombinatorické objekty a díky tomu se o nich něco dozvědět.

Hodně zdaru s úlohami 2. seriálové série a na viděnou ve třetím díle.

Návody ke cvičením

3. Vlastnost (v).

5. $p-2$.

6. 0 a r.

8. Zkus třeba zařídit, aby $Q(a) \pmod{p^2}$ bylo konstantní.

9. (i), (ii), (iii) jsou snadné. V (iv) pak stačí, když tvrzení dokážeme pro $P(x)=x^k$, $Q(x)=x^\ell$. Pro (v) pomůže rozmyslet si nejprve speciální případ $(P^k)' = kP^{k-1}P'$.

Návody k úlohám

1. Modulo 8.

2. Moc jich není – za protipříklad zkus vzít něco jako a, $a+P(a)$, jen musíš zvolit vhodné a.

3. Zvol si jedno n a následně jej posuň o $|P(n)|$.

4. Vezmi liché prvočíslo p a dokaž $p \mid P(2)$. Potom totéž zopakuj pro $P(4)$, $P(8)$, $P(16)$ atp.

5. Jedna odvěsna dělí druhou.

6. $(a-b)^2 \mid (P(a)-P(b))^2$.

7. Nahlédni, že $a^2-b^2 \mid P(a)-P(b)$ pro všechna a, b implikuje $P(x)=Q(x^2)$, pak pokračuj indukcí.

8. Bylo by to sudé celé číslo, najdi spor modulo 4.

9. Polynom s kořeny $\frac{a}{b}$, $\frac{b}{c}$, $\frac{c}{a}$.

10. Nahlédni do důkazu Henselova lemmatu – co by pro hodnoty $Q(r+tp) \pmod{p^2}$ znamenalo $Q'(r) \equiv 0 \pmod{p}$?

Řešení cvičení

1. Pokud $b=ac$, pak nutně $c=\frac{b}{a}$. Naopak když $\frac{b}{a} \in \mathbb{Z}$, pak v definici dělitelnosti můžeme zvolit $b = a \cdot \frac{b}{a}$.

2. (i): $a = 1 \cdot a$, $a = a \cdot 1$, $0 = a \cdot 0$.
(ii): $b=ak$ a $c=b\ell$, potom $c=a(k\ell)$.
(iv): $b=ak$ a $d=c\ell$, potom $bd=ac(k\ell)$.

3. Je-li $b \neq 0$, pak každé $a \mid b$ musí splňovat $|a| \leq |b|$. Tuto nerovnost ale splňuje jen konečně mnoho (konkrétně $2|b|+1$) celých čísel, takže nenulové b skutečně může mít jen konečně mnoho dělitelů.

4. Nejprve ať $b=ac$ a zapišme si $c = p_1^{\gamma_1}\cdots p_k^{\gamma_k}$ (žádná jiná prvočísla nemohou c dělit, dělila by totiž i b), potom

$$p_1^{\beta_1}\cdots p_k^{\beta_k} = b = ac = \left(p_1^{\alpha_1}\cdots p_k^{\alpha_k}\right)\left(p_1^{\gamma_1}\cdots p_k^{\gamma_k}\right) = p_1^{\alpha_1+\gamma_1}\cdots p_k^{\alpha_k+\gamma_k},$$

z čehož díky jednoznačnosti prvočíselného rozkladu plyne $\beta_i = \alpha_i + \gamma_i \geq \alpha_i$ pro všechna i.

Pokud naopak $\beta_i \geq \alpha_i$ pro všechna i, pak si můžeme označit nezáporná celá čísla $\gamma_i = \beta_i - \alpha_i$ a předepsat $c = p_1^{\gamma_1}\cdots p_k^{\gamma_k}$. Z této konstrukce okamžitě plyne $b=ac$, takže $a \mid b$.

5. Funguje vzít $b=a^{p-2}$, protože potom $ab = a^{p-1} \equiv 1 \pmod{p}$ z malé Fermatovy věty.

Alternativně se dá nahlédnout do důkazu zmíněné věty a všimnout si, že když už jsme dokázali, že v $\{a, 2a, \ldots, (p-1)a\}$ jsou zastoupeny všechny nenulové zbytky modulo p, je tam zastoupen i zbytek 1. Tedy pro některé $b \in \{1,2,\ldots,p-1\}$ (dokonce právě jedno!) bylo $ba \equiv 1 \pmod{p}$.

6. Máme $r \mid -r = 0-r \mid P(0)-P(r) = a_0 - 0 = a_0$.

7. Ve značení z věty o racionálním kořeny máme $a_n = 1$, takže kdykoliv je $\frac{u}{v} \in \mathbb{Q}$ kořen zapsaný jako zlomek v základním tvaru, pak $v \mid 1$, tedy $v = \pm 1$, a náš kořen tak je jen $\pm u \in \mathbb{Z}$.

8. Zcela nestydatě funguje třeba konstantní $Q(x) = p$. Pokud bychom nechtěli přímo takhle podvádět, můžeme vzít třeba $Q(x) = p^2x + p$.

