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

Milý příteli,

minule jsme se s polynomy seznámili ve velmi obecné rovině[1]. 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.

[1] 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:[2]

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

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

[2]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 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, …, $p-1$ 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

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

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[3] $n = p^e$. 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[4]:

(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

[3] 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*.

[4] 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

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

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.