Polynomy 1 – Ke kořenům a zase zpátky

Milý příteli,

vítej u prvního dílu letošního seriálu, v němž budeme brouzdat světem polynomů. *Polynom*, nebo též hezky česky *mnohočlen*, je pojem, který už jsi dost možná někdy potkal(a). Schovává se za ním výraz s proměnnou x a s koeficienty $a_0, a_1, \ldots, a_n$, který může vypadat nějak takhle:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x_1 + a_0.$$

Matematiky často zajímá hledání kořenů, tedy jaká čísla za x můžeme dosadit, aby celý výraz nabyl nulové hodnoty. I nás budou kořeny na naší cestě provázet: po osvojení základních pojmů si v tomto díle ukážeme, jak s pomocí kořenů faktorizovat polynom na součin a k čemu je to dobré. Poté prozkoumáme, jak se od kořenů vrátit zpět ke koeficientům, a na úplný závěr představíme pár hezkých i špinavých triků na úlohy, v nichž hledáme neznámý polynom.

Pokud jsi potkal(a) polynomy ve škole, pravděpodobně jste jako proměnné, kořeny i koeficienty brali reálná čísla. Spousta zajímavých úloh ale vznikne tak, že místo o reálných číslech začneme přemýšlet jenom o těch celých nebo racionálních. Nebo si naopak můžeme svět reálných čísel zvětšit na komplexní čísla. Abychom podchytili co nejvíc z této rozmanitosti, budeme se teorii snažit budovat trochu obecně. Díky tomu pak budeme schopni snadno přepínat, zda zrovna hovoříme o polynomech „nad“ reálnými, celými, racionálními, … či jakýmikoliv exotičtějšími čísly.

Seriál pro Tebe letos píší Majda Mišinová, Matěj Doležálek a Tom Flídr. Zavrtá-li se Ti do hlavy při čtení jakákoliv otázka či nejasnost, neváhej se na nás obrátit na mailových adresách *magdalena.misinova@gmail.com*, *matej@prase.cz* a *tomas@flidr.name*. Přejeme příjemné čtení!

O příkladech, cvičeních a úlohách

V seriálu bychom Ti rádi pomohli procvičit si počítání a řešení úloh. V textu jsou k tomuto účelu rozesety tři druhy pomůcek. **Příklady** jsou řešené ukázky, na kterých Ti chceme osvětlit nejtypičtější metody, které se při řešení úloh hodí znát. **Cvičení** jsou zamyšlení, která by Tě měla ubezpečit v osvojení zavedených pojmů, či menší tvrzení, která je podle nás hodnotnější si nejprve zkusit sám/sama. Pokud by se Ti to nedařilo, nezoufej, na konci dílu najdeš návody k některým z nich a ještě o kousek dál řešení úplně všech. Konečně **Úlohy** jsou problémy olympiádního typu, podobně jako běžně můžeš potkat na soutěžích. Některé mohou být těžší než Cvičení, na oplátku zase ale bývají hezčí. Stejně jako cvičení jsou pak i úlohy opatřeny návody a řešeními na konci textu.

Základní definice

V tomto seriálu budeme polynomy uvažovat jen s koeficienty branými z množin, kterým říkáme *obory*. Obor je ve zkratce struktura, v níž máme význačné prvky 0 a 1 a ve které můžeme násobit, sčítat a odečítat tak, jak jsi zvyklý/zvyklá. Tím myslíme třeba to, že při sčítání nezávisí na pořadí ani na uzávorkování, že můžeme roznásobovat závorky jako $a \cdot (b+c) = ab+ac$ nebo že součin ab může být nulový, jen když je a nebo b (nebo obojí) nula. Pozor, schopnost dělit v oboru nevyžadujeme.

Příklady oborů jsou celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reálná čísla $\mathbb{R}$ nebo komplexní čísla[1] $\mathbb{C}$. Pokud by Tě během čtení seriálu pojem „obor“ znervózňoval, klidně si představuj, že je to jen některý ze $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ či $\mathbb{C}$, neboť stejné myšlenky budou povětšinou fungovat jak s jedním konkrétním oborem, tak s libovolným jiným. Pokud jsi už někdy potkal(a) modulární aritmetiku, můžeš si jako bonus pro každé prvočíslo p představovat také $\mathbb{Z}_p$ (celá čísla modulo p), neboť to je též oborem.

Definice. Je-li R obor, pak *polynomem nad* R myslíme výraz tvaru $P(x) = a_n x^n + \cdots + a_1 x + a_0$, kde n je nějaké nezáporné celé číslo a $a_0, a_1, \ldots, a_n \in R$. Množinu všech polynomů nad R v proměnné x značíme $R[x]$.

Pokud $a_n \neq 0$, nazýváme a_n *vedoucím koeficientem* polynomu P. Naproti tomu a_0 nazýváme *konstantním* nebo též *absolutním členem* polynomu P. Domluvme se také, že si v zápisu polynomů dovolíme vynechávat jedničkové koeficienty a členy s nulovým koeficientem a že záporná znaménka bude psát pomocí rozdílu: např. tedy napíšeme $x^2 - 1$ namísto striktně formálního $1x^2 + 0x + (-1)$. Podobně se domluvme, že pokud se odkážeme na koeficient s indexem větším než n, bereme, že je to nula.

Na polynomy se primárně díváme jako na výrazy s proměnnou. Přirozené je ale taky vnímat polynomy jako funkce: když máme polynom $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ a nějaký prvek $r \in R$, můžeme jej *dosadit* a získat tak nějaký nový prvek $P(r) = a_n r^n + \cdots + a_1 r + a_0 \in R$. Když napíšeme $P(x) = Q(x)$, budeme tím myslet, že P a Q mají stejné koeficienty u každé mocniny x. Pozor, to obecně není ekvivalentní s tím, že $P(r) = Q(r)$ pro každé $r \in R$. V tomto díle tuhle situaci nepotkáme, ale nad některými obory mohou existovat polynomy, které jsou různé, ale přesto dosazením libovolného prvku dávají vždy stejnou hodnotu. (Pokud si rozumíš s obory $\mathbb{Z}_p$, můžeš si rozmyslet, že x^2 a x dávají nad $\mathbb{Z}_2$ vždy stejné hodnoty, ale přesto jsou to různé polynomy.)

Definice. O $\alpha \in R$ řekneme, že je *kořenem* polynomu P, pokud $P(\alpha) = 0$. Pokud takové $\alpha \in R$ existuje, říkáme, že P *má kořen* v R.

Definice. Je-li $P \in R[x]$ polynom $P(x) = a_n x^n + \cdots + a_1 x + a_0$ a $a_n \neq 0$, pak n nazveme *stupněm* P, což značíme jako $\deg(P) = n$. Speciálně definujeme $\deg(0) = -\infty$.

Pro nízké stupně existují zažité názvy: polynom nazýváme *konstantním*, pokud má stupeň 0 nebo je nulový, *lineárním*, pokud má stupeň 1, *kvadratickým*, pokud má stupeň 2, *kubickým*, pokud má stupeň 3, atd.

Všimni si, že každé celé číslo je racionální a každé racionální číslo je reálné. Máme-li tedy polynom s celočíselnými koeficienty, můžeme ho interpretovat jako polynom nad $\mathbb{Z}$, nad $\mathbb{Q}$ i jako polynom nad $\mathbb{R}$. Podobně u polynomu nad $\mathbb{Z}$ můžeme koeficienty interpretovat jen jako zbytkové třídy modulo nějaké p a získat tak polynom nad $\mathbb{Z}_p$. Zápis bude mít pořád stejný, ale jeho vlastnosti se můžou značně lišit.

Cvičení 1. Najdi polynom s celočíselnými koeficienty takový, že

(i) má kořen v $\mathbb{Q}$, ale ne v $\mathbb{Z}$,
(ii) má kořen v $\mathbb{R}$, ale ne v $\mathbb{Q}$,
(iii) (jen pokud znáš $\mathbb{Z}_p$) má kořen v $\mathbb{R}$, ale ne v $\mathbb{Z}_5$,
(iv) (jen pokud znáš $\mathbb{Z}_p$) má kořen v $\mathbb{Z}_5$, ale ne v $\mathbb{R}$.

Úloha 1. Ať je dán nenulový polynom $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ a číslo $0 \neq r \in \mathbb{R}$, které je jeho kořenem. Najdi nějaký polynom nad $\mathbb{Q}$, jehož kořenem je $\frac{1}{r}$.

V tomto díle se budeme zabývat hlavně polynomy nad $\mathbb{R}$ (a později nad $\mathbb{C}$), v zájmu obecnosti se toho však budeme snažit co nejvíce zformulovat a dokázat nad obecným oborem.

[1] Pokud se s komplexními čísly zatím nekamarádíš, nevěš hlavu – v tomto dílu vás seznámíme.

Sumy

Polynomy typicky píšeme jako součty jejich členů. Zatím jsme pro to používali notaci s třemi tečkami, která má ale jisté nevýhody. Zabírá více místa, a hlavně není vždy jednoznačná: $3 + 5 + \cdots + 11$ může být jak součet lichých čísel od 3 do 11, tak součet prvočísel v témže rozsahu. Oba tyto problémy řeší zápis pomocí sum: máme-li výrazy $f_k, f_{k+1}, \ldots, f_n$, jejich součet můžeme napsat jako $\sum_{j=k}^{n} f_j = f_k + f_{k+1} + \cdots + f_n$. Například tedy polynom

$$a_n x^n + \cdots + a_1 x_1 + a_0 \qquad \text{můžeme napsat jako} \qquad \sum_{j=0}^{n} a_j x^j.$$

Všimni si, že v tištěné podobě se počáteční a koncový index píšou jak nad a pod sumační symbol, tak i vedle – co do významu v tom není žádný rozdíl. Abychom mohli sumami pohodlně zapisovat polynomy, domluvme se, že x^0 vždy znamená 1, jinak bychom striktně vzato při dosazování $x = 0$ dostávali nedefinovaný výraz 0^0.

Na pořadí sčítanců nezáleží a proměnná, přes kterou sčítáme, je použita pouze uvnitř sumy. Můžeme tak s podobou sumy trochu čachrovat – musíme si ale dát pozor, aby byl každý sčítanec zahrnut právě jednou. Například

$$\sum_{j=0}^{n} f_j = \sum_{j=1}^{n+1} f_{j-1} = \sum_{j=0}^{n} f_{n-j}.$$

Sčítat můžeme i přes více proměnných, to si lze představit jako sčítání hodnot zapsaných v políčkách nějaké tabulky. Sumy přes různé proměnné můžeme prohazovat, tak jako v tabulce nezáleží na tom, jestli sčítáme přes řádky, nebo přes sloupce:[2]

$$\sum_{j=1}^{n} \sum_{k=1}^{m} f_{jk} = \sum_{k=1}^{m} \sum_{j=1}^{n} f_{jk}.$$

Operace s polynomy

Když dostaneš dva polynomy, $P(x) = a_n x^n + \cdots + a_1 x_1 + a_0$ a $Q(x) = b_m x^m + \cdots + b_1 x_1 + b_0$, jsou v zásadě tři věci, které s nimi můžeš udělat:

(1) Sečíst je. Potom prostě sečteš jejich koeficienty u příslušných mocnin proměnné:

$$(P + Q)(x) = \sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j.$$

(2) Vynásobit je. Pro mocniny neznámé pak může existovat hodně způsobů, jak ji získat jakou součin členu v p a členu v q:

$$(P \cdot Q)(x) = \sum_{j=0}^{n} \sum_{k=0}^{m} a_j b_k x^{j+k} = \sum_{\ell=0}^{n+m} \left(\sum_{j=0}^{\ell} a_j b_{\ell-j} \right) x^{\ell}.$$

(3) Složit je, neboli dosadit jeden do druhého. Potom se stane něco hodně divokého, neboť budeme hodně násobit:

$$P(Q(x)) = \sum_{j=0}^{n} a_j Q(x)^j = \sum_{j=0}^{n} a_j \left(\sum_{k=0}^{m} b_k x^k \right)^j.$$

Může se zdát, že jsme občas použili nějaký nedefinovaný koeficient. Pokud nás ale zajímá koeficient na pozici vyšší, než je stupeň polynomu, řekneme prostě, že je to nula.

[2] Kdybychom zkoušeli sčítat nekonečně mnoho prvků, mohli bychom se dostat do problémů. Naštěstí je ale každý polynom součet konečně mnoha členů.

Tvrzení. (operace s polynomy a stupně) *Nechť P a Q jsou nenulové polynomy nad oborem R. Potom:*

(i) $\deg(P \cdot Q) = \deg(P) + \deg(Q)$,
(ii) $\deg(P(Q(x)) = \deg(P) \cdot \deg(Q)$,
(iii) $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$. *Pokud* $\deg(P) \neq \deg(Q)$, *pak už dokonce v předchozí nerovnosti nastane rovnost.*

Cvičení 2. Najdi nad $\mathbb{R}$ polynomy P a Q takové, že $\deg\big(P(x)+Q(x)\big) < \max\{\deg(P), \deg(Q)\}$.

Kořeny

Když dostaneme nějaký polynom, nejpřirozenější otázkou je, jaké má kořeny. S řešením kvadratické rovnice ses jistě setkal(a) ve škole, tím Tě tu proto nudit nebudeme :-). Pro polynomy vyšších stupňů je hledání kořenů výrazně těžší a pro polynomy pátého a vyššího stupně je dokonce nemožné najít formulku, která by kořeny polynomu vyjádřila pomocí jeho koeficientů. Přesto můžeme o kořenech obecného polynomu říct spoustu věcí.

Tvrzení. *Je-li R obor a $P \in R[x]$ polynom s kořenem $\alpha \in R$, pak existuje polynom $Q \in R[x]$ takový, že $P(x) = (x-\alpha) \cdot Q(x)$.*

Důkaz. Uvažujme „posunutý“ polynom $\tilde{P}(x) = P(x+\alpha)$ a označme si jeho koeficienty jako $\tilde{P}(x) = a_n x^n + \cdots + a_1 x + a_0$. Dosazením $x = 0$ se vynulují všechny členy kromě absolutního, takže získáme $a_0 = \tilde{P}(0)$. Na druhou stranu ale víme $\tilde{P}(0) = P(\alpha) = 0$, protože α je kořenem P. Člen $a_0 = 0$ nám tak zmizí a můžeme zapsat

$$\tilde{P}(x) = a_n x^n + \cdots + a_1 x = x \cdot \underbrace{\big(a_n x^{n-1} + \cdots + a_1\big)}_{=\tilde{Q}(x)},$$

kde jsme označením polynomu v poslední závorce jako $\tilde{Q}$ získali $\tilde{P}(x) = x \cdot \tilde{Q}(x)$. Nakonec ještě pojmenujme $Q(x) = \tilde{Q}(x-\alpha)$, čímž už dostaneme

$$P(x) = P((x-\alpha)+\alpha) = \tilde{P}(x-\alpha) = (x-\alpha)\tilde{Q}(x-\alpha) = (x-\alpha)Q(x). \qquad \square$$

Tvrzení. *Nenulový polynom P stupně n nad oborem R má v R nanejvýš n kořenů. Pokud má n různých kořenů $\alpha_1, \ldots, \alpha_n \in R$, pak už jej lze zapsat ve tvaru $P(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ pro nějaké $c \in R$.*

Důkaz. Budeme postupovat matematickou indukcí. Jako základní případ vyřešme $n = 0$, pak je P konstantní a nenulový, tedy $P(x) = c$ pro nějaké $0 \neq c \in R$. Automaticky tudíž P nemůže mít kořen, protože ať dosadíme cokoliv, výsledná hodnota bude c. Skutečně tak P má nanejvýš 0 kořenů, navíc jsme jej vyjádřili v odpovídajícím součinovém[3] tvaru $P(x) = c$.