9. Označme si vždy $P(x) = \sum_{k=0}^{n} a_k x^k$, $Q(x) = \sum_{k=0}^{n} b_k x^k$, přičemž má-li jeden z polynomů stupeň menší než n, prostě do něj doplníme členy s nulovými koeficienty. Potom:

(i) BÚNO ať $a_n \neq 0$, potom $\deg(P) = n$. Díky nekonstantnosti P je $n > 0$, takže pak je i $na_n \neq 0$. To je ale koeficient P' u x^{n-1}, přičemž žádné členy vyššího stupně P' nemá, takže $\deg(P') = n - 1$.

(ii) $(c \cdot P)'(x) = \left(\sum_{k=0}^{n} (ca_k)x^k\right)' = \sum_{k=1}^{n} kca_k x^{k-1} = c \cdot \sum_{k=1}^{n} ka_k x^{k-1} = c \cdot P'(x)$.

(iii) $(P+Q)'(x) = \left(\sum_{k=0}^{n} (a_k + b_k)x^k\right)' = \sum_{k=1}^{n} k(a_k + b_k)x^{k-1} = \sum_{k=1}^{n} ka_k x^{k-1} + \sum_{k=1}^{n} kb_k x^{k-1} = P'(x) + Q'(x)$.

(iv) Už víme, že derivace se chová dobře k součtu a násobení konstantou. Můžeme si tedy představit, že $P \cdot Q$ nejprve roznásobíme na součet jednotlivých $a_k x^k \cdot b_j x^j$. Na těchto malých kouscích snadno ověříme

$$(x^k \cdot x^j)' = (x^{k+j})' = (k+j)x^{k+j-1} = kx^{k-1} \cdot x^j + x^k \cdot jx^{j-1} = (x^k)' \cdot x^j + x^k \cdot (x^j)'.$$

Skrze předchozí dvě vlastnosti (sčítání a násobení konstantou) pak toto poskládáme zpět do $(P \cdot Q)' = P' \cdot Q + P \cdot Q'$.

(v) Opět nejprve můžeme rozepsat $P(Q(x))$ na součet jednotlivých $a_k Q(x)^k$, načež nám stačí dokazovat pouze pro $P(x) = x^k$. Pro $k = 0$ tvrzení zjevně platí, protože $P' = 0$, zatímco $P(Q(x)) = 1$, takže skutečně $1' = 0 \cdot Q'(x)$. Dále berme $k \geq 1$.

Zde využijeme indukci podle k k tomu, abychom dokázali $(Q(x)^k)' = kQ(x)^{k-1} \cdot Q'(x)$, což odpovídá dokazovanému vztahu, protože $P'(x) = kx^{k-1}$. Pro $k = 1$ tvrzení platí, protože $P(Q(x)) = Q(x)$ a $P'(x) = 1$, takže $(P(Q(x))' = Q'(x) = 1 \cdot Q'(x) = P'(Q(x)) \cdot Q'(x)$. Pro $k \geq 2$ pak zapíšeme $Q(x)^k = Q(x) \cdot Q(x)^{k-1}$, takže vzorečkem pro derivaci součinu obdržíme

$$(Q(x)^k)' = Q'(x) \cdot Q(x)^{k-1} + Q(x) \cdot (k-1)Q(x)^{k-2}Q'(x) = (1 + k - 1)Q(x)^{k-1}Q'(x),$$

jak jsme chtěli.

10. Vezměme si polynom $Q(x) = x^2 + 1$ a prvočíslo $p = 5$. Formální derivace je $Q'(x) = 2x$. Zvolíme třeba $r_1 = 2$, pak $Q(r_1) \equiv 0 \pmod{p}$, ale přitom $Q'(r_1) \equiv 4 \not\equiv 0 \pmod{p}$. Jsou splněny předpoklady Henselova lemmatu, takže už r_1 dovedeme zdvihnout na nějaké r, které splní i $Q(r) \equiv 0 \pmod{p^{2025}}$.

Řešení úloh

1. Modulo 8 se rovnice zredukuje na kongruenci $x^2 + y^2 + z^2 \equiv 7 \pmod{8}$. Jenže $x^2 \pmod{8}$ nabývá pouze zbytků 0, 1, 4 (to lze ověřit třeba vyzkoušením všech osmi možných zbytků $x \pmod{8}$) a vyzkoušením všech možných kombinací těchto tří zbytků pro x^2, y^2 a $z^2 \pmod{8}$ zjistíme, že zbytku 7 nelze docílit.

2. Jsou to právě polynomy tvaru $P(x) = \pm x^k$ pro $k \in \{0, 1, 2, \dots\}$. Že tyto vyhovují zadání je zřejmé, dokážeme tedy, že ostatní nevyhovují.

Buď tedy P polynom, který vyhovuje zadání. Zjevně $P \neq 0$. Vytkněme z P co největší mocninu x, pišme tedy $P(x) = x^k Q(x)$, kde $Q \in \mathbb{Z}[x]$ je polynom s nenulovým absolutním členem $Q(0) \neq 0$.