Dále předpokládejme, že P je polynom stupně n a všechny polynomy stupně $n-1$ mají nejvýše $n-1$ kořenů. Pokud P nemá žádný kořen, pak už jsme vyhráli. Pokud má kořen $\alpha \in R$, pak z předchozího tvrzení platí $P(x) = (x-\alpha)Q(x)$ pro nějaký polynom Q. Stupeň P je o jedna vyšší než stupeň Q, takže Q má stupeň $n-1$, a tudíž nejvýše $n-1$ kořenů. Každý kořen P je buď α nebo kořen Q, takže P má nejvýše n kořenů. Navíc pokud P má přesně n různých kořenů, pak jich Q také musel mít $n-1$ různých, takže $Q(x) = c(x-\alpha_1)\cdots(x-\alpha_{n-1})$ pro nějaké c a kořeny $\alpha_1, \ldots, \alpha_{n-1}$. Pojmenováním $\alpha_n = \alpha$ a přidáním činitele $(x-\alpha_n)$ pak máme součinový tvar i pro $P(x)$. $\square$

Speciálním důsledkem tvrzení je, že když má polynom kořenů více, je to už nutně nulový polynom. Díky tomu můžeme poznat, jestli jsou dva polynomy P a Q stejné: jejich rozdíl má stupeň

[3] Představujeme si, že součin s nula činiteli je prostě 1.

nejvýše $\max\{\deg(P), \deg(Q)\}$ a jeho kořeny jsou argumenty, pro něž se P a Q shodují. Pokud se tedy P a Q shodují v alespoň $\max\{\deg(P), \deg(Q)\} + 1$ bodech, je jejich rozdíl nulový polynom, tedy P a Q jsou tentýž polynom. Ještě speciálněji, pokud se P a Q shodují v nekonečně mnoha bodech, pak předchozí argument funguje i bez toho, abychom něco věděli o jejich stupních.

Pojďme si to ukázat na příkladech z praxe:

Příklad. Nenulový polynom $P \in \mathbb{R}[x]$ stupně n nazveme *vteřinovým*, pokud má n různých reálných kořenů $r_1, \ldots, r_n$, a navíc pro každé $j \in \{1, \ldots, n\}$ splňuje $P(r_j + 1) = 1$. Najdi všechny vteřinové polynomy. (PraSe 39–3j–5)

Řešení. Nenulové konstantní polynomy vyhovují triviálně všechny (nemají žádné kořeny, takže podmínka „pro všechny kořeny“ automaticky platí), nadále se proto zabývejme jen nekonstantními P. Ukážeme, že mezi nimi vyhovují právě ty tvaru $P(x) = x + c$ pro $c \in \mathbb{R}$. Že všechny tyto vyhovují, je zjevné.

Uvažujme tedy nekonstantní vteřinový polynom P stupně n a označme $Q(x) = P(x+1) - P(x)$. Tvrdíme, že $Q(x)$ má stupeň $n-1$. K tomu rozepišme $P(x) = \sum_{k=0}^{n} a_k x^k$. Roznásobením závorek $(x+1)^k$ podle binomické věty[4] bude zápis polynomu $P(x+1)$ začínat

$$P(x+1) = a_n \underbrace{(x^n + nx^{n-1} + \cdots)}_{(x+1)^n} + a_{n-1} \underbrace{(x^{n-1} + \cdots)}_{(x+1)^{n-1}} + \cdots,$$

přičemž pod trojtečkami se vždy skrývají členy stupně $n-2$ či nižšího. Podobně nám začíná $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots$, takže jejich odečtením získáme

$$Q(x) = (a_n - a_n)x^n + (a_n n + a_{n-1} - a_{n-1})x^{n-1} + \cdots = n a_n x^{n-1} + \cdots$$

Jelikož a_n muselo být nenulové (protože $\deg(P) = n$), znamená to, že $\deg(Q) = n - 1$.

Nyní si ale povšimneme, že podle zadané podmínky pro každé $j \in \{1, \ldots, n\}$ platí

$$Q(r_j) = P(r_j + 1) - P(r_j) = 1 - 0 = 1.$$

Jinými slovy, polynom Q a konstantní polynom 1, jež mají oba stupeň nanejvýš $n-1$, se shodují v n různých bodech. To znamená, že už musí být totožné, tedy $Q(x) = 1$ je konstantní polynom.

Už zbývá jen vydedukovat, jak mohl vypadat původní P. Ze stupňů máme $n - 1 = \deg(Q) = \deg(1) = 0$, takže P byl lineární. Navíc jsme při důkazu $\deg(Q) = n - 1$ mimoděk odhalili, že vedoucím koeficientem Q je na_n. Vedoucí koeficient konstantního polynomu 1 je 1, takže $1 = na_n = 1 \cdot a_1$ nám prozrazuje jeden ze dvou koeficientů lineárního polynomu P. Musí tak být $P(x) = x + c$ pro nějaké $c \in \mathbb{R}$, což už jsme ověřili, že vyhovuje zadání. Našli jsme tak všechna řešení: nenulové konstanty a lineární polynomy s vedoucím koeficientem 1.

Příklad. Polynom $P \in \mathbb{R}[x]$ stupně 2024 splňuje $P(k) = \frac{1}{k}$ pro každé $k \in \{1, 2, \ldots, 2025\}$. Urči $P(2026)$.

Řešení. Uvažme polynom $Q(x) = x \cdot P(x) - 1$. Má o 1 větší stupeň než P, takže $\deg(Q) = 2025$. Zároveň pro $k \in \{1, 2, \ldots, 2025\}$ máme

$$Q(k) = kP(k) - 1 = k \cdot \frac{1}{k} - 1 = 0.$$

Nalezli jsme tak 2025 různých kořenů tohoto polynomu stupně 2025, musí se proto už jednat o všechny jeho kořeny. Navíc dostáváme součinový tvar

$$Q(x) = c(x-1)(x-2)\cdots(x-2025)$$

[4] Binomická věta říká $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$, kde $\binom{n}{k}$ jsou kombinační čísla.

pro nějaké zatím neznámé $c \in \mathbb{R}$. Toto c dopočítáme dosazením $x = 0$, dostaneme

$$Q(0) = c(-1)(-2)\cdots(-2025) = c(-1)^{2025}2025!,$$

ale zároveň $Q(0) = 0 \cdot P(0) - 1 = -1$, z čehož už plyne $c = \frac{1}{2025!}$. Víme tedy už přesně, jak vypadá $Q(x)$. Abychom se dopídili $P(2026)$, dosadíme tento argument do Q a dopočteme

$$2026 \cdot P(2026) - 1 = Q(2026) = \frac{1}{2025!}(2026-1)(2026-2)\cdot(2026-2025) = \frac{1}{2025!}\cdot 2025! = 1,$$
$$P(2026) = \frac{1+1}{2026} = \frac{1}{1013}.$$

Úloha 2. Ať jsou a, b, c navzájem různá reálná čísla. Nahlédni bez roznásobování, na co se zjednoduší součet polynomů

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

Úloha 3. Jsou dána navzájem různá reálná čísla a_1, a_2, a_3 a další reálné číslo c. Pokud víš, že řešeními rovnice

$$(x-a_1)(x-a_2)(x-a_3) = c$$

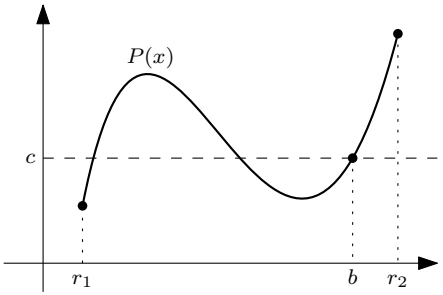
jsou tři různá $b_1, b_2, b_3 \in \mathbb{R}$, urči všechna reálná řešení rovnice

$$(x+b_1)(x+b_2)(x+b_3) = c.$$

Jeden trend, kterého si můžeš povšimnout v dosavadních tvrzeních, je to, že vždy nejprve předpokládáme, že nějaký kořen máme – obecně totiž není garantováno, že nějaký kořen existuje (to bylo k vidění ve Cvičení 1). V některých konkrétních situacích ale existenci kořenu garantovat umíme:

Cvičení 3. Každý lineární polynom nad $\mathbb{Q}$ má v $\mathbb{Q}$ kořen.

Cvičení 4. Nechť má polynom $P \in \mathbb{R}[x]$ lichý stupeň. Dokaž, že potom má P kořen v $\mathbb{R}$. (Můžeš předpokládat následující: pokud čísla $r_1, r_2, c \in \mathbb{R}$ splňují $P(r_1) \le c \le P(r_2)$, pak existuje $b \in \mathbb{R}$ splňující $P(b) = c$.)



Úloha 4. Ať mají oba $P, Q \in \mathbb{R}[x]$ stupeň 10 a vedoucí koeficient 1. Je-li známo, že rovnice $P(x) = Q(x)$ nemá reálné řešení, dokaž, že $P(x+1) = Q(x-1)$ už reálné řešení má.

Úloha 5. Uvažujme dva kubické polynomy $F, G \in \mathbb{R}[x]$ s vedoucími koeficienty 1. Dejme tomu, že rovnice

$$F(x) = 0, \qquad G(x) = 0, \qquad F(x) = G(x)$$

mají dohromady 8 různých reálných řešení. Rozhodni, zda to největší a to nejmenší z nich mohou obě být řešeními $F(x) = 0$. (PraSe 38–4p–4)

Odbočka do komplexní roviny

Nyní už dovedeme namotivovat komplexní čísla a seznámit Tě s nimi, pokud se ještě neznáte. Polynomy lichého stupně nad $\mathbb{R}$ mají vždy kořen, ty se sudým stupněm však mohou kořeny stále postrádat. Snad nejjednodušším možným příkladem je polynom $x^2 + 1$, který všude na reálné ose nabývá kladných hodnot, a proto nikde nemá kořen. Tento stav věcí matematiky raného novověku trápil natolik, až se jej rozhodli vyřešit neortodoxním způsobem – prostě si tento chybějící kořen vymysleli a začali zkoumat, k čemu dalšímu to povede.[5] Pojďme následovat jejich cestu.

Začneme tím, že prohlásíme, že existuje jakési i (říkejme mu *imaginární jednotka*), které splňuje $i^2 = -1$. To znamená, že i bude kořenem polynomu $x^2 + 1$. *Komplexními čísly* budeme rozumět čísla tvaru $a + bi$, kde $a, b \in \mathbb{R}$, a množinu všech komplexních čísel označíme $\mathbb{C}$. Podobně jako u polynomů se domluvme, že v zápise komplexních čísel dovolíme přirozená zjednodušení, např. tedy budeme psát i místo $0 + 1i$, 0 místo $0 + 0i$ či $1 - i$ místo $1 + (-1)i$.

Pojďme si rozmyslet, jak s komplexními čísly počítat, k tomu uvažujme $a + bi$ a $c + di$. Sčítání je snadné:

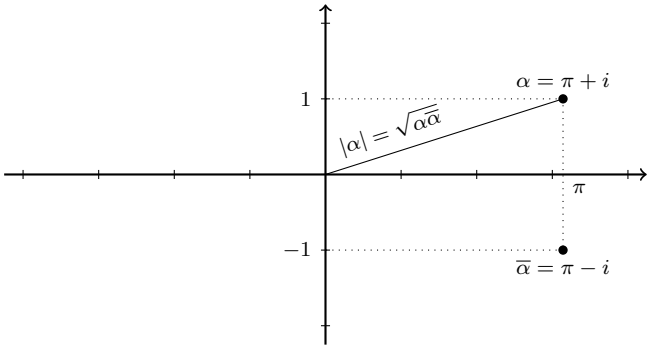
$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

podobně tak i odčítání. Při násobení dostaneme roznásobením

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2,$$

což s využitím $i^2 = -1$ zjednodušíme na $(ac - bd) + (ad + bc)i$, takže jde opět o komplexní číslo. Z hlediska úprav výrazů fungují tyto počty s komplexními čísly stejně jako počítání v reálných číslech – všechny obvyklé poučky jako komutativita[6] a asociativita[7] sčítání a násobení či roznásobování závorek zůstávají v platnosti. Teď by bylo přirozené osvětlit ještě dělení, ale to se nám prozatím vyplatí odložit a místo toho si nakreslit obrázek.

Komplexní čísla jsme zavedli jako $a + bi$ pro $a, b \in \mathbb{R}$, je tedy přirozené se na ně dívat jako na dvojice reálných čísel. Ty můžeme interpretovat jako souřadnice bodu v rovině – říkáme jí *komplexní* nebo též *Gaussova rovina*. Typicky ji kreslíme s vodorovnou, x-ovou osou reprezentující reálnou složku a svislou, y-ovou osou reprezentující imaginární složku.



Pro $\alpha = a + bi$ definujeme jeho *komplexně sdružené číslo* jako $\overline{\alpha} = a - bi$ (čti „alfa s pruhem“). V obrázku komplexní roviny to odpovídá osové souměrnosti podle reálné osy. Dále si můžeme všimnout, že

$$\alpha \cdot \overline{\alpha} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2$$

[5] Tady velice, velice zjednodušujeme, historie je o něco složitější. Prosíme, odpusť nám to :-).

[6] „Nezávisí na pořadí.“

[7] „Nezávisí na uzávorkování.“

je vždy reálné číslo. Přesněji řečeno je to dokonce druhá mocnina vzdálenosti bodu $[a, b]$ od počátku. Obvykle se proto tímto definuje absolutní hodnota komplexního čísla jako $|\alpha| = \sqrt{\alpha\overline{\alpha}} = \sqrt{a^2 + b^2}$, jež je pro každé $\alpha \neq 0$ kladná.

Cvičení 5. Ověř, že pro $\alpha, \beta \in \mathbb{C}$ platí

$$\overline{(\alpha + \beta)} = \overline{\alpha} + \overline{\beta}, \qquad \overline{(\alpha \cdot \beta)} = \overline{\alpha} \cdot \overline{\beta}.$$

Z předchozího cvičení také plyne, že $|\alpha\beta| = \sqrt{(\alpha\beta)\overline{(\alpha\beta)}} = \sqrt{\alpha\overline{\alpha}} \cdot \sqrt{\beta\overline{\beta}} = |\alpha| \cdot |\beta|$. To speciálně znamená, že $\alpha\beta = 0$ může nastat pouze tehdy, když $0 = |\alpha\beta| = |\alpha| \cdot |\beta|$, což je právě tehdy, když jedno z α, β má nulovou absolutní hodnotu neboli je nulou. S tímto posledním střípkem skládačky jsme tak oprávněni tvrdit, že $\mathbb{C}$ je obor – můžeme tedy nad $\mathbb{C}$ zvesela vypustit všechnu polynomiální mašinerii, kterou si vybudujeme.