Všimněme si, že pokud P vyhovuje zadání, pak mu musí vyhovovat i Q. Dokážeme, že Q musí být konstantní – ať pro spor není.

Pak zvolíme a, jež je nesoudělné s $Q(0)$ (to lze, protože se jedná o nenulové číslo) a zároveň je dost velké na to, aby $|Q(a)| > 1$. Označme si pak $b = a + Q(a)$. Zaprvé, na (ne)soudělnosti jakéhokoliv celého čísla n s a se nic nezmění, když n libovolně posuneme modulo a, takže vzhledem k $b = a + Q(a) \equiv Q(a) \equiv Q(0) \pmod{a}$, což je nesoudělné s a, je i b nesoudělné s a. Tudíž by i $Q(a)$, $Q(b)$ měla být nesoudělná. Obě je však dělí $Q(a)$, protože

$$Q(b) = Q(a + Q(a)) \equiv Q(a + 0) \equiv 0 \pmod{Q(a)}.$$

Vzhledem k $|Q(a)| > 1$ to znamená, že $Q(a)$, $Q(b)$ jsou soudělná, což je spor.

Skutečně tedy Q muselo být konstantní $Q(x) = c$ pro nějaké nenulové $c \in \mathbb{Z}$. Kdyby c nebylo ± 1, pak by libovolné dvě hodnoty Q byly soudělné, což by volbou jakýchkoliv dvou nesoudělných a, b dalo spor. Nutně tedy $Q(x) = \pm 1$, což návratem zpět k P odpovídá $P(x) = \pm x^k$, jak jsme chtěli.

3. Dokážeme, že to jsou jen konstantní polynomy $P(x) = 1$ a $P(x) = -1$.

Nejprve si všimněme, že P nemůže mít kladný celočíselný kořen – kdyby jím nějaké n bylo, pak dostaneme $0 \mid n! + 2$, což je absurdní. Uvažujme dále libovolné kladné celé n. Víme, že $P(n) \mid n! + 2$. Pokud označíme $m = n + |P(n)|$, pak máme

$$P(n) \mid |P(n)| = m - n \mid P(m) - P(n),$$

takže i $P(n) \mid P(m) \mid m! + 2$. Jenomže díky $m > |P(n)|$ se ve faktoriálu $m!$ vyskytuje činitel $|P(n)|$, což způsobí $P(n) \mid m!$. Dohromady tak $P(n) \mid 2$, což je výsledek, který máme pro všechna n. Pro každé n tak musí být $P(n) \in \{-2, -1, 1, 2\}$. Kdyby nyní byl P nekonstantní, pro dost velká n bude $P(n) > 2$ (pokud má P kladný vedoucí koeficient) nebo $P(n) < -2$ (pokud má záporný vedoucí koeficient), což by dalo spor. Určitě tedy P musel být konstantní, a z $P(n) \in \{-2, -1, 1, 2\}$ je jasné, o jaké konstanty by se mohlo jednat.

Dokázali jsme tak nutnou podmínku, že P musí být jedním z konstantních polynomů -2, -1, 1 či 2. Dosazením $n = 1$ ale zjistíme, že naše konstanta by měla dělit liché číslo $1! + 2 = 3$, takže konstanty ± 2 nepřichází v úvahu. Pro ± 1 naopak bude požadovaná dělitelnost platit triviálně, takže vyhovují.

4. Ukážeme, že podmínku splňuje jen nulový polynom. Uvažujme liché prvočíslo p a libovolné kladné celé k. Malá Fermatova věta nám potom dá $2^{kp} = (2^k)^p \equiv 2^k \pmod{p}$. Dosazením $n = kp$ v zadané podmínce pak získáme

$$p \mid kp \mid P(2^{kp}),$$

takže $0 \equiv P(2^{kp}) \equiv P(2^k) \pmod{p}$. Dokázali jsme tak, že každé liché prvočíslo dělí $P(2^k)$. To už znamená, že $P(2^k) = 0$, protože každé nenulové celé číslo má jen konečně mnoho prvočíselných dělitelů, kdežto lichých prvočísel je nekonečně mnoho. To už ale znamená, že P má nekonečně mnoho kořenů (všechny mocniny dvojky), takže už to musí být nulový polynom.

5. Úloha říká, že $\sqrt{(b-a)^2 + (P(b) - P(a))^2}$ má být celé číslo, tedy že

$$c^2 = (b-a)^2 + (P(b) - P(a))^2$$

pro nějaké $c \in \mathbb{Z}$. My však víme, že $b - a \mid P(b) - P(a)$, můžeme proto označit $P(b) - P(a) = k(b-a)$ pro nějaké $k \in \mathbb{Z}$ a následně psát

$$c^2 = (b-a)^2 + k^2(b-a)^2 = (k^2+1)(b-a)^2.$$

Z toho $(b-a)^2 \mid c^2$, což implikuje $b - a \mid c$, takže $c = d \cdot (b-a)$ pro jisté $d \in \mathbb{Z}$. Tím už se rovnice zjednoduší na $d^2 = k^2 + 1$, tedy $1 = d^2 - k^2 = (d-k)(d+k)$. Jedničku lze na součin celých čísel

rozložit jen jako $1 \cdot 1$ nebo $(-1) \cdot (-1)$, takže určitě $d - k = d + k$, což implikuje $k = 0$. Když se vrátíme zpět sérií substitucí, které jsme udělali, zjistíme, že toto znamená $P(b) - P(a) = 0$ neboli $P(a) = P(b)$, takže úsečka spojující $[a, P(a)]$ a $[b, P(b)]$ skutečně byla vodorovná.

6. Čísla a, b jsou různá, takže $P(a)P(b) = -(a-b)^2 \neq 0$, takže $P(a)$ i $P(b)$ jsou nenulová. Dále díky $a - b \mid P(a) - P(b)$ máme též $(a-b)^2 \mid (P(a) - P(b))^2$, z čehož zadanou podmínkou plyne $P(a)P(b) \mid (P(a) - P(b))^2$. Na pravé straně dělitelnosti roznásobíme $P(a)^2 - 2P(a)P(b) + P(b)^2$ a můžeme se zbavit $-2P(a)P(b)$ jakožto násobku $P(a)P(b)$.

Máme tedy $P(a)P(b) \mid P(a)^2 + P(b)^2$. Dokážeme, že pro libovolná nenulová celá čísla m, n splňující $mn \mid m^2 + n^2$ už musí platit $|m| = |n|$. Pro spor ať to nějaká m, n nesplňují a vyberme si takovou dvojici (m, n), pro kterou je součet $|m| + |n|$ nejmenší možný. Zjevně musí být aspoň $1 + 1 = 2$, protože m i n jsou nenulová. Kdyby bylo $|m| + |n| = 2$, pak $|m| = |n| = 1$ a máme vyhráno, ať tedy $|m| + |n| > 2$. BÚNO tedy $|m| > 1$, takže má m nějakého prvočíselného dělitele p. Z dělitelnosti pak $p \mid mn \mid m^2 + n^2$, takže i $p \mid n^2$, protože m^2 už je násobek p. Nyní tedy n^2 obsahuje p ve svém prvočíselném rozkladu, totéž proto musí platit i pro n, tedy $p \mid n$. Můžeme proto v dělitelnosti pokrátit p^2 a získat $\frac{m}{p} \cdot \frac{n}{p} \mid \left(\frac{m}{p}\right)^2 + \left(\frac{n}{p}\right)^2$. To je opět exemplář dvojice nenulových celých čísel, která splňuje naši původní dělitelnost. Navíc když $|m| \neq |n|$, určitě i $\left|\frac{m}{p}\right| \neq \left|\frac{n}{p}\right|$. Přitom ale určitě $\left|\frac{m}{p}\right| + \left|\frac{n}{p}\right| < |m| + |n|$, takže máme spor s tím, že jsme m, n zvolili jako dvojici s tím nejmenším možným součtem $|m| + |n|$. Muselo proto skutečně platit $|m| = |n|$.

Když to aplikujeme zpět na naše $m = P(a)$, $n = P(b)$, znamená to $P(a) = \pm P(b)$. Kdyby ale $P(a) = P(b)$, bylo by $P(a)^2 = P(a)P(b) = -(a-b)^2$ kladné i záporné zároveň, což je absurdní. Proto určitě $P(a) = -P(b)$ neboli $P(a) + P(b) = 0$, jak jsme měli dokázat.

7. Ať $\mathbb{Z}^2$ značí množinu uspořádaných dvojic celých čísel. Podmnožinu $S \subseteq \mathbb{Z}^2$ nazvěme *širokou*, pokud existuje nekonečně mnoho $a \in \mathbb{Z}$, pro něž existuje nekonečně mnoho b takových, že $(a, b) \in S$.

Lemma. *Pokud polynom $P \in \mathbb{Z}[x]$ splňuje $a^2 - b^2 \mid P(a) - P(b)$ pro všechna (a, b) z nějaké široké množiny S, pak $P(x) = Q(x^2)$ pro nějaké $Q \in \mathbb{Z}[x]$.*

Důkaz. Všimněme si, že $a+b \mid a^2 - b^2$. Modulo $a+b$ máme $b \equiv -a$, takže $0 \equiv P(a) - P(b) \equiv P(a) - P(-a)$. Ze širokosti S nyní existuje nekonečně mnoho a, jež k sobě mají nekonečně mnoho b tak, aby $a+b \mid P(a) - P(-a)$. Celé číslo $P(a) - P(-a)$ tak má nekonečně mnoho dělitelů, je to tedy nula. Polynom $P(x) - P(-x)$ tedy má nekonečně mnoho kořenů, takže už $P(x) - P(-x) = 0$. V rozdílu $P(x) - P(-x)$ se ale přesně vyruší všechny členy sudých stupňů, zatímco ty lichých stupňů budou mít dvojnásobné koeficienty. Všechny členy lichých stupňů tak už musely v P mít nulové koeficienty. Můžeme tedy zapsat $P(x) = \sum_{k=0}^{n} a_{2k} x^{2k}$ a následně $P(x) = Q(x^2)$ pro $Q(x) = \sum_{k=0}^{n} a_{2k} x^k$. □