Cvičení 6. Najdi všechny kořeny polynomu $x^4 + 1$ v komplexních číslech.

Cvičení 7. Rozmysli si, že v $\mathbb{C}$ dovedeme dělit libovolným nenulovým číslem pomocí rozšíření komplexně sdruženým číslem: $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}}$.

Zatím jsme osvětlili, *jak* pracovat v komplexních číslech, nemusí být ale stále jasné, *proč* se to vyplatí. Naše motivace započala tím, že vyrobíme kořen pro jeden konkrétní polynom. Nastává však velká magie (jejíž důkaz je bohužel nad naše možnosti) – v komplexních číslech už najednou mají kořen *všechny* (nekonstantní) polynomy. A to dokonce nejen všechny polynomy s reálnými koeficienty, ale i všechny ty, které mají komplexní koeficienty:

Věta. (základní věta algebry) *Každý nekonstantní polynom $P \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.*

Se základní větou algebry v rukou už se můžeme – alespoň když pracujeme nad $\mathbb{C}$ – zbavit podmínek stylu „*pokud* nějaký kořen existuje ...“ a vyslovit rozklad polynomů na součinový tvar bezpodmínečně:

Důsledek. *Nenulový polynom $P \in \mathbb{C}[x]$ stupně n lze zapsat ve tvaru $P(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, kde $c \in \mathbb{C}$ je vedoucí koeficient a $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ kořeny (ne nutně různé).*

Důkaz postupuje prakticky stejnou indukcí jako ve verzi, kdy jsme nad obecným oborem měli existenci kořenů jako předpoklad – nebudeme jej tu proto opakovat.

Cvičení 8. Uvažujme polynom $P \in \mathbb{R}[x]$ jako polynom nad $\mathbb{C}$. Nahlédni, že pokud je $\alpha \in \mathbb{C}$ kořenem P, pak je i $\overline{\alpha}$ kořenem P.

Úloha 6. Jsou dány polynomy $F, G, H \in \mathbb{R}[x]$ splňující rovnost

$$(x^2 + x + 1)F(x) = G(x^3) + xH(x^3).$$

Dokaž, že 1 je kořenem G i H.

Viètovy vztahy

Náš dosavadní pohled na věc nabádá k tomu, že začneme s polynomem zapsaným pomocí koeficientů a chceme najít jeho kořeny. Neméně užitečná (a navíc snazší) je však cesta opačným směrem – představujeme si, že už známe kořeny, a dopočítáváme pomocí nich koeficienty. Přesně toto zařizují tzv. *Viètovy vztahy*.

Domluvme se, že když řekneme, že polynom P *má kořeny* $r_1, \ldots, r_n$, myslíme tím, že se faktorizuje jako $P(x) = c(x - r_1)\cdots(x - r_n)$ pro nějaké c. Pointou je, že by se nemuselo jednat o n navzájem různých kořenů, některé by se mohly opakovat – včetně těchto opakování se ale dohromady nastřádá n kořenů.

Tvrzení. (Viètovy vztahy) *Mějme polynom nad komplexními čísly* $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, *který má kořeny* $r_1, r_2, \ldots, r_n$. *Pak pro každé* $k \in \{1, 2, \ldots, n\}$ *platí*

$$\sum_{1 \le j_1 < \cdots < j_k \le n} r_{j_1} \cdot r_{j_2} \cdots r_{j_k} = (-1)^k \cdot \frac{a_{n-k}}{a_n}.$$

Výraz na levé straně může vypadat děsivě, ale je to jenom sumační zápis toho, že vezmeme všechny součiny obsahující právě k různých kořenů a sečteme je. Zejména pro některé „krajní" koeficienty vypadá výsledná formulka celkem hezky: pro $k = 1$ a $k = n$ dostaneme po řadě

$$r_1 + r_2 + \cdots + r_n = -\frac{a_{n-1}}{a_n} \qquad \text{a} \qquad r_1 r_2 \cdots r_n = (-1)^n \frac{a_0}{a_n}.$$

Další zjednodušení přichází v případě $a_n = 1$: pak je absolutní člen (až na znaménko!) součinem kořenů, zatímco druhý nejvyšší koeficient je mínus součet kořenů.

Cvičení 9.

(i) Napiš si Viètovy vztahy pro polynom stupně 2 a pro polynom stupně 3.
(ii) Najdi koeficienty nějakého polynomu, jehož kořeny jsou 2, 3 a 5.

Polynom ve formulaci Viètových vztahů výše jsme vzali nad komplexními čísly, protože tam máme zajištěno, že opravdu má n kořenů. Taky je ale možné postupovat obecněji:

Cvičení 10. Zformuluj Viètovy vztahy nad libovolným oborem pro polynom stupně n s kořeny $r_1, \ldots, r_n$ v případě, že má vedoucí koeficient $a_n = 1$.

Pojďme si nyní ukázat, jak Viètovy vztahy použít v úlohách. Sice nám nepomohou v řešení polynomiální rovnice, často ale umožňují vyřešit úlohy týkající se kořenů, aniž bychom kořeny explicitně počítali.

Příklad. Označme α a β (komplexní) kořeny rovnice $2x^2 - 4x + 9 = 0$. Urči $\alpha^2 + \beta^2$.

Řešení. Víme, že $\alpha + \beta = -\left(-\frac{4}{2}\right) = 2$ a $\alpha\beta = \frac{9}{2}$. Nyní je naším úkolem vyrobit $\alpha^2 + \beta^2$ z $\alpha + \beta$ a $\alpha\beta$. K tomu si stačí uvědomit, že $(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2$, tedy

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 2^2 - 2 \cdot \frac{9}{2} = -5.$$

Na první pohled může vypadat překvapivě, že součet dvou čtverců vyšel záporně. To je ale jen tím, že α a β jsou ve skutečnosti komplexní čísla.

Příklad. Označme (komplexní) kořeny polynomu $x^3 - 3x^2 + 1$ jako α, β, γ. Najdi kubický polynom s kořeny α^2, β^2, γ^2.

Řešení. Nejprve si shrňme Viètovy vztahy pro $x^3 - 3x^2 + 1$. Pro koeficienty u x^2, x a 1 postupně dostáváme

$$\alpha + \beta + \gamma = -(-3) = 3, \qquad \alpha\beta + \beta\gamma + \gamma\alpha = 0, \qquad \alpha\beta\gamma = -1.$$

Nyní chceme pomocí těchto výrazů vyjádřit vzorečky pro α^2, β^2, γ^2. Začneme součtem kořenů, což je až na znaménko koeficient u x^2. Využijeme vztah $(\alpha+\beta+\gamma)^2 = \alpha^2+\beta^2+\gamma^2+2\alpha\beta+2\beta\gamma+2\gamma\alpha$ k vyjádření

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = 3^2 - 2 \cdot 0 = 9.$$

Následuje koeficient u x, zde podobným využitím závorky mocněné na druhou získáme

$$\begin{aligned}\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha^2\beta\gamma - 2\alpha\beta^2\gamma - 2\alpha\beta\gamma^2 = \\ &= (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = 0^2 - 2 \cdot (-1) \cdot 3 = 6.\end{aligned}$$

Konečně absolutní člen, který odpovídá součinu kořenů, což dá

$$\alpha^2\beta^2\gamma^2 = (\alpha\beta\gamma)^2 = (-1)^2 = 1.$$

Na závěr už ke spočteným výrazům musíme přidat střídající se znaménka, čímž ve výsledku dostaneme, že α^2, β^2, γ^2 jsou kořeny polynomu $x^3 - 9x^2 + 6x - 1$.

Cvičení 11. Buď $P \in \mathbb{Q}[x]$ polynom, který má v $\mathbb{C}$ kořeny $r_1, \ldots, r_n$. Pokud víš, že $r_1, \ldots, r_{n-1}$ jsou ve skutečnosti racionální, nahlédni, že i r_n musí být racionální.

Úloha 7. Jsou dána komplexní čísla a, b, c, d taková, že $a + b = c + d$ a zároveň $ab = cd$. Dokaž, že $\{a, b\} = \{c, d\}$, tedy že se jedná (možná až na pořadí) o stejné dvojice.

Úloha 8. Pokud víš, že reálná čísla $a \neq b$ splňují $a^2 + 4a + 1 = b^2 + 4b + 1 = 0$, urči $\frac{a}{b} + \frac{b}{a}$.

Úloha 9. Jsou dána $a, b, c \in \mathbb{R}$ taková, že platí nerovnosti

$$a + b + c > 0, \qquad ab + bc + ca > 0, \qquad abc > 0.$$

Dokaž, že $a, b, c > 0$.

Úloha 10. Jsou dány kvadratické polynomy $P(x)$ a $Q(x)$ takové, že $P(Q(x))$ má čtyři různé reálné kořeny $r_1 < r_2 < r_3 < r_4$. Dokaž, že $r_1 + r_4 = r_2 + r_3$. (PraSe 43–1p–4)

Úloha 11. Jsou dána $a, b, c, d \in \mathbb{R}$, z nichž alespoň jedno je nenulové. Dokaž, že polynom $x^6 + ax^3 + bx^2 + cx + d$ nemá všechny kořeny reálné.

Úloha 12. Uvažujme celá čísla $n \geq 2$ a $p, q \geq 0$. Dokaž, že pokud existuje polynom $x^n - px^{n-1} + qx^{n-2} + a_{n-3}x^{n-3} + \cdots + a_1x + a_0 \in \mathbb{C}[x]$, jehož všechny komplexní kořeny jsou nezáporná celá čísla, pak lze do roviny nakreslit p přímek protínajících se v q různých bodech.

Hledání polynomů

V olympiádě můžeš najít úlohy následujícího typu: dostaneš rovnici, v níž vystupuje nějaký neznámý polynom, případně polynomy. Tvým úkolem je pak přijít na to, které to mohou být.

Co lze s takovou úlohou dělat:

(1) Porovnat stupně. To je poměrně jednoduché a může to možná řešení značně omezit.
(2) Porovnat jednotlivé koeficienty. Nejsnadněji se typicky dopočítávají „krajní“ koeficienty, tzn. vedoucí, absolutní, lineární, ...
(3) Porovnat hodnoty v určitých bodech. Často může být šikovné dosadit kořen některého polynomu, který se v úloze vyskytuje.

Kromě těchto obecných rad můžeme nabídnout už jen přání kuráže a houževnatosti – polynomiální rovnice dovedou být rozmanité a mnohdy si v nich pořádně započítáme. Ukážeme na příkladu:

Příklad. Najdi všechny dvojice nekonstantních polynomů $P, Q \in \mathbb{R}[x]$ splňující

$$P\left(Q(x)^3\right) = x \cdot P(x) \cdot Q(x)^3.$$

(PraSe 41–4p–6)

Řešení. Připomeňme, že rovností polynomů na levé a na pravé straně myslíme to, že mají stejné koeficienty u každé mocniny x. To ale implikuje i to, že dosazením libovolného čísla dávají stejné hodnoty, což později využijeme.

Začněme porovnáním stupňů, označme $n = \deg(P)$, $m = \deg(Q)$. Jelikož hledáme nekonstantní polynomy, půjde o kladná celá čísla. Pak na levé straně máme stupeň $n \cdot 3m$, zatímco na pravé $1 + n + 3m$. Postupně upravíme

$$\begin{aligned} 3nm &= n + 3m + 1, \\ 3nm - 3m - n + 1 &= 2, \\ (3m - 1)(n - 1) &= 2. \end{aligned}$$

Máme tedy 2 rozloženo na součin dvou (nezáporných) celých čísel, což jde jen dvěma způsoby: $1 \cdot 2$ a $2 \cdot 1$. Jelikož $3m - 1 = 1$ není možné, zbývá jenom $3m - 1 = 2$ a $n - 1 = 1$ neboli $m = 1$, $n = 2$.

Nyní víme, že Q je lineární. Jakožto reálný polynom s lichým stupněm tak má nějaký reálný kořen r. Dosazením $x = r$ do zadané rovnice získáme $P(0) = P(Q(r)^3) = r \cdot P(r) \cdot Q(r)^3 = r \cdot P(r) \cdot 0^3 = 0$, takže 0 je kořenem P.

Vytkněme činitel x odpovídající tomuto kořenu, tím dostaneme $P(x) = xR(x)$ pro nějaké $R \in \mathbb{R}[x]$. Dosazením tohoto vyjádření P pak dostaneme

$$Q(x)^3 \cdot R(Q(x)^3) = x^2 \cdot R(x) \cdot Q(x)^3.$$

Pro $a \in \mathbb{R}$ různé od r je $Q(a) \neq 0$, protože Q má jen jeden kořen, takže v těchto bodech zjednodušíme $Q(a)^3 \cdot R(Q(a)^3) = a^2 \cdot R(a) \cdot Q(a)^3$ na $R(Q(a)^3) = a^2 R(a)$. Toto má platit ve všech reálných bodech kromě jednoho, tedy v nekonečně mnoha bodech, což nám umožňuje tuto rovnost zesílit na rovnost polynomů

$$R(Q(x)^3) = x^2 \cdot R(x)$$

(jinými slovy, i když jsme nejprve museli vyloučit bod $x = r$, později ho dostaneme zpátky).

Jelikož P měl stupeň 2, R musí mít stupeň 1, takže má v $\mathbb{R}$ právě jeden kořen, označme jej s. Dosazením $x = 0$ nyní dostaneme $R(Q(0)^3) = 0$, takže $Q(0)^3 = s$. Obdobně ale taky dosazením $x = s$ dostaneme $R(Q(s)^3) = s^2 R(s) = 0$, takže i $Q(s)^3 = s$. Dohromady jsme získali $Q(0)^3 = Q(s)^3$, takže také $Q(0) = Q(s)$. Označíme-li si koeficienty Q třeba jako $Q(x) = ux + v$, kde $u \neq 0$, pak už snadno vidíme, že z $u \cdot 0 + v = us + v$ plyne $0 = s$.

Odhalili jsme tedy, že kořenem R je opět 0, takže máme $R(x) = cx$ pro nějaké $0 \neq c \in \mathbb{R}$, a tedy $P(x) = cx^2$. Navíc jsme měli $Q(0)^3 = s = 0$, tedy $Q(0) = 0$. Jelikož Q bylo taktéž lineární, zbavíme se absolutního členu, čímž zbude $Q(x) = ux$. Dosazením do $R(Q(x)^3) = x^2 R(x)$ dostaneme $c(ux)^3 = x^2 \cdot cx$, z čehož porovnáním koeficientů dostaneme $cu^3 = c$, tedy $u^3 = 1$, tedy $u = 1$.

Dokázali jsme tak, že všechna řešení musí být tvaru $(P, Q) = (cx^2, x)$ pro $0 \neq c \in \mathbb{R}$. Zkouškou už ověříme, že všechny dvojice tohoto tvaru vyhovují původní rovnici:

$$P(Q(x)^3) = c(x^3)^2 = cx^6 = x \cdot cx^2 \cdot x^3 = x \cdot P(x) \cdot Q(x)^3.$$

Prochroustal(a) ses úspěšně řešením? Dobrá práce, na dalších úlohách se můžeš procvičit:

Úloha 13. Najdi všechny nenulové polynomy $P \in \mathbb{R}[x]$, jež splňují $P(x^2) = x^2(x^2 + 1)P(x)$.

Úloha 14. Najdi všechny polynomy $P \in \mathbb{R}[x]$ splňující $xP(x - 1) = (x + 1)P(x)$.

(PraSe 34–2j–3)

Úloha 15. Najdi všechny polynomy $P \in \mathbb{R}[x]$, které splňují $P(0) = 0$ a zároveň $P(x^2 + 1) = P(x)^2 + 1$.

Úloha 16. (těžká) Jsou dány polynomy $P, Q \in \mathbb{R}[x]$, jež splňují $P(Q(x)^2 + x + 1) = Q(P(x)^2 + x + 1)$. Navíc je známo, že P má nějaký reálný kořen a Q má nějaký reálný kořen. Dokaž, že potom už $P = Q$.

Závěr

Vítej na konci prvního dílu, jsme rádi, že ses dočetl(a) až sem. Ptáš se, co očekávat v díle druhém? Namísto reálné přímky či komplexní roviny zabrousíme do světa celých čísel a prozkoumáme zákoutí, kde se polynomy potkávají s teorií čísel – těšit se můžeš například na poučku „rozdíl argumentů dělí rozdíl hodnot“ či na větu o racionálním kořenu.

Přejeme hodně úspěchu při řešení úloh 1. seriálové série a těšíme se na zdárnou shledanou u druhého dílu!

Návody ke cvičením

2. Členy nejvyššího stupně se musí navzájem vyrušit.

3. Umíme dělit.

4. Dokaž, že pro dost velká kladná r je $P(r)$ kladné a pro dost malá záporná r je $P(r)$ záporné... anebo naopak.

8. $P(\overline{\alpha}) = \overline{(P(\alpha))}$.

10. Pokud $a_n = 1$, skoro nic nezmění. Jen chceme, aby sis rozmyslel(a), že kromě záruky existence kořenů jsme nepoužili nic specifického pro $\mathbb{C}$:-).

11. Součet kořenů je...?

Návody k úlohám

1. Obrať pořadí koeficientů.

2. Dosaď postupně $x = a, b, c$.

3. $(x-a_1)(x-a_2)(x-a_3) - c = (x-b_1)(x-b_2)(x-b_3)$.

4. Co se v rozdílech děje s členem stupně 9?

5. Nemůže – zkoumej, kde polynomy F, G a $F-G$ nabývají kladných a záporných hodnot.

6. Dosazuj komplexní kořeny polynomu $x^2 + x + 1$.

7. Kořeny kvadratického polynomu.

8. Viètovy vztahy pro polynom $x^4 + 4x + 1$.

9. $(x+a)(x+b)(x+c)$.

10. Dívej se na Viètovy vztahy polynomů $Q(x) - s$, kde s je kořen P.

11. Předpokládej, že všech šest kořenů $r_1, \ldots, r_6$ je reálných, a vyjádři $r_1^2 + \cdots + r_6^2$.

12. Interpretuj kořeny jako skupinky rovnoběžek.

13. Stupeň určíš snadno. Potom hledej kořeny P dosazováním takových argumentů, aby se pravá strana vynulovala.

14. Polynom $(x+1)P(x)$ má vždy stejné hodnoty v $r-1$ a r.

15. Induktivně najdi nekonečně mnoho přirozených m, pro něž $P(m) = m$.

16. Nejprve najdi bod, kde se P a Q shodují. Potom vyráběj další a další.

Řešení cvičení

1. Příkladů je mnoho, my jsme si vybrali následující: (i) $2x-1$, (ii) x^2-2, (iii) x^2-2, (iv) x^2+1.

2. Funguje např. $P(x) = x+1$ a $Q(x) = -x$, neboť pak $P(x) + Q(x) = 1$.

3. Označíme-li si polynom $ax+b$, kde $a \neq 0$, pak je $-\frac{b}{a} \in \mathbb{Q}$ kořenem.

4. Rozepišme $P(x) = \sum_{k=0}^{n} a_k x^k$, přičemž $a_n \neq 0$ a n je liché. BÚNO nechť $a_n > 0$. Nejprve si rozmyslíme, že pro nějaké dost velké r je $P(r)$ kladné, jelikož člen $a_n r^n$ „přebije“ všechny ostatní. To je intuitivně celkem zjevné, ale abychom to dokázali pořádně, budeme si muset vyhrnout rukávy – pokud by Ti následující odstavec dělal potíže, klidně se jen intuitivně smiř s tím, že člen většího stupně přebije ty menší, a pokračuj dál :-).

Postupujme třeba následovně: nejprve označme $A = \max\left\{\frac{|a_0|}{a_n}, \frac{|a_1|}{a_n}, \ldots, \frac{|a_{n-1}|}{a_n}\right\} + 1$. Potom zvolme $r = \max\{1, n \cdot A\}$. Tím následně dovedeme pro každé $k \in \{0, 1, \ldots, n-1\}$ odhadnout $|a_k r^k| < \frac{1}{n} a_n r^n$: pokud $a_k = 0$, pak to platí triviálně, a pokud $a_k \neq 0$, tak dostaneme

$$|a_k r^k| = |a_k| r^k \leq |a_k| r^{n-1} \leq r^n \cdot \frac{|a_k|}{nA} < r^n \cdot \frac{|a_k|}{n \cdot \frac{|a_k|}{a_n}} = \frac{1}{n} a_n r^n.$$

Sečtením tohoto odhadu přes nultý, první, ... , $(n-1)$-tý člen v $P(r)$ a aplikováním trojúhelníkové nerovnosti pak získáme, že vedoucí člen v absolutní hodnotě skutečně přebíjí všechny ostatní dohromady, neboť

$$\left|\sum_{k=0}^{n-1} a_k r^k\right| \le \sum_{k=0}^{n-1} |a_k r^k| < n \cdot \frac{1}{n} a_n r^n = a_n r^n.$$

Tudíž v tom nejnešťastnějším možném případě, kdy by všechny nižší členy přispívali do $P(r)$ zápornými příspěvky, dostaneme

$$P(r) = a_n r^n + \sum_{k=0}^{n-1} a_k r^k \ge a_n r^n - \left|\sum_{k=0}^{n-1} a_k r^k\right| > a_n r^n - a_n r^n = 0,$$

takže $P(r)$ je kladné.

Díky tomu, že n je liché, bude obdobně $a_n(-r)^n$ natolik malé (daleko v záporném směru na číselné ose), že ostatní členy jej nedokážou přebít, takže $P(-r)$ bude záporné. Víme tedy, že P někde nabývá záporné a někde jinde kladné hodnoty. Jelikož je to reálný polynom, musí někde mezi nabývat i nuly, a tento bod je potom naším hledaným kořenem.

5. Označme $\alpha = a + bi$ a $\beta = c + di$, pak přímočaře ověříme:

$$\overline{(\alpha+\beta)} = \overline{(a+c)+(b+d)i} = (a+c)-(b+d)i = (a-bi)+(c-di) = \overline{\alpha}+\overline{\beta},$$
$$\overline{(\alpha\cdot\beta)} = \overline{(ac-bd)+(ad+bc)i} = (ac-cd)-(ad+bc)i = (a-bi)(c-di) = \overline{\alpha}\cdot\overline{\beta}.$$

6. Jsou to všechny čtyři kombinace znamének v $\pm\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i$.

7. Je to skutečně tak, nekecali jsme. Jelikož předpokládáme $\beta \neq 0$, je $\beta\overline{\beta} = |\beta|^2$ kladné reálné číslo. Stačí tedy spočítat součin $\alpha\overline{\beta}$ a poté obě složky podělit tímto reálným číslem $|\beta|^2$.

8. Ať $P(x) = \sum_{k=0}^{n} c_k x^k$. Jelikož $c_k \in \mathbb{R}$, platí $c_k = \overline{c_k}$, takže dostaneme

$$P(\overline{\alpha}) = \sum_{k=0}^{n} c_k (\overline{\alpha})^k = \sum_{k=0}^{n} \overline{(c_k \alpha^k)} = \overline{\left(\sum_{k=0}^{n} c_k \alpha^k\right)} = \overline{(P(\alpha))} = \overline{0} = 0.$$

9. (i) Pro kvadratický polynom $P(x) = a_2x^2 + a_1x + a_0$ s kořeny r_1, r_2 dostaneme

$$r_1 + r_2 = -\frac{a_1}{a_2} \qquad \text{a} \qquad r_1 r_2 = \frac{a_0}{a_2}.$$

Pro kubický $P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ s kořeny r_1, r_2, r_3 to pak bude

$$r_1 + r_2 + r_3 = -\frac{a_2}{a_3}, \qquad r_1r_2 + r_2r_3 + r_3r_1 = \frac{a_1}{a_3}, \qquad \text{a} \qquad r_1r_2r_3 = -\frac{a_0}{a_3}.$$

(ii) Kýžené kořeny si můžeme zařídit třeba tím, že si polynom zvolíme v součinovém tvaru jako $(x-2)(x-3)(x-5)$. Roznásobením závorek, což odpovídá počítání Viètových vztahů, pak získáme

$$x^3 - (2+3+5)x^2 + (2\cdot 3 + 3\cdot 5 + 5\cdot 2)x - 2\cdot 3\cdot 5 = x^3 - 10x^2 + 31x - 30.$$

10. Můžeme zformulovat třeba takto: Ať je $P(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$ polynom nad oborem R a nechť má v R kořeny $r_1, \ldots, r_n$. Potom pro každé $k \in \{1, 2, \ldots, n\}$ platí

$$\sum_{1 \le j_1 < \cdots < j_k \le n} r_{j_1} \cdots r_{j_k} = (-1)^k a_{n-k}.$$

11. Označme $P(x) = \sum_{k=0}^{n} a_k x^k$, kde jednotlivá a_k jsou racionální. Z Viètova vztahu pro a_{n-1} máme $r_1 + \cdots + r_{n-1} + r_n = -\frac{a_{n-1}}{a_n}$, což upravíme na $r_n = -\left(r_1 + \cdots + r_{n-1} + \frac{a_{n-1}}{a_n}\right)$. V tomto výrazu jsou na pravé straně samá racionální čísla, takže i r_n je racionální.

Řešení úloh

1. BÚNO[8] předpokládejme $a_n \neq 0$. Stejně tak předpokládejme $a_0 \neq 0$, v opačném případě bychom vytknuli x a vzali za P polynom s menším stupněm.

Pak označme $Q(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Q}[x]$ polynom, který z P vznikne obrácením pořadí koeficientů. Pro $0 \neq t \in \mathbb{R}$ pak platí $Q(t) = t^n P\left(\frac{1}{t}\right)$. Speciálně tedy pro $t = \frac{1}{r}$ dostaneme $Q\left(\frac{1}{r}\right) = \frac{1}{r^n}P(r) = \frac{0}{r^n} = 0$, takže $\frac{1}{r}$ je kořenem Q.

2. Označme zadaný součet jako polynom $P(x)$. Každý ze tří sčítanců má stupeň 2, takže také $\deg(P) \leq 2$. Dosazením $x = a$ dostaneme v prvním sčítanci $\frac{(a-b)(a-c)}{(a-b)(a-c)} = 1$, zatímco v každém ze zbylých dvou sčítanců objevíme nulovou závorku $(a - a)$. Celkem tedy $P(a) = 1$ a obdobně máme též $P(b) = P(c) = 1$. Polynomy P a 1 (konstantní polynom), oba stupně nanejvýš 2, se tak shodují ve $2 + 1$ různých bodech, takže už se musí rovnat. Zjednodušíme tedy $P(x) = 1$.

3. Známe kořeny polynomu $(x-a_1)(x-a_2)(x-a_3)-c$, takže jej můžeme vyjádřit součinem jako $(x - b_1)(x - b_2)(x - b_3)$. Přesunutím c pak hned máme, že kořeny $(x-b_1)(x-b_2)(x-b_3)+c$ jsou a_1, a_2, a_3. Naše původní tři čísla jsou tak řešeními $(x - b_1)(x - b_2)(x - b_3) = -c$. Dosazením $-x$ místo x a přenásobením rovnice mínus jedničkou pak získáme přesně rovnici $(x + b_1)(x + b_2)(x + b_3) = c$, jejímiž řešeními tak jsou $-a_1$, $-a_2$, $-a_3$.

4. Podmínka o (ne)řešitelnosti rovnic nám říká, že $P(x) - Q(x)$ nemá reálný kořen. Polynom nad $\mathbb{R}$ může nemít kořen jen tehdy, když má sudý stupeň. Pokud $P(x) = x^{10} + a_9x^9 + \cdots + a_1x + a_0$ a $Q(x) = x^{10} + b_9x^9 + \cdots + b_1x + b_0$, pak nám toto speciálně říká, že v rozdílu

$$P(x) - Q(x) = (a_9 - b_9)x^9 + \cdots$$

musel zmizet člen stupně 9, takže $a_9 = b_9$. Teď už stačí jen vyvodit, že v $P(x + 1) - Q(x - 1)$ už člen stupně 9 nezmizí. K tomu spočítáme

$$\begin{aligned} P(x+1) - Q(x-1) &= \Big((x^{10} + 10x^9 + \cdots) + a_9(x^9 + \cdots) + \cdots\Big) - \\ &\quad - \Big((x^{10} - 10x^9 + \cdots) + b_9(x^9 - \cdots) + \cdots\Big) = \\ &= \Big((10 + a_9) - (-10 + b_9\Big)x^9 + \cdots = 20x^9 + \cdots \end{aligned}$$

protože $a_9 - b_9 = 0$. Díky lichému stupni tak $P(x+1) - Q(x-1)$ má reálný kořen, tedy $P(x+1) = Q(x - 1)$ má řešení.

5. Řešení $F(x) = G(x)$ jsou přesně kořeny polynomu $F - G$. Všimněme si, díky shodným vedoucím koeficientům se kubické členy v $F - G$ vyruší, takže půjde nanejvýš o kvadratický polynom. Dohromady nám naše tři rovnice tedy nemohou dát více než $3 + 3 + 2 = 8$ různých řešení. To, že máme všech osm, znamená, že už se dohromady jedná o všechny kořeny těchto polynomů a také že $F - G$ má skutečně stupeň 2 (a nikoliv nižší).

Ať je a ten nejmenší a b ten největší z kořenů. Pro spor předpokládejme, že jsou to oba kořeny F. Jelikož má G vedoucí koeficient 1, nabývá dostatečně daleko vlevo na číselné ose (v záporných číslech) záporné hodnoty. Zároveň na intervalu $(-\infty, a\rangle$ nemůže měnit znaménko, protože všechny kořeny G jsou větší než a. To znamená, že $G(a) < 0$, takže $(F-G)(a) = F(a)-G(a) = -G(a) > 0$. Taktéž $F - G$ nemůže na intervalu $(-\infty, a\rangle$ měnit znaménko, takže také všude dostatečně daleko vlevo na číselné ose nabývá kladných hodnot. Protože je $F - G$ kvadratický polynom (má sudý stupeň), znamená to, že jeho vedoucí koeficient je kladný.