Nyní dokažme indukcí podle k: pokud $a^{2^k} - b^{2^k} \mid P(a) - P(b)$, pak $P(x) = Q\left(x^{2^k}\right)$ pro nějaké Q. Pro $k = 0$ tvrzení platí triviálně, dále tedy uvažujme $k \geq 1$ a předpokládejme, že tvrzení již platí pro $k - 1$. Máme

$$a^{2^{k-1}} - b^{2^{k-1}} \mid a^{2^k} - b^{2^k} \mid P(a) - P(b),$$

takže z indukčního předpokladu $P(x) = Q\left(x^{2^{k-1}}\right)$ pro nějaké Q. Pak vidíme, že $a^2 - b^2 \mid Q(a) - Q(b)$ pro všechna (a, b) z

$$S = \left\{ \left(a^{2^{k-1}}, b^{2^{k-1}}\right) \mid a, b \in \mathbb{Z} \right\},$$

což je zjevně široká množina, takže z lemmatu $Q(x) = R(x^2)$ pro nějaké $R \in \mathbb{Z}[x]$, načež $P(x) = R\left(x^{2^k}\right)$, jak jsme chtěli.

8. Vedoucí koeficient je 1, takže racionálním kořenem by mohlo být leda nějaké celé číslo a. Dosazením máme $a^2 + 2ma + 2n = 0$, takže speciálně musí a^2 být sudé, takže i a je sudé. Potom jsou ale a^2 i $2ma$ násobky 4, proto taktéž $4 \mid 2n$, což však neplatí, protože n je liché. Racionální kořen proto nemůže existovat.

9. Uvažujme polynom

$$P(x) = \left(x - \frac{a}{b}\right)\left(x - \frac{b}{c}\right)\left(x - \frac{c}{a}\right) = x^3 - \left(\frac{a}{b} + \frac{b}{c} + \frac{c}{a}\right) + \left(\frac{a}{c} + \frac{b}{a} + \frac{c}{b}\right)x - 1.$$

Díky zadané podmínce jsou koeficienty celočíselné, takže $P \in \mathbb{Z}[x]$. Víme, že kořeny P jsou racionální čísla $\frac{a}{b}$, $\frac{b}{c}$, $\frac{c}{a}$. Jelikož se ale jedná o polynom s vedoucím koeficientem 1, musí tyto kořeny být podle Cvičení 7 celočíselné. Jinými slovy $a \mid b$, $b \mid c$ i $c \mid a$, z čehož vyplývají nerovnosti $|a| \leq |b| \leq |c| \leq |a|$, takže $|a| = |b| = |c|$.

10. Dokažme nejprve, že $Q'(r) \not\equiv 0 \pmod{p}$ pro každé $r \in \{0, 1, \ldots, p-1\}$. Kdyby totiž $Q'(r) \equiv 0 \pmod{p}$, znamenalo by to podle jedné z kongruencí z důkazu Henselova lemmatu

$$Q(r + tp) \equiv Q(r) + tpQ'(r) \equiv Q(r) \pmod{p^2}$$

pro každé t. Takže Q by nebylo bijekce modulo p^2, protože by dalo stejnou hodnotu modulo p^2 několika různým zbytkům $r, r+p, r+2p, \ldots$, což je spor se zadáním (v případě potřeby tyto zbytky posuneme o násobek p^2 tak, aby spadly do množiny $\{0, 1, \ldots, p^2 - 1\}$.

Nyní uvažujme jakékoliv $a \in \{0, 1, \ldots, p^3 - 1\}$ a zmodulme ho modulo p. Q dává modulo p navzájem různých p zbytků, takže nabývá všech, takže pro nějaké $b \in \{0, 1, \ldots, p-1\}$ nastane $Q(b) \equiv a \pmod{p}$. Označme si dále polynom $\tilde{Q}(x) = Q(x) - a$. Od Q se liší jen o konstantní člen, takže má stejnou derivaci. Navíc je b jeho kořenem modulo p, jelikož $\tilde{Q}(b) = Q(b) - a \equiv a - a \equiv 0 \pmod{p}$. Už jsme dokázali, že $Q'(b) \not\equiv 0 \pmod{p}$, takže Henselovým lemmatem nyní dovedeme zdvihnout b na nějaké b_3, které je kořenem $\tilde{Q}$ modulo p^3. BÚNO opět vezměme toto b_3 z množiny $\{0, 1, \ldots, p^3 - 1\}$.

Takže $\tilde{Q}(b_3) \equiv 0 \pmod{p^3}$ neboli $Q(b_3) \equiv a \pmod{p^3}$. Toto jsme dokázali pro jakékoliv a, takže už víme, že v bodech $0, 1, \ldots, p^3 - 1$ nabývá Q všech p^3 různých zbytků $0, 1, \ldots, p^3 - 1$. To lze jen tehdy, pokud v každém z uvedených bodů nabývá jiného zbytku, což znamená, že Q je bijekce modulo p^3.