Analogickou argumentací na druhé straně číselné osy zjistíme, že $G(b) > 0$, takže $(F-G)(b) < 0$, což ale implikuje, že $F - G$ má záporný vedoucí koeficient. To je spor, takže a i b nemohly být současně kořeny F.

[8] Zkratka pro „bez újmy na obecnosti“. Myslí se tím, že činíme nějaké zjednodušení nebo volbu, která nic podstatného nezmění.

6. Uvažujme komplexní kořeny polynomu x^2+x+1: dosazením snadno ověříme, že to jsou $\alpha_1 = \frac{-1+i\sqrt{3}}{2}$ a $\alpha_2 = \frac{-1-i\sqrt{3}}{2}$. Navíc to pak musí být rovnou i kořeny $(x-1)(x^2+x+1) = x^3-1$, takže $\alpha_1^3 = 1 = \alpha_2^3$. Jejich dosazením do zadané rovnosti tak pro $j \in \{1,2\}$ dostaneme $0 = G(1)+\alpha_j H(1)$. Na to se můžeme dívat jako na soustavu dvou rovnic s neznámými $G(1)$ a $H(1)$. Odečtením rovnic od sebe dostaneme $0 = (\alpha_1-\alpha_2)H(1) = i\sqrt{3}\cdot H(1)$, takže $H(1) = 0$. Z toho už pak snadno vyplývá $G(1) = 0$.

7. Uvažme $P(x) = (x-a)(x-b)$, $Q(x) = (x-c)(x-d)$. Použitím Viètových vztahů zjistíme, že P a Q mají totožný lineární koeficient $-(a+b) = -(c+d)$ i totožný absolutní člen $ab = cd$, takže už $P(x) = Q(x)$. Musí tedy mít i stejnou sadu kořenů $\{a,b\} = \{c,d\}$.

8. Chceme výraz $\frac{a}{b}+\frac{b}{a}$ vztáhnout k viètovským výrazům ab a $a+b$, čehož docílíme třeba pomocí

$$\frac{a}{b}+\frac{b}{a} = \frac{a^2+b^2}{ab} = \frac{(a+b)^2-2ab}{ab} = \frac{(a+b)^2}{ab} - 2.$$

Dosazením $a+b=-4$, $ab=1$ tak získáme $\frac{(-4)^2}{1} - 2 = 14$.

9. Uvažme polynom $P(x) = (x+a)(x+b)(x+c)$. Podle Viètových vztahů (anebo prostě roznásobením závorek) obdržíme $P(x) = x^3 + (a+b+c)x^2 + (ab+bc+ca)x + abc$. Jedná se tedy o polynom se samými kladnými koeficienty, speciálně tak dosazením jakéhokoliv $r \geq 0$ dostaneme $P(r) > 0$. Přitom ale z definice vidíme, že P má kořeny $-a$, $-b$, $-c$. Ty tak musí být záporné, což už je ekvivalentní $a,b,c > 0$.

10. Všimneme si, že P má reálný kořen $s_1 = Q(r_1)$. Rozkládá se potom tedy na $P(x) = (x-s_1)\cdot(ux+v)$ pro nějaký lineární polynom $ux+v$. Z toho pak plyne, že má P i druhý reálný kořen $s_2 = -\frac{v}{u}$. Nyní můžeme změnit úhel pohledu a na kořeny $P(Q(x))$ se dívat jako na kořeny jednoho z polynomů $Q(x)-s_1$ a $Q(x)-s_2$, načež víme, že r_1, r_2, r_3, r_4 se mezi tyto dva polynomy nějakým způsobem rozdělí do dvou dvojiček.

Jelikož však $Q(x)-s_1$ a $Q(x)-s_2$ mají stejný koeficient u x (liší se totiž jen o konstantu), znamená to, že tyto dvě dvojičky kořenů dají stejný součet. To už ale vzhledem k seřazení $r_1 < r_2 < r_3 < r_4$ jde jenom tehdy, když se spáruje nejmenší s největším a poté dva prostřední spolu, tedy $r_1 + r_4 = r_2 + r_3$.

11. Ať jsou kořeny polynomu $r_1, \ldots, r_6$. Koeficienty u x^5 a x^4 jsou nulové, což znamená

$$\sum_{k=1}^{6} r_k = 0 = \sum_{\leq j<k\leq 6} r_j r_k.$$

Díky tomu dovedeme vyjádřit

$$\sum_{k=1}^{6} r_k^2 = \left(\sum_{k=1}^{6} r_k\right)^2 - 2\left(\sum_{1\leq j<k\leq 6} r_j r_k\right) = 0^2 - 2\cdot 0 = 0.$$

Nyní pro spor předpokládejme, že všechny $r_1, \ldots, r_k$ jsou reálné. Pak máme součet čtverců několika reálných čísel nulový, což mohlo nastat jen tehdy, pokud jsou všechny nulové, tedy $r_1 = \cdots = r_6 = 0$. Pak je ale celý polynom roven x^6, což je spor s předpokladem, že alespoň jedno z a, b, c, d je nenulové.

12. Označme si kořeny $r_1, \ldots, r_n$. Vyberme si v rovině n navzájem nerovnoběžných přímek a přidejme ke každé nějaké její rovnoběžky tak, abychom nakonec v k-tém směru měli r_k rovnoběžek. Proveďme to navíc tak, aby se žádné tři z vybraných přímek neprotly v jednom bodě – kdyby se to stalo, prostě vezmeme jednu z inkriminovaných přímek a nahradíme ji za jinou rovnoběžku.

Přímek je nyní dohromady $\sum_{k=1}^{n} r_k$, což je podle Viètovách vztahů $-(-p) = p$. Průsečíky pak odpovídají dvojicím přímek z rozdílných skupinek, takže jejich celkový počet získáme posčítáním všech součinů různých r_k, což podle Viètových vztahů dá přesně q.

13. Označme $n = \deg(P)$, potom na levé straně máme stupeň $2n$ a na pravé $2 + 2 + n$, z čehož vyvodíme $n = 4$. Nyní zkusíme dosazovat: $x = 0$ vynuluje pravou stranu, takže $P(0^2) = 0$. Dále budeme chtít za x dosazovat i komplexní hodnoty – to můžeme z toho důvodu, že i kdybychom věděli jen to, že $P(x^2) = x^2(x^2 + 1)P(x)$ platí ve všech reálných bodech x, stále to znamená, že polynomy na levé a na pravé straně uvažované nad $\mathbb{C}$ mají nekonečně mnoho bodů, kde se shodují, takže už to musí být stejné polynomy i nad $\mathbb{C}$. Můžeme tedy dosadit třeba $x = i$, čímž bude na pravé straně $i^2 + 1 = 0$, takže v důsledku $P(i^2) = 0$. Dohromady jsme tak odhalili, že P má kořeny 0 a -1, takže $P(x) = x(x + 1)Q(x)$ pro nějaký $Q \in \mathbb{R}[x]$.

S tímto vyjádřením v rovnici dostaneme $x^2(x^2+1)Q(x^2) = x^2(x^2+1)x(x+1)Q(x)$. Pro všechna nenulová $a \in \mathbb{R}$ je $a^2(a^2 + 1) \neq 0$, takže v těchto bodech dostaneme

$$a^2(a^2 + 1)Q(a^2) = a^2(a^2 + 1)a(a + 1)Q(a) \qquad \Longrightarrow \qquad Q(a^2) = a(a + 1)Q(a).$$

Vzhledem k tomu, že to je rovnost v nekonečně mnoha bodech, dostáváme $Q(x^2) = x(x + 1)Q(x)$.

Nyní provedeme něco podobného ještě jednou: dosadíme $x = 0$ a $x = -1$, abychom vynulovali pravou stranu, čímž zjistíme, že 0^2 a $(-1)^2 = 1$ jsou kořeny Q. Vzhledem k $\deg(Q) = \deg(P)-2 = 2$ pak už musí být $Q(x) = cx(x-1)$ pro nějaké $0 \neq c \in \mathbb{R}$, takže $P(x) = cx(x+1)x(x-1) = cx^2(x^2-1)$. Zkouškou snadno ověříme, že všechny polynomy tohoto tvaru jsou řešeními.

14. $P(x) = 0$ zjevně funguje. Ukážeme, že žádné nenulové polynomy už nevyhovují. Označme $Q(x) = (x + 1)P(x)$. Zadání nám říká $Q(x - 1) = Q(x)$, takže pokud označíme třeba $c = Q(0)$, polynom Q nabývá této hodnoty v nekonečně mnoha bodech

$$c = Q(0) = Q(1) = Q(2) = \cdots$$

To už znamená, že $Q(x)$ a konstantní polynom c jsou totožné. To je ale možné jen pro $P = 0$, protože jinak by mělo Q stupeň $\deg(P) + 1 \geq 1$, což pro konstantu není možné.

15. Tvrdíme, že vyhovuje pouze $P(x) = x$. Že toto skutečně vyhovuje, je zjevné.

Nyní ať P splňuje podmínky zadání. Definujme posloupnost $a_0, a_1, \ldots$ pomocí $a_0 = 0$ a rekurence $a_{n+1} = a_n^2 + 1$. Snadno pozorujeme, že to je rostoucí posloupnost. Indukcí dokážeme, že každý člen splňuje $P(a_n) = a_n$. Pro $n = 0$ to platí hned ze zadání, protože $P(0) = 0$. Dále dokážeme indukční krok: pokud $P(a_n) = a_n$, pak už taky

$$P(a_{n+1}) = P(a_n^2 + 1) = P(a_n)^2 + 1 = a_n^2 + 1 = a_{n+1}.$$

Důkaz indukcí je tím hotov. Díky němu máme nekonečně mnoho různých $m \in \mathbb{R}$ splňujících $P(m) = m$. Polynom $P(x)$ a x se tak shodují v nekonečně mnoha bodech, takže musí být totožné.

16. Nejprve dokážeme, že v nějakém bodě a nastane $P(a) = Q(a)$. Máme zadáno, že P i Q mají nějaký reálný kořen, ať tedy $P(u) = 0$ a $Q(v) = 0$ pro nějaká $u, v \in \mathbb{R}$. Uvažujme polynom $R(x) = P(x)^2 - Q(x)^2$. V bodě $x = v$ má hodnotu $R(v) = P(v)^2 \geq 0$, takže R někde nabývá nezáporné hodnoty. Podobně v bodě $x = u$ dostaneme $R(u) = -Q(u)^2 \leq 0$, takže R někde nabývá taky nekladné hodnoty. „Někde mezi“ (viz Cvičení 4) už proto musí nabývat nulové hodnoty, tedy R má reálný kořen, nazvěme ho r. V něm platí $P(r)^2 = Q(r)^2$, takže když označíme $a = P(r)^2 + r + 1 = Q(r)^2 + r + 1$, dostaneme dosazením $x = r$ v zadané rovnosti, že $P(a) = Q(a)$.

Našli jsme tak jedno reálné a splňující $P(a) = Q(a)$. Teď ukážeme, že jich dokonce musí být nekonečně mnoho. Pro spor tedy předpokládejme, že jich je jen konečně mnoho. Potom si můžeme vybrat to největší z nich a označit si $b = P(a) = Q(a)$. Dosazením $x = a$ v zadané rovnici pak zjistíme, že P a Q se shodují též v $b^2 + a + 1$. Přitom ale $b^2 + a + 1 \geq a + 1 > a$, což je spor s tím, že a bylo největší číslo, kde se P a Q shodují. Takových bodů proto muselo existovat nekonečně mnoho, a tudíž $P = Q$.

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.

Polynomy 3 – Kombinatorické nahlížení

Na první pohled by se mohlo zdát, že polynomy s kombinatorikou vůbec nesouvisí. Není tomu ale tak – mnohdy se vyplatí kombinatorické objekty vzít a zakódovat do polynomu. Důvodem je, že okolo polynomů máme vybudovanou spoustu nástrojů a teorie, které je možné využít. Struktura, která by pak v čistě kombinatorické formulaci nebyla vidět, je najednou snadno vyjádřitelná.

Poznamenejme, že toto je poměrně aktivní oblast výzkumu, bohužel ty nejzajímavější výsledky jsou mimo dosah tohoto seriálu, neboť využívají právě onu polynomiální mašinerii. Ber tedy tento díl seriálu jako ochutnávku toho, jak spolu kombinatorika a polynomy můžou souviset.

Kombinační čísla

Kombinatorické problémy se často ptají na počet objektů či možností. Základním kamenem jsou *faktoriály*: $n!$ je (pro nezáporné celé číslo n) počet možností, jak seřadit n objektů. Jejich vybíráním po jednom si můžeme rozmyslet, že $n! = n \cdot (n-1) \cdots 2 \cdot 1$, protože nejdřív máme n možností, jak obsadit první pozici, poté $n-1$ možností, jak obsadit druhou pozici, atd. S touto představou vidíme, že $0! = 1$: je právě jedna možnost, jak může vypadat prázdná posloupnost.

Podobnou – a podobně zásadní – otázkou je počet možností, jak z n-prvkové množiny vybrat k-prvkovou podmnožinu (k a n jsou opět celá nezáporná čísla) – jde tedy o výběr k různých prvků bez ohledu na pořadí výběru. Tomuto počtu říkáme *kombinační číslo* a značíme jej $\binom{n}{k}$. O $\binom{n}{k}$ můžeme mluvit jako o počtu možností, jak vybrat k z n prvků, i pro $k > n$: mezi n prvky nedovedeme vybrat k různých, takže prostě $\binom{n}{k} = 0$. Podobně jako v případě faktoriálů máme právě jednu možnost, jak vybrat nula prvků (i pro $n = 0$), neboli $\binom{n}{0} = 1$. Pro $k \leq n$ je výběr těch k prvků, které do podmnožiny vezmeme, ekvivalentní výběru těch $n-k$ prvků, které nevezmeme. Díky tomu platí $\binom{n}{k} = \binom{n}{n-k}$.

Tuto rovnost můžeme nahlédnout i tím, že vyjádříme kombinační čísla pomocí faktoriálů. Předpokládejme, že $k \leq n$ a vybírejme prvky do podmnožiny postupně: první můžeme vybrat n způsoby, druhý $n-1$ způsoby, $\ldots$, k-tý $n-k+1$ způsoby. Dohromady máme $n \cdot (n-1) \cdots (n-k+1) = \frac{n!}{(n-k)!}$ možností, jak vybrat k prvků s určením pořadí. Každou k-prvkovou podmnožinu takto získáme v každém jejím možném seřazení, tedy přesně $k!$-krát. Díky tomu můžeme určit, že počet různých podmnožin, tedy neuspořádaných k-tic, je $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$.