Výsledky po 3. podzimní sérii

	jméno	příjmení	r.	škola	1p	2p	3p	1s	celkem	hist.
1.	*Jakub*	*Trčka*	2	GKepleraPH	25	22	24	15	**86,04**	299
2.	*Alexis Théodore*	*Dachary*	3	LSG Letohrad	24	22	25	15	**85,90**	489
3.	*Lukáš*	*Komín*	2	GOpatovPH	25	20	24	15	**84,07**	84
4.	*Štěpán*	*Sikora*	0	GNadŠtolPH	24	23	23	11	**80,91**	81
5.	*Petr*	*Starý*	3	G Jírov ČB	22	21	23	15	**80,71**	81
6.	*Jakub*	*Kuchařík*	2	G Dobříš	23	21	22	14	**79,71**	80
7.	*Anna*	*Košťáková*	1	GMensaPH	22	22	21	13	**79,40**	79
8.	*Michal*	*Roček*	3	SPŠMasarLI	22	20	22	15	**79,17**	79
9.	*Tereza*	*Kubínová*	2	GLitoměřPH	22	22	23	11	**78,91**	269
10.	*Dan*	*Školař*	0	ŠkBřezová	24	23	23	9	**78,73**	79
11.–12.	*Jakub*	*Hříbal*	2	G Beroun	24	19	21	14	**78,38**	101
11.–12.	*Anna-Kristina*	*Migel*	2	SPŠSmíchov	23	21	21	14	**78,38**	78
13.	*David*	*Hytha*	4	BrooklineHS	21	23	21	13	**77,05**	114
14.	*Erik*	*Ježek*	3	SPŠSmíchov	19	20	22	15	**76,50**	623
15.	*Ondřej*	*Sedláček*	4	GOPavla PH	22	19	19	15	**76,12**	297
16.	*Svatava*	*Šimečková*	3	GJarošeBO	21	21	20	15	**75,89**	342
17.	*Veronika*	*Menšíková*	3	ArcibisGPH	22	22	19	13	**75,15**	678
18.	*Richard*	*Dobíšek*	4	GMensaPH	19	19	21	15	**73,92**	350
19.	*Ema*	*Vlková*	1	GKepleraPH	22	21	19	12	**73,70**	74
20.	*David*	*Hromádka*	4	GNadAlejPH	20	20	21	12	**73,38**	750
21.	*Mikuláš*	*Pater*	1	GKepleraPH	22	22	16	12	**72,36**	130
22.	*Dominik*	*Rigasz*	4	GJHroncaBA	15	17	25	15	**71,59**	486
23.	*Petr*	*Hanák*	3	SPŠTBatiZL	22	20	22	5	**69,69**	239
24.	*Filip*	*Říha*	3	GVoděraPH	21	20	22	6	**69,03**	69
25.	*Miriam*	*Barešová*	1	G Dobruška	15	19	19	15	**68,09**	68
26.	*Anna*	*Haltufová*	3	GKepleraPH	15	19	18	15	**66,69**	248
27.	*Anna*	*Trnková*	4	GBudějovPH	17	18	16	15	**66,25**	145
28.	*Ondřej*	*Vočka*	4	GJNerudyPH	21	23	22	–	**65,85**	152
29.	*Petra*	*Strážnická*	1	G Tišnov	19	21	17	10	**65,56**	66
30.	*Šimon*	*Komara*	1	G Grössa BA	22	14	20	8	**63,95**	162
31.	*Tereza*	*Matějková*	4	GVoděraPH	17	17	16	12	**63,31**	237
32.	*Alexander*	*Košťál*	3	GJarošeBO	22	17	17	6	**62,45**	92
33.	*Patrik*	*Štencel*	4	MendelG OP	25	–	24	11	**60,03**	528
34.	*Lucie*	*Zůnová*	4	GNVPlániPH	16	14	15	15	**60,00**	60
35.	*Lucia*	*Chladná*	4	G Grössa BA	20	20	17	4	**59,92**	275
36.	*Michal*	*Imrišek*	4	G Grössa BA	22	16	22	–	**59,84**	391
37.	*Markéta*	*Honsejková*	4	GJeronýmLI	19	19	19	3	**59,63**	416
38.	*Lucian*	*Poljak*	3	GJŠkodyPŘ	22	–	23	15	**59,30**	347
39.	*Jakub*	*Krivošík*	4	GJHroncaBA	22	13	19	4	**57,48**	232

40.	*Tomáš*	*Pazourek*	3	GJarošeBO	19	9	18	10	**56,69**	336
41.	*Adam*	*Pustka*	3	GFXŠaldyLI	19	16	20	–	**54,59**	204
42.	*Vojtěch*	*Černý*	2	GKepleraPH	22	13	19	–	**54,06**	200
43.	*Ondřej*	*Nevěřil*	3	G Zábřeh	21	11	10	13	**53,95**	303
44.	*Rudolf*	*Krzystek*	2	GNadAlejPH	19	3	20	12	**53,91**	172
45.	*Tomáš*	*Zuzík*	1	G Gröss BA	22	14	10	6	**52,34**	227
46.	*Oldřich*	*Marek*	2	GPatočkyPH	21	2	17	12	**51,58**	52
47.	*Helena*	*Muchová*	3	GKepleraPH	22	13	10	4	**49,66**	517
48.	*Petr*	*Švorc*	2	G PostupPH	17	12	13	7	**49,53**	160
49.	*Matěj*	*Bajgar*	2	G Jírov ČB	19	13	18	–	**49,36**	49
50.	*Jiří*	*Preč*	3	G UherBrod	18	14	14	4	**49,23**	386
51.	*Michail*	*Smirnov*	2	GČeskoliPH	15	10	16	7	**48,20**	165
52.	*Vít*	*Kubal*	2	G ČKrumlov	19	5	17	7	**48,12**	48
53.	*Jakub*	*Klicnar*	2	G Jírov ČB	16	12	20	–	**47,81**	59
54.	*Kateřina*	*Kučerová*	0	GHeyrovPH	21	12	12	–	**45,07**	91
55.	*Vít Jiří*	*Houfek*	2	GKepleraPH	23	11	12	–	**44,95**	72
56.	*Petr*	*Karlík*	2	GVoděraPH	21	–	18	6	**44,93**	85
57.	*Jindřich*	*Kaplický*	3	G Čelákov	17	17	11	–	**44,47**	305
58.	*Jana*	*Feldbabelová*	1	KGTřebíč	22	22	–	–	**44,31**	44
59.	*Johana*	*Štěchová*	3	GHeyrovPH	17	9	12	6	**43,83**	96
60.	*Lukáš*	*Koucký*	2	GKepleraPH	22	8	13	–	**43,13**	296
61.	*Michael*	*Jarvis*	3	GŠpitálsPH	15	6	17	5	**43,01**	170
62.	*Adam*	*Vášek*	3	G Beroun	22	21	–	–	**42,80**	43
63.	*Barbora*	*Slavíková*	2	G Vlašim	15	12	8	7	**42,51**	128
64.	*Irena*	*Bártová*	1	GKepleraPH	18	7	16	–	**40,38**	40
65.	*Eliška*	*Vimmerová*	3	G Dobříš	10	13	11	6	**40,02**	83
66.	*Vladislav*	*Bredikhin*	2	GKepleraPH	23	15	–	–	**37,80**	147
67.	*Filip*	*Urban*	4	GChodoviPH	19	7	9	–	**35,01**	124
68.	*Vojtěch*	*Fila*	4	G Litomyšl	8	10	12	5	**35,00**	35
69.	*Arne*	*Štoudek*	1	GJarošeBO	23	11	–	–	**34,80**	35
70.	*Kryštof*	*Kadlčák*	4	1ITGPH	9	13	8	4	**34,00**	34
71.	*Jan*	*Sanitrník*	1	G ČesLípa	–	15	15	3	**32,29**	32
72.	*David*	*Křemen*	4	GMHS	–	10	12	10	**32,00**	32
73.	*Veronika*	*Mašíčková*	3	PORG PH	–	13	19	–	**31,91**	298
74.	*Lada*	*Spoustová*	1	GKepleraPH	15	7	10	–	**31,68**	32
75.	*Marek*	*Valkovič*	4	GLesníZlín	16	15	–	–	**31,27**	370
76.	*Gabriela*	*Filipská*	1	GJarošeBO	19	13	–	–	**31,16**	31
77.–78.	*Eliška*	*Sysrová*	2	G Ústí n O	11	9	9	–	**29,68**	30
77.–78.	*Kristýna*	*Pospíšilíková*	2	G Příbor	9	9	11	–	**29,68**	30
79.	*Matěj*	*Hladeček*	3	1ITGPH	8	–	14	6	**28,87**	29
80.	*Samuel*	*Zubák*	0	GTomkovaOL	16	12	–	–	**28,08**	28
81.	*Rozárka*	*Michálková*	3	G Čelákov	10	10	8	–	**27,53**	217
82.	*Šimon*	*Podstavek*	3	GJHroncaBA	–	11	10	5	**26,96**	27
83.–84.	*David*	*Briet*	1	GMensaPH	15	11	–	–	**26,27**	26
83.–84.	*Alexander*	*Nalimov*	1	GMensaPH	15	11	–	–	**26,27**	26
85.	*Jana*	*Uglickich*	3	GÚstavníPH	6	8	11	–	**24,99**	79
86.	*Jan*	*Jedlička*	3	CírkGPlzeň	14	11	–	–	**24,98**	63
87.	*Daniela*	*Dobíšková*	1	PORG PH	15	10	–	–	**24,89**	25
88.	*Johana*	*Pišťáková*	2	GJarkovPH	–	15	10	–	**24,67**	178
89.	*Natálie*	*Jochová*	2	G MasNámTŘ	13	9	–	–	**22,48**	22
90.	*Michaela*	*Urbanová*	2	GFXŠaldyLI	22	–	–	–	**22,45**	153
91.	*Radim*	*Aulický*	4	GNadAlejPH	22	–	–	–	**22,09**	258