Tento vzoreček je velmi užitečný, ale často je lepší místo něj používat původní kombinatorickou definici. To platí i pro následující tvrzení:

Tvrzení. *Pro celá nezáporná čísla n, k platí*

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}.$$

Důkaz. Kombinační číslo $\binom{n+1}{k+1}$ značí, že chceme vybrat $k+1$ prvků z $(n+1)$-prvkové množiny. Označme si jeden z těchto $n+1$ prvků, ze kterých vybíráme, jako a. Pokud vybereme a, potřebujeme vybrat dalších k prvků z n zbývajících. Máme tedy $\binom{n}{k}$ výběrů, které obsahují a. Pokud a nevybereme, potřebujeme vybrat všech $k+1$ prvků z n zbývajících. Počet výběrů, které neobsahují a, je tedy $\binom{n}{k+1}$. Součtem obou možností získáme dokazované tvrzení. □

Toto tvrzení nám společně s pozorováním, že $\binom{n}{n} = \binom{n}{0} = 1$, umožňuje kombinační čísla vizualizovat a efektivněji počítat. Uspořádejme kombinační čísla do trojúhelníku jako na obrázku vlevo (říká se mu *Pascalův trojúhelník*[1]). Díky tvrzení pak platí, že každé kombinační číslo se rovná součtu dvou čísel nad ním v předchozím řádku. Toto platí i pro krajní $\binom{n}{0}$ a $\binom{n}{n}$, pokud si představíš volná místa nalevo i napravo od trojúhelníku vyplněná nulami. Vyčíslením kombinačních čísel získáme trojúhelník napravo. Pokud Ti prvních několik řádků něco připomíná, jsi na správné stopě, přijde to na přetřes již za okamžik :-).

$$\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0}\ \binom{1}{1} \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} \\
\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}
\end{array}
\qquad
\begin{array}{c}
1 \\
1\quad 1 \\
1\quad 2\quad 1 \\
1\quad 3\quad 3\quad 1 \\
1\quad 4\quad 6\quad 4\quad 1 \\
1\quad 5\quad 10\quad 10\quad 5\quad 1
\end{array}$$

Kombinační čísla a Pascalův trojúhelník mají spoustu dalších zajímavých vlastností:

Úloha 1. (součet řádku) Nahlédni, že $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Úloha 2. (hokejková identita) Nahlédni, že pro $m \geq k$ platí $\sum_{n=k}^{m} \binom{n}{k} = \binom{m+1}{k+1}$.

Úloha 3. Kolika způsoby se z levého dolního políčka šachovnice 9×9 můžeme dostat do pravého horního rohu , pokud se v každém tahu můžeme posunout buď o dvě políčka nahoru nebo o jedno políčko doprava?

Úloha 4. Kolika způsoby můžeme rozdělit 10 bonbónů do tří různých sáčků?

Generující funkce poprvé

Hlavní myšlenka, kterou v tomto díle budeme využívat, je následující: když vezmeme posloupnost nějakých čísel (pro začátek si představuj konečnou posloupnost) a interpretujeme ji jako koeficienty polynomu, pak dovedeme komplikované úkony interpretovat jako algebraické operace, a naopak. Například posloupnost $(a_0, a_1, a_2) = (2, 3, 4)$ bude odpovídat polynomu $P(x) = a_0 + a_1 x + a_2 x^2 = 2 + 3x + 4x^2$.

Jeden klasický příklad tohoto překladu mezi kombinatorikou a algebrou jsme už v seriálu letmo potkali.[2] Je to tak základní pomůcka při úpravách výrazů, že nad ní běžně moc nepřemýšlíme. Pojďme se na ni podívat pořádně:

Věta. (binomická) *V oboru polynomů $\mathbb{C}[x]$ pro nezáporné celé číslo n platí*

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

V roli jedničky bychom samozřejmě mohli mít nějaký obecnější výraz y a vlastně bychom vůbec nemuseli mluvit o polynomech (a když už, tak ne jen nad $\mathbb{C}$), takže formulace výše je v nějakém smyslu zbytečně slabá. Pro naše účely ale bude názorné dívat se prozatím na binomickou větu jen

[1] Správně by měl pokračovat do nekonečna, ale to se nám bohužel nevešlo na stránku.

[2] Bylo to v poznámce pod čarou. Ano, přesně v takové poznámce pod čarou, jako je tahle.

jako na mocnění jednoho polynomu v proměnné x. Mimochodem, nabízí se taky dobrá mnemotechnická pomůcka: co se týče koeficientů, vypadá $(1+x)^n$ po roznásobení přesně jako n-tý řádek Pascalova trojúhelníku (když řádky číslujeme od nuly). Nyní už ale důkaz:

Důkaz. Výsledek mocnění $(1+x)^n$ určitě bude mít stupeň n, chceme proto jenom najít jeho koeficienty u 1, x, $\ldots$, x^n. Když opakovaně roznásobíme závorky v

$$\underbrace{(1+x)\cdot(1+x)\cdots(1+x)}_{n\text{-krát}},$$

dostaneme součet 2^n členů, jelikož každý odpovídá tomu, že jsme si v n závorkách nezávisle vybrali, zda si vzít 1, nebo x. Každý člen tedy odpovídá výběru nějakého (libovolného) množství prvků z $\{1, 2, \ldots, n\}$, jež označují, z kolikáté závorky jsme si vzali x (posléze jsme si z ostatních museli vzít jedničku). Jak takový člen bude vypadat? Bude to prostě x^k, kde k je počet prvků, které jsme si vybrali. Ale k prvků si můžeme vybrat přesně $\binom{n}{k}$ způsoby. To znamená, že posbíráním všech členů musíme dostat $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$. □

Myšlenka, kterou bychom Ti tu rádi prodali, zní: v polynomu $1+x$ ani v exponentu n se o kombinačních číslech, o vybírání čehokoliv odkudkoliv ani o žádné jiné kombinatorice nic nepsalo. Přesto se na pravé straně zjevila kombinační čísla. V nějakém smyslu tedy samy algebraické operace „vědí o kombinatorice“. Zde jsme tohle propojení použili tak, že nám kombinatorika vypomohla v algebře. Co kdybychom to zkusili naopak a vypůjčili si algebraická kladívka na pomoc v kombinatorice?

Příklad. Pro nezáporné celé číslo n urči $\sum_{k=0}^{n} \binom{n}{k}^2$.

Řešení. Máme sumu kombinatoricky definovaných výrazů. Existují kombinatorické způsoby, jak ji upočítat, my se ji ale namísto toho pokusíme interpretovat jako jeden koeficient nějakého polynomu. Posléze spočteme rovnou celý ten polynom a už jen přečteme kýžený koeficient.

Nejprve trik: v součinu $\binom{n}{k} \cdot \binom{n}{k}$ jedno $\binom{n}{k}$ přepíšeme na $\binom{n}{n-k}$. Tím se hodnota jednotlivých součinů ani celé sumy nezmění díky symetrii v kombinačních číslech. Poté si všimneme, že

$$\sum_{k=0}^{n} \binom{n}{k} \binom{n}{n-k}$$

nápadně připomíná výrazy, které vznikají při násobení dvou polynomů – takový součin dvou polynomů vypadá obecně takhle:

$$\left(\sum_{i=0}^{u} a_i x^i\right) \cdot \left(\sum_{j=0}^{v} b_j x^j\right) = \sum_{n=0}^{u+v} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

(dívej se na závorku před x^n). Hledanou sumu proto lze interpretovat jako koeficient u x^n v součinu $\sum_{i=0}^{n} \binom{n}{i} x^i$ s $\sum_{j=0}^{n} \binom{n}{j} x^j$. Oba tyhle činitele jsou podle binomické věty rovny $(1+x)^n$, takže hledáme koeficient u x^n v

$$(1+x)^n \cdot (1+x)^n = (1+x)^{2n},$$

což po dalším použití binomické věty dává $\binom{2n}{n}$.

Úloha 5. Pro kladné celé číslo n urči $\sum_{k=0}^{n} (-1)^k \binom{n}{k}^2$.

Úloha 6. (zobecnění příkladu) Pro nezáporná celá čísla a, b, n urči $\sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k}$.

Úloha 7. (těžší) Pro kladné celé číslo n urči $\sum_{k=0}^{n} k\binom{n}{k}$.

Zde bys mohl(a) namítnout, že předchozí sumy lze úspěšně zdolat i některou z ryze kombinatorických metod, třeba počítáním dvěma způsoby[3]. Dobrá tedy, zkusme další ukázku.

[3]Pokud jej neznáš, lze se mu přiučit třeba v tomto příspěvku: *https://prase.cz//library/DvojiPocitaniFC/DvojiPocitaniFC.pdf*.

Příklad. *Hrací kostkou* rozumějme zařízení, které má šest kladných celých čísel (mohou se opakovat) a které při hodu vrátí jednu z těchto hodnot, každou se stejnou pravděpodobností. *Standardní* hrací kostka je ta s čísly $1, \ldots, 6$. Rozhodněte, zdali existují jiné hrací kostky A, B takové, že součet hodu A a hodu B se chová stejně jako součet hodů dvěma standardními kostkami. (Tím rozumíme, že se objevují ty samé hodnoty, stejně často.)

Řešení. Možné výsledky hodu jednou standardní kostkou zakódujeme jako polynom $x+x^2+x^3+x^4+x^5+x^6$, to znamená, že čísla $1, \ldots, 6$ (v roli exponentů) jsou na kostce zastoupena každé jednou (koeficienty 1 u příslušných členů), zatímco všechna ostatní čísla nulakrát. Když hodíme dvěma kostkami, sadu možných součtů získáme popárováním možných hodů na jednotlivých kostkách, každý s každým, a sečtením. Popárování každého s každým a sečtení je ale přesně to, co se děje s exponenty $x^i \cdot x^j = x^{i+j}$, když roznásobujeme dva polynomy.

Možné součty při hodu dvěma standardními kostkami, včetně četností, tak můžeme přečíst ze součinu polynomů $(x + x^2 + x^3 + x^4 + x^5 + x^6) \cdot (x + x^2 + x^3 + x^4 + x^5 + x^6)$. Stejný princip bude fungovat pro hypotetické hrací kostky A, B, pokud si je zakódujeme každou svým polynomem a tyto polynomy znásobíme. Algebraický překlad je tedy následovný: dovedeme polynom $(x + x^2 + x^3 + x^4 + x^5 + x^6)^2$ rozložit na součin dvou polynomů, které

- mají za koeficienty nezáporná celá čísla (četnost čehokoliv dává smysl jen nezáporná),
- mají koeficienty se součtem 6 (hrací kostka má šest čísel)
- mají nulový absolutní člen (hrací kostka má mít kladná čísla, takže zakazujeme nenulový koeficient u x^0)

jinak než přímočarým způsobem $(x + x^2 + x^3 + x^4 + x^5 + x^6) \cdot (x + x^2 + x^3 + x^4 + x^5 + x^6)$?

Polynom standardní kostky si rozložíme na součin

$$x + x^2 + x^3 + x^4 + x^5 + x^6 = x(x+1)(x^2+x+1)(x^2-x+1),$$

takže

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^2 = x^2(x+1)^2(x^2+x+1)^2(x^2-x+1)^2.$$

Tyto činitele bychom chtěli rozdělit na dva dílčí součiny $A(x)$ a $B(x)$ tak, aby se každý roznásobil na polynom, který kóduje hrací kostku. Zde už lze v principu postupovat zkoušením konečně mnoha možností, ale můžeme si ještě trochu pomoct. Zaprvé, dva činitele x rozdělíme jeden do A a druhý do B, abychom si zajistili nulové absolutní členy. Zadruhé, potřebujeme, aby $A(1) = B(1) = 6$ (součet koeficientů), přitom faktory v součinu výše mají při dosazení $x = 1$ hodnoty $1 + 1 = 2$, $1^2 + 1 + 1 = 3$ a $1^2 - 1 + 1 = 1$. To naznačuje, že i dvojice činitelů $(x + 1)$ a $(x^2 + x + 1)$ musíme dát od sebe, zatímco s $(x^2 - x + 1)$ můžeme zkusit hýbat.

S touto malou nápovědou narazíme na rozdělení

$$A(x) = x(x+1)(x^2+x+1) = x + 2x^2 + 2x^3 + x^4,$$
$$B(x) = x(x+1)(x^2+x+1)(x^2-x+1)^2 = x + x^3 + x^4 + x^5 + x^6 + x^8,$$

což kóduje kostky s čísly $(1, 2, 2, 3, 3, 4)$ a $(1, 3, 4, 5, 6, 8)$. Pokud ještě stoprocentně nedůvěřujeme překladu mezi kombinatorikou a algebrou, můžeme zkouškou ověřit, že tyto dvě kostky skutečně dávají stejnou sadu součtů jako dvě standardní kostky, ale formálně to není nutné – algebraická úloha se součiny polynomů je zcela ekvivalentní té kombinatorické s kostkami.

Úloha 8. Konečnou množinu celých čísel nazvěme *sudou*, pokud je sudý součet jejích prvků. Urči, kolik má $\{1, 2, \ldots, n\}$ pro kladné celé n sudých podmnožin.

Úloha 9. (těžká) Je dána konečná množina nezáporných celých čísel S_0. Dále pro každé $n \geq 0$ je S_{n+1} tvořena těmi celými čísly a, pro něž právě jedno z a, $a - 1$ leží v S_n. Dokaž, že existuje nekonečně mnoho n, pro něž je $S_n = S_0 \cup \{a + n \mid a \in S_0\}$.

Mocninné řady

Už jsme viděli, že převedení posloupnosti na polynom nám umožňuje „automatizovat“ kombinatorické kroky do algebraických operací. Omezující však je, že toto umíme provést jen s konečnou posloupností. Jistě, nekonečnou posloupnost bychom mohli zkusit aproximovat pomocí stále delších a delších konečných kusů, ale to nezní moc jako zábava. Namísto toho si rozšíříme náš algebraický arzenál o „polynomy s nekonečně mnoha členy“.

Říká se jim *mocninné řady*. Musíme Tě však hned varovat: v mnohém se chovají dost jinak než obyčejné polynomy a některé operace s nimi si bez velkých kusů vysokoškolské mašinerie nemůžeme dovolit. Základní mantrou pro nás bude, že nedává smysl sečíst (či znásobit či cokoliv) nekonečně mnoho čísel do jednoho výsledku.[4] Naproti tomu provést nekonečně mnoho konečných součtů (či součinů či čehokoliv) naráz je zcela v pořádku.

Pro konkrétnost zde budeme pracovat jen nad komplexními čísly. Vesměs vše, co v tomto díle řekneme, bude fungovat i nad $\mathbb{R}$ nebo nad $\mathbb{Q}$, takže pokud Ti ještě komplexní čísla nepřirostla dostatečně k srdci, klidně si místo nich představuj ta reálná či racionální.

Definice. *(Formální) mocninnou řadou* (nad $\mathbb{C}$) budeme rozumět výraz tvaru

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{k=0}^{\infty} a_k x^k,$$

kde *koeficienty* $a_0, a_1, a_2, \ldots$ představují posloupnost komplexních čísel. Množinu všech mocninných řad budeme značit $\mathbb{C}[[x]]$.