92.	*Anna*	*Lošonská*	0	GOhradníPH	4	–	8	9	**21,45**	21
93.	*Lucie*	*Bělová*	0	GOpatovPH	12	10	–	–	**21,32**	21
94.	*Tomáš*	*Černý*	1	G Grösse BA	21	–	–	–	**21,30**	21
95.	*Matúš*	*Pokorný*	3	G Grösse BA	21	–	–	–	**21,13**	231
96.–97.	*Mykhailo*	*Degtyar*	3	GJNerudyPH	21	–	–	–	**20,63**	21
96.–97.	*Jindřich*	*Heissiger*	3	GDoppleraPH	21	–	–	–	**20,63**	21
98.	*Jozef*	*Smolár*	4	GNámestovo	12	7	–	–	**18,95**	206
99.	*Martin*	*Šnejdar*	2	GKepleraPH	18	–	–	–	**17,57**	51
100.	*Tomáš*	*Havlin*	3	BiskG Brno	17	–	–	–	**17,13**	37
101.	*Lukáš*	*Lipka*	1	ŠpMNDaG BA	17	–	–	–	**16,83**	17
102.	*Noel*	*Probst*	0	PORG PH	13	4	–	–	**16,69**	17
103.	*Samuel*	*Probst*	2	PORG PH	17	–	–	–	**16,63**	61
104.	*Matyáš*	*Hazdra*	0	GNadAlejPH	16	–	–	–	**16,42**	16
105.	*Adam*	*Dedek*	3	GMensaPH	16	–	–	–	**16,36**	16
106.	*Kateřina*	*Volná*	4	MendelG OP	16	–	–	–	**16,34**	66
107.	*Patrik*	*Šenkýř*	1	G Sokolov	16	–	–	–	**15,89**	16
108.	*Kristian*	*Fukac*	3	ScotsCollegeNZ	–	11	4	–	**15,62**	16
109.	*Gabriel*	*Hamrle*	3	GKepleraPH	16	–	–	–	**15,57**	114
110.	*Simon*	*Svrček*	3	GJHroncaBA	16	–	–	–	**15,54**	117
111.	*Michal*	*Korčák*	2	GJSeiferPH	15	–	–	–	**15,05**	15
112.	*Petr*	*Vojtěch*	1	GKepleraPH	15	–	–	–	**14,89**	15
113.	*František*	*Nouza*	2	GRychnovKn	5	–	9	–	**14,75**	15
114.	*Matěj*	*Tabach*	0	GNZatlanPH	–	14	–	–	**14,27**	14
115.–116.	*Matej*	*Kucharčík*	1	ŠpMNDaG BA	14	–	–	–	**13,81**	14
115.–116.	*Martin*	*Vávra*	1	KGTřebíč	14	–	–	–	**13,81**	14
117.–118.	*Ema*	*Čekalová*	3	GBudějovPH	13	–	–	–	**13,47**	13
117.–118.	*Tomáš*	*Olšinár*	3		13	–	–	–	**13,47**	13
119.	*Samuel Gregor*	*Kalický*	3	GNadAlejPH	9	4	–	–	**12,89**	134
120.	*Anna*	*Musialková*	2	GJSeiferPH	12	–	–	–	**11,81**	24
121.	*Filip*	*Sichrovský*	3	G ČesLípa	11	–	–	–	**11,39**	11
122.	*Ella Michaela*	*Patrášová*	1	GTajBanBys	11	–	–	–	**11,38**	11
123.	*Pavel*	*Apukhtin*	3	TrojskéGPH	–	–	–	11	**11,23**	11
124.	*Alžběta*	*Reitmayerová*	0	GŠpitálsPH	4	0	6	–	**9,91**	10
125.–126.	*Michael*	*Ambros*	2	GTomkovaOL	9	–	–	–	**9,48**	9
125.–126.	*Markéta*	*Tobolová*	2	GStrážnice	9	–	–	–	**9,48**	9
127.	*Barbora*	*Salajová*	3	GLitoměřPH	3	–	–	6	**9,28**	9
128.	*Luisa*	*Troupová*	1	PORG PH	8	0	–	–	**8,48**	8
129.	*Ľudmila*	*Kvašná*	2	GSvobHumen	8	–	–	–	**8,17**	8
130.–131.	*Ondřej*	*Adamec*	4	G Trutnov	8	–	–	–	**8,00**	8
130.–131.	*Vojtěch*	*Křižan*	3	G ValMez	8	–	–	–	**8,00**	8
132.	*Martin*	*Soles*	3	SPŠMasarLI	6	–	–	–	**5,53**	6
133.–134.	*Martin*	*Grünwald*	3	G Blansko	4	0	–	–	**4,23**	4
133.–134.	*Eva*	*Martikánová*	3	MendelG OP	4	–	–	–	**4,23**	4
135.	*Petr*	*Molhanec*	4	GKepleraPH	3	–	–	–	**2,94**	11

adresa: *Matematický korespondenční seminář*
KAM MFF UK
Malostranské náměstí 25
118 00 Praha 1
web: *https://prase.cz/*
e-mail: *info@prase.cz*