Všimni si, že každý polynom je taky mocninná řada – prostě si představíme, že u všech členů vyšších než stupeň jsou koeficienty nula. Můžeme tedy psát $\mathbb{C}[x] \subset \mathbb{C}[[x]]$, speciálně jednotlivá komplexní čísla z si můžeme představovat jako konstantní řady $z + 0x + 0x^2 + \cdots$ Na rozdíl od polynomů si ale nedovolíme do mocninných řad dosazovat – to by totiž znamenalo sečíst nekonečně mnoho věcí, což jsme si zakázali. Proto ani žádné z poznatků o kořenech nebudou mít v našich mocninných řadách analogii. Taktéž nemá moc smysl hovořit o „stupni“ obecné mocninné řady.

Pojďme s mocninnými řadami taky počítat. Sčítání je snadné, sečteme koeficient po koeficientu:

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) + \left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty} (a_k + b_k) x^k.$$

Všimni si, že tohle neodporuje mantře zformulované výše – provedli jsme sice nekonečně mnoho součtů, ale každý z nich je jen konečný.

Násobení se může zdát na první pohled děsivé, ale neliší se moc od násobení polynomů – roznásobíme „každý s každým“ a posbíráme členy stejného stupně. Klíčem je, že ačkoliv máme po roznásobení nekonečnou hromadu členů, těch s x^k je jen konečně mnoho (pro každé k), protože $x^i \cdot x^j = x^k$ dává smysl jen pro $i, j \leq k$. V zápisu sumami proto bude součin mocninných řad vypadat naprosto stejně jako ten pro polynomy, jen takto posbíráme nekonečně mnoho výsledných koeficientů:

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j}\right) x^k.$$

I toto je pro nás v pořádku, protože každý jednotlivý koeficient je výsledkem nějakého konečného výpočtu.

Zkus si to na příkladu:

Cvičení 1. Označme $F(x) = \sum_{k=0}^{\infty} x^k$. Vyjádři koeficienty řady $F(x)^2$.

[4] Přes toto omezení se dá přenést s pomocí matematické analýzy. To je mocná, ale taky nebezpečná zbraň a při neopatrném zacházení bychom si s ní snadno ublížili, proto se jí vyhneme.

Cvičení 2. Nahlédni, že součin dvou nenulových mocninných řad je opět nenulová mocninná řada. To speciálně znamená, že $\mathbb{C}[[x]]$ obor (ve smyslu, který jsme používali v prvním díle).

Ilustrujme na první pohled zvláštní jevy, které se při násobení mocninných řad mohou dít. V součinu

$$(1-x)\cdot\left(1+x+x^2+x^3+x^4+\cdots\right) = \left(1+x+x^2+x^3+x^4+\cdots\right) + \\ + \left(-x-x^2-x^3-x^4-\cdots\right)$$

se nám skoro všechny členy vyruší (v koeficientech se nasbírá $1-1=0$) a zbude jen konstantní jednička. To je celkem v rozporu s intuicí pro polynomy – nekonstantní polynom by se neměl umět znásobit s čímkoliv na konstantu. Součin výše je ale naprosto validní. Když trochu přimhouříme oči, znamená to, že násobit řadou $1+x+x^2+x^3+x^4+\cdots$ je totéž jako „dělit“ polynomem $1-x$. (Anebo též naopak, „dělit“ řadou $1+x+x^2+x^3+x^4+\cdots$ je totéž jako násobit polynomem $1-x$.) Z tohoto důvodu si dovolíme psát

$$1+x+x^2+x^3+x^4+\cdots = \sum_{k=0}^{\infty} x^k = \frac{1}{1-x}.$$

Mějme ale na paměti, že do řady na levé straně si nepovolujeme dosazovat. Naproti tomu na $\frac{1}{1-x}$ můžeme nahlížet jako na „zlomek polynomů“. Výrazům $\frac{P(x)}{Q(x)}$, kde $P, Q \in \mathbb{C}[x]$, $Q \neq 0$ jsou polynomy, se učeně říká *racionální funkce*. Do těch v principu dosadit $x = a$ pro nějaké $a \in \mathbb{C}$ umíme, pokud tedy zrovna nebude a kořenem Q, což by vedlo na dělení nulou. Občas se nám proto bude hodit, když skrze úpravy mocninných řad nakonec vyrobíme rovnost racionálních funkcí – do těch pak můžeme zkusit dosazovat, anebo se rozšířením zbavit jmenovatelů a pracovat čistě s polynomy. Když se nám mocninnou řadu s koeficienty $a_0, a_1, a_2, \ldots$ podaří vyjádřit jako racionální funkci $R(x)$, nazveme ji *generující funkcí* posloupnosti $(a_0, a_1, a_2, \ldots)$.[5]

Příklad s $1+x+x^2+x^3+x^4+\cdots$ ukazuje, že některými řadami „jde dělit“ v tom smyslu, že se umí s jinou řadou znásobit na jedničku. Ukazuje se, že to není až tak neobvyklá vlastnost:

Definice. Řekneme, že mocninná řada $F(x)$ je *invertibilní*, pokud existuje $G \in \mathbb{C}[[x]]$ taková, že $F(x)\cdot G(x) = 1$.

Tvrzení. *Mocninná řada $F = \sum_{n=0}^{\infty} a_n x^n$ je invertibilní právě tehdy, když $a_0 \neq 0$.*

Důkaz. Označme si neznámou řadu $G(x) = \sum_{k=0}^{\infty} b_k x^k$. Koeficienty součinu $F(x)\cdot G(x)$ budou

$$\sum_{j=0}^{k} a_j b_{k-j}.$$

V jednom směru je tvrzení snadné: pokud $F(x)\cdot G(x) = 1$, pak speciálně koeficient u x^0 musí být $a_0 b_0 = 1$, takže a_0 nesmělo být nulové.

V opačném směru předpokládejme $a_0 \neq 0$ a navolme koeficienty b_k tak, aby se první koeficient stal jedničkou a všechny ostatní nulami. Máme zadáno $a_0 \neq 0$, takže dává smysl zvolit $b_0 = \frac{1}{a_0}$, což už zajistí koeficient 1 v členu stupně 0. Další b_k navolíme postupně v závislosti na předešlých: vždy předepíšeme

$$b_k = -\frac{1}{a_0}\sum_{j=1}^{k} a_j b_{k-j}.$$

[5] Obecněji se dá v roli generujících funkcí pracovat i s jinými než racionálními funkcemi, je to ale technicky náročnější, proto se v tomto seriálu omezíme jen na racionální funkce.

To dává smysl, protože a_0 není nula a pravá strana se odkazuje jen na $b_0, b_1, \dots, b_{k-1}$, která už jsou zvolena. Přitom poslední rovnost je po přeuspořádání přesně $\sum_{j=0}^{k} a_j b_{k-j} = 0$. Tedy zbude úvodní jednička a všechny ostatní koeficienty součinu se vynulují. □

Vztah $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$ můžeme zobecnit a najít řady i pro racionální funkce jako $\frac{1}{(1-x)^2}$, $\frac{1}{(1-x)^3}$, apod. Dostaneme tím řadu s kombinačními čísly – jinou než tu z binomické věty – která se bude později celkem hodit.

Tvrzení. *Pro nezáporné celé číslo d platí* $\frac{1}{(1-x)^{d+1}} = \sum_{k=0}^{\infty} \binom{k+d}{d} x^k$.

Důkaz. Pro $d = 0$ už máme hotovo, protože $\binom{k+0}{0} = 1$, takže jde o naši známou řadu $\sum_{k=0}^{\infty} x^k$. Dále postupujeme indukcí: řadu $\sum_{k=0}^{\infty} \binom{k+d}{d} x^k$ přenásobíme polynomem $1 - x$, čímž vznikne

$$\begin{aligned}(1-x) \cdot \sum_{k=0}^{\infty} \binom{k+d}{d} x^k &= \sum_{k=0}^{\infty} \binom{k+d}{d} x^k - \sum_{k=0}^{\infty} \binom{k+d}{d} x^{k+1} = \\ &= 1 + \sum_{k=1}^{\infty} \left(\binom{k+d}{d} - \binom{k-1+d}{d} \right) x^k = \\ &= 1 + \sum_{k=1}^{\infty} \binom{k-1+d}{d-1} x^k = \sum_{k=0}^{\infty} \binom{k-1+d}{d-1} x^k = \frac{1}{(1-x)^{d-1+1}}.\end{aligned}$$

Uprostřed jsme upravili číslování v řadě $\sum_{k=0}^{\infty} \binom{k+d}{d} x^{k+1} = \sum_{k=1}^{\infty} \binom{k-1+d}{d} x^k$ a následně použili vztah kombinačních čísel $\binom{n}{j} + \binom{n}{j+1} = \binom{n+1}{j+1}$, v poslední rovnosti jsme pak využili indukční předpoklad. Převedením $1 - x$ z levé strany na pravou pak dostáváme $\sum_{k=0}^{\infty} \binom{k+d}{d} x^k = \frac{1}{(1-x)^{d+1}}$, jak jsme chtěli. □

Extra super jsou tyto řady v tom, že na $\binom{k+d}{d}$ můžeme nahlížet jako na polynomy v proměnné k, a následně se dokonce každý polynom dá vyjádřit pomocí jednotlivých $\binom{k+d}{d}$. V principu tedy můžeme jakoukoliv řadu, která má koeficienty $a_k = P(k)$ pro nějaké $P \in \mathbb{C}[x]$, vyjádřit jako „polynom v $\frac{1}{1-x}$“.

Cvičení 3. Najdi racionální funkce, které se rovnají mocninným řadám:

(a) $\sum_{k=0}^{\infty} k^2 x^k$, (b) $\sum_{k=0}^{\infty} (k^3 - k) x^k$.

Obecněji, když už nalezneme generující funkci jedné posloupnosti, můžeme některé úpravy posloupnosti rovnou překládat na úpravy generující funkce:

Cvičení 4. Pokud víš, že racionální funkce $R(x)$ je generující funkcí posloupnosti $(a_0, a_1, a_2, \dots)$, najdi generující funkce posloupností:

(i) $(ca_0, ca_1, ca_2, \dots)$, tj. když každý člen přenásobíme jistým $c \in \mathbb{C}$,
(ii) $(0, a_0, a_1, a_2, \dots)$, tj. když posloupnost posuneme doprava a na začátek přidáme nulu,
(iii) $(a_1, a_2, a_3, \dots)$, tj. když posloupnost posuneme doleva a počáteční člen zahodíme,
(iv) $(a_0, 0, a_1, 0, a_2, 0, \dots)$, tj. když mezi každé dva členy posloupnosti vložíme nulu navíc,
(v) $(a_0, ca_1, c^2 a_2, c^3 a_3, \dots)$, tj. když vždy j-tý člen vynásobíme c^j pro jisté $c \in \mathbb{C}$,
(vi) $(a_0, 0, a_2, 0, a_4, 0, \dots)$, tj. členy na lichých pozicích škrtneme a nahradíme nulami,
(vii) (těžší) $(a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots)$, tj. posloupnost částečných součtů.

Generující funkce podruhé

Nyní už se dovedeme podívat na generující funkce v plné síle. Strategie zní: zajímá nás posloupnost komplexních (anebo reálných, racionálních…) čísel $a_0, a_1, a_2, \ldots$ Namísto ní uvážíme její generující funkci, mocninnou řadu $F(x) = \sum_{k=0}^{\infty} a_k x^k$, a pokusíme se cokoliv, co nás zajímá, interpretovat jako nějaké algebraické manipulace s F. Dobrým krokem pak bývá upravovat nekonečné mocninné řady na racionální funkce, neb ty jsou o něco skladnější a můžeme do nich zkoušet dosazovat. Jiným užitečným nápadem může být po úpravách něco rozvinout zpět na mocninnou řadu a znovu přečíst koeficienty. Ukažme si to názorně:

Příklad. Posloupnost *Fibonacciho čísel* je zadána pomocí $f_0 = 0$, $f_1 = 1$ a následně rekurentních vztahů $f_{k+2} = f_{k+1} + f_k$ pro každé celé $k \geq 0$. Vyjádřete f_k explicitním předpisem závisejícím pouze na k.

Řešení. Uvážíme mocninnou řadu Fibonacciho posloupnosti $F(x) = \sum_{k=0}^{\infty} f_k x^k$. Chtěli bychom ji vyjádřit jako racionální funkci a tušíme, že se k tomu bude hodit zadaná rekurence $f_{k+2} = f_{k+1} + f_k$. Zkusíme s její pomocí rozepsat koeficienty $F(x)$ (vyjma prvních dvou) a výsledek zase posbírat zpět do několika kusů, které by připomínaly $F(x)$. Výsledkem bude

$$F(x) = 0 + x + \sum_{k=2}^{\infty} f_k x^k = x + \sum_{k=0}^{\infty} f_{k+2} x^{k+2} = x + \sum_{k=0} (f_{k+1} + f_k) x^{k+2} =$$
$$= x + x \cdot \sum_{k=1}^{\infty} f_k x^k + x^2 \sum_{k=0} f_k x^k = x + x \cdot (F(x) - 0) + x^2 \cdot F(x),$$

z čehož už vyjádříme generující funkci

$$F(x) = \frac{x}{1 - x - x^2}.$$

Co teď s ní? Když označíme $\varphi_{1,2} = \frac{1 \pm \sqrt{5}}{2}$, můžeme jmenovatel rozložit na součin $1 - x - x^2 = (1 - \varphi_1 x)(1 - \varphi_2 x)$. Nyní provedeme trik a složitější zlomek rozepíšeme jako rozdíl jednodušších:[6] platí

$$\frac{1}{1 - \varphi_1 x} - \frac{1}{1 - \varphi_2 x} = \frac{(1 - \varphi_2 x) - (1 - \varphi_1 x)}{(1 - \varphi_1 x)(1 - \varphi_2 x)} = \frac{x(\varphi_1 - \varphi_2)}{(1 - \varphi_1 x)(1 - \varphi_2 x)}.$$

Zároveň $\varphi_1 - \varphi_2 = \sqrt{5}$, takže tuto odmocninu pak můžeme podělit a získáme

$$F(x) = \frac{x}{(1 - \varphi_1 x)(1 - \varphi_2 x)} = \frac{1}{\sqrt{5}(1 - \varphi_1 x)} - \frac{1}{\sqrt{5}(1 - \varphi_2 x)}.$$

Racionální funkce tvaru $\frac{1}{1 - cx}$ už ale umíme rozvinout do mocninné řady $\sum_{k=0}^{\infty} c^k x^k$, takže získáme

$$F(x) = \sum_{k=0}^{\infty} \frac{1}{\sqrt{5}} \left(\varphi_1^k - \varphi_2^k \right) x^k.$$

Porovnáním s původní definicí pomocí koeficientů f_k tak získáme předpis

$$f_k = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}}.$$

[6] Učeně se tomu někdy říká *rozklad na parciální zlomky.*

Kromě manipulace s posloupnostmi můžeme nahlížet i o něco nápaditější úložky. Hezkou myšlenkou, kterou ilustruje následující příklad, je, že jakoukoliv množinu S nezáporných celých čísel můžeme zakódovat jako řadu $\sum_{k\in S} x^k$:

Příklad. Nezáporná celá čísla jsou rozdělena do několika disjunktních nekonečných aritmetických posloupností s diferencemi $d_1, \ldots, d_k$. Dokaž, že musí platit $\frac{1}{d_1} + \cdots + \frac{1}{d_k} = 1$.

Řešení. Ať jsou $a_1, \ldots, a_k$ první členy příslušných aritmetických posloupností. Řadu, do níž zakódujeme aritmetickou posloupnost $a, a+d, a+2d, \ldots$, můžeme upravit pomocí

$$\sum_{n=0}^{\infty} x^{a+nd} = x^a \cdot \sum_{n=0}^{\infty} (x^d)^n = \frac{x^a}{1-x^d}.$$

Jestliže jsme tedy nezáporná celá čísla rozdělili na několik aritmetických posloupností, znamená to, že jsme $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$ rozložili na součet několika řad tvaru výše. Můžeme tedy zkoumat

$$\frac{1}{1-x} = \frac{x^{a_1}}{1-x^{d_1}} + \cdots + \frac{x^{a_k}}{1-x^{d_k}}.$$

To je rovnost racionálních funkcí: zápisu pomocí řad jsme se zbavili, můžeme proto začít dosazovat. Musíme se přitom ale stále vyhnout kořenům jmenovatelů, abychom nedělili nulou – zde by například nastaly trable při dosazení $x = 1$.

Zrovna v případě jedničky se ale této obtíže dovedeme zbavit. Jednička je kořenem všech jmenovatelů, tedy všichni jmenovatelé jsou násobky $1-x$. Když proto na obou stranách vynásobíme $1-x$, přičemž napravo zkrátíme skrze známý vzoreček $1 - x^d = (1-x)\left(1 + x + \cdots + x^{d-1}\right)$, dostaneme

$$1 = \frac{x^{a_1}}{1 + x + \cdots + x^{d_1-1}} + \cdots + \frac{x^{a_k}}{1 + x + \cdots + x^{d_k-1}}.$$

Zde už je dosazení $x = 1$ zcela validní – z každého jmenovatele $1 + x + \cdots + x^{d_i-1}$ se stane jen d_i, speciálně to tedy nebude nula. Zbude nám $1 = \frac{1}{d_1} + \cdots + \frac{1}{d_k}$, což jsme přesně chtěli dokázat.

Úloha 10. Nahlédni hokejkovou identitu $\sum_{n=k}^{m} \binom{n}{k} = \binom{m+1}{k+1}$ (viz Úlohu 2) za pomoci řady $\sum_{k=0}^{\infty} \binom{k+d}{d} x^k$.

Úloha 11. V závislosti na nezáporných celých $m \geq 1$, $n \geq 0$ spočti $\sum_{k=0}^{n} (-1)^k \binom{m}{n-k} \binom{m+k-1}{k}$.

Úloha 12. Jolča má bednu s nekonečně mnoha jablky, hruškami, pomeranči a ananasy. Urči, kolika způsoby může poskládat salát z n kusů ovoce tak, aby současně

(i) obsahoval nejvýše čtyři jablka,
(ii) obsahoval nejvýše jednu hrušku,
(iii) počet pomerančů byl sudý,
(iv) počet ananasů byl dělitelný pěti.

(Jednotlivé kusy téhož druhu ovoce jsou od sebe nerozlišitelné.)

Úloha 13. Dokaž, že Fibonacciho čísla splňují pro každé $n \geq 0$ vztah

$$\sum_{k=0}^{n} f_k = f_{n+2} - 1.$$

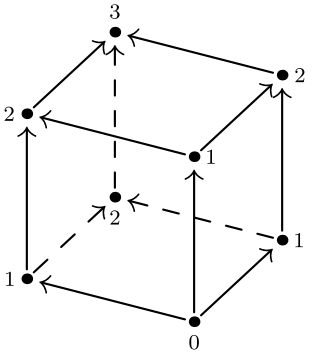
Úloha 14. V chlívku bydlí 30 růžových PraSátek, 40 černých a 50 flekatých, přičemž PraSátka se stejným barevným schématem jsou od sebe nerozlišitelná. Kolika způsoby můžeme z chlívku vybrat 70hlavé podstádo?

Úloha 15. (těžší) Nezáporná celá čísla jsou rozdělena do několika (alespoň dvou) disjunktních nekonečných aritmetických posloupností s diferencemi $d_1, \ldots, d_k$. Dokaž, že se mezi diferencemi nějaká opakuje, tedy že pro nějaká dvě $i \neq j$ bude $d_i = d_j$.

Mnohostěny

Idea generujících funkcí, kdy vezmeme svou oblíbenou posloupnost a napíšeme ji jako koeficienty mocninné řady, se objevuje i mimo olympiádní úlohy. Je to například jeden ze zásadních kroků v odpovědi na otázku „Kolik může mít mnohostěn vrcholů, hran a stěn?“, zobecněné i do více než tří rozměrů. Jenom zformulovat odpověď je mimo dosah tohoto seriálu, my se podíváme na první krok na cestě, která k ní vede. Představíme si dvě různé posloupnosti, které lze přiřadit mnohostěnu, a ukážeme si, jak spolu souvisí pomocí operací s polynomy.

Příklad. (krychle a čtyřstěn) Jak je známo, krychle má 8 vrcholů, 12 hran a 6 stěn. Nyní si představ krychli „postavenou na špičku“ a na každou hranu nakresli šipku ve směru nahoru.



Spočítej do kolika vrcholů nevede žádná šipka, do kolika jedna, do kolika dvě a do kolika tři. Pokud počítáš správně, mělo by Ti vyjít 1, 3, 3, 1. Posléze platí následující vztahy:

$$8 = 1\cdot 1 + 1\cdot 3 + 1\cdot 3 + 1\cdot 1 = \binom{3}{0}\cdot 1 + \binom{2}{0}\cdot 3 + \binom{1}{0}\cdot 3 + \binom{0}{0}\cdot 1,$$

$$12 = 3\cdot 1 + 2\cdot 3 + 1\cdot 3 + 0\cdot 1 = \binom{3}{1}\cdot 1 + \binom{2}{1}\cdot 3 + \binom{1}{1}\cdot 3 + \binom{0}{1}\cdot 1,$$

$$6 = 3\cdot 1 + 1\cdot 3 + 0\cdot 3 + 0\cdot 1 = \binom{3}{2}\cdot 1 + \binom{2}{2}\cdot 3 + \binom{1}{2}\cdot 3 + \binom{0}{2}\cdot 1.$$

Přichází čas na pár definic. Protože k pořádnému definování mnohostěnu a jeho stěn je třeba vysokoškolské matematiky, budeme spoléhat na intuici ze tří rozměrů. V této kapitole budeme uvažovat d rozměrný prostor. Souslovím „d-rozměrný mnohostěn“ potom myslíme mnohostěn v d rozměrech (například čtverec je dvourozměrný mnohostěn, nikoli třírozměrný). Pokud se více rozměrů bojíš, neváhej všechna d nahradit trojkou. Věz ale, že nebudeme využívat žádná tvrzení, v nichž by se více rozměrů odlišovalo od těch tří.

Abychom mohli jedním pojmem odkazovat na vrcholy, hrany, stěny i jejich vícerozměrné ekvivalenty, budeme je všechny nazývat *stěnami*. Zároveň je budeme rozlišovat podle jejich rozměru, tedy například vrchol je 0-rozměrná stěna a hrana je 1-rozměrná stěna.

Definice. Nechť M je d-rozměrný mnohostěn. Potom označíme jako $f_i(M)$ počet jeho i-rozměrných stěn. Speciálně dodefinujeme $f_d(M)$ jako 1.

Na definici $f_d(M) = 1$ se dá dívat tak, že mnohostěn M je svou vlastní d-rozměrnou stěnou.

Definice. Mnohostěn M v d rozměrech nazveme *jednoduchým*, pokud každý jeho vrchol leží v právě d stěnách dimenze $d-1$.

Tedy čtyřstěn, krychle a dvanáctistěn jsou jednoduché mnohostěny, zatímco pravidelný osmistěn či dvacetistěn nikoli. Uvažme nyní libovolný jednoduchý mnohostěn M a jeho vrchol v. Nejen, že

je obsažen v d stěnách o $d-1$ rozměrech, ale taky z něj musí vést d hran. Vybereme-li libovolných i z těchto hran, existuje i-rozměrná stěna mnohostěnu M, která je obsahuje. Tato stěna zároveň neobsahuje žádné další hrany z v.

Definice. Předpokládejme, že mnohostěn M je natočený tak, že jeho vrcholy mají po dvou různou výšku. Jeho hrany orientujeme (tj. nakreslíme na ně šipku) tak, aby vedly z nižšího do vyššího vrcholu. Jako $h_k(M)$ označíme počet vrcholů, do nichž směřuje k orientovaných hran.

Tvrzení. *Nechť M je jednoduchý mnohostěn. Potom*

$$f_i(M) = \sum_{k=0}^{d-i} \binom{d-k}{i} h_k(M).$$

Důkaz. Chceme spočítat i-rozměrné stěny. Každá taková má jednoznačně určený nejnižší vrchol. Všimněme si dále, že pokud vrchol na dané stěně není nejnižší, potom do něj vede nějaká hrana.

Na druhou stranu, uvažme nějaký vrchol v a zamysleme se nad tím, pro kolik stěn dimenze i je tento vrchol nejnižší. Nechť s je nějaká taková stěna. Všechny hrany s obsahující v musí být orientované pryč od v. Protože M je jednoduchý, každá i-tice hran vedoucích z v určuje nějakou stěnu dimenze i. Pokud do v vede k hran, $d-k$ hran vede z v pryč, tedy v je nejnižší vrchol na $\binom{d-k}{i}$ stěnách. Celkový počet stěn pak získáme sečtením $\binom{d-k}{i}$ přes všechny vrcholy, čímž přesně získáme dokazovanou rovnost. □

Cvičení 5. Ověř předcházející tvrzení pro pravidelný čtyřstěn, a pokud Tě to baví, tak i pro pravidelný dvanáctistěn.

Díky tomuto tvrzení máme $d+1$ rovnic vyjadřujících $f_i(M)$ v závislosti na $h_k(M)$. Pokud ale známe $(f_0(M), \ldots, f_d(M))$, můžeme z těchto rovnic naopak dopočítat $(h_0(M), \ldots, h_d(M))$:

$$\begin{aligned}
h_0(M) &= f_d(M),\\
h_1(M) &= f_{d-1}(M) - \binom{d}{d-1} \cdot h_0(M),\\
h_2(M) &= f_{d-2}(M) - \binom{d}{d-2} \cdot h_0(M) - \binom{d-1}{d-2} \cdot h_1(M),\\
&\vdots
\end{aligned}$$

To znamená, že jakýkoli poznatek o $(f_0(M), \ldots, f_d(M))$ umíme přeložit do jazyka $(h_0(M), \ldots, h_d(M))$ a naopak. Také díky tomu víme, že čísla $h_k(M)$ jsou jednoznačně určená. Ze samotné definice $h_k(M)$ není jasné, jestli tato čísla náhodou nezávisí na tom, jak jsme M natočili. Vzhledem k tomu, že $(f_0(M), \ldots, f_d(M))$ na natočení nezávisí, nezávisí na něm ani $(h_0(M), \ldots, h_d(M))$.

Až do teď to nevypadá, že by tohle všechno nějak souviselo s polynomy. Pojďme si ale napsat generující funkce našich posloupností. Protože jsou to posloupnosti konečné, dostaneme dokonce polynomy.

Definice. Nechť je M jednoduchý mnohostěn v d rozměrech. Potom definujeme polynomy

$$f_M(x) = \sum_{i=0}^{d} f_i(M) x^i, \qquad h_M(x) = \sum_{k=0}^{d} h_k(M) x^k.$$

Předcházející tvrzení se dá nyní elegantně vyjádřit pomocí polynomů.

Tvrzení. *Nechť M je jednoduchý mnohostěn. Potom platí*

$$h_M(x) = x^d \cdot f_M\left(\frac{1-x}{x}\right).$$

Důkaz. Dosazování racionální funkce může vypadat děsivě, ale násobení x^d to zase spraví. Po rozepsání se pravá strana rovná

$$x^d \cdot \sum_{i=0}^{d} \frac{f_i(M) \cdot (1-x)^i}{x^i} = \sum_{i=0}^{d} f_i(M) \cdot x^{d-i} \cdot (1-x)^i.$$

Nyní je na čase dosadit za $f_i(M)$ z předchozího tvrzení a pak sumy vyměnit:

$$\sum_{i=0}^{d} \left(\sum_{k=0}^{d-i} \binom{d-k}{i} h_k(M) \right) \cdot x^{d-i} \cdot (1-x)^i = \sum_{k=0}^{d} \left(\sum_{i=0}^{d-k} \binom{d-k}{i} \cdot x^{d-i} \cdot (1-x)^i \right) h_k(M) =$$
$$= \sum_{k=0}^{d} x^k \left(\sum_{i=0}^{d-k} \binom{d-k}{i} \cdot x^{d-k-i} \cdot (1-x)^i \right) h_k(M) = \sum_{k=0}^{d} h_k(M) \cdot x^k \cdot (x+(1-x))^{d-k} = h_M(x).$$

V předposledním rovnítku jsme využili binomické věty. □

Posloupnost $(h_0(M), \ldots, h_d(M))$ je hezčí než $(f_0(M), \ldots, f_d(M))$, protože platí $h_k = h_{d-k}$ pro každé $k = 0, \ldots, d$. Proč? V definici jsme nějak otočili mnohostěn M. Obraťme nyní co je „nahoru" a co „dolů". Protože do každého vrcholu vede d hran, do těch, do nichž vedlo k hran, nyní povede $d-k$ hran. Protože $(h_0(M), \ldots, h_d(M))$ nezávisí na konkrétním otočení M, získáváme rovnost $h_k = h_{d-k}$.

Pojďme nyní naše dvě posloupnosti využít pro trojrozměrné mnohostěny.

Tvrzení. *Jediné jednoduché pravidelné trojrozměrné mnohostěny jsou čtyřstěn, krychle a dvanáctistěn.*

Důkaz. Nechť M je nějaký takový mnohostěn. Již víme, že $h_0(M) = f_d(M) = 1$. Označme $h_1(M)$ jako h. Potom z odstavce nad tímto tvrzením víme, že $h_2(M) = h_1(M) = h$ a $h_3(M) = h_0(M) = 1$. Ze vztahu pro $f_i(M)$ spočítáme

$$f_1(M) = \binom{3}{1} \cdot 1 + \binom{2}{1} \cdot h + \binom{1}{1} \cdot h = 3h + 3,$$
$$f_2(M) = \binom{3}{2} \cdot 1 + \binom{2}{2} \cdot h = h + 3.$$

Každá hrana je obsažena právě ve dvou stěnách. Na druhou stranu mnohostěn M je pravidelný, tedy každá stěna má právě a hran pro nějaké pevné celé číslo a. Tedy počet dvojic hrana a stěna, která ji obsahuje, je $2 \cdot (3h+3) = a \cdot (h+3)$. Tedy $h+3$ je dělitelem $6h+6$, tím pádem i $(6h+6) - 6 \cdot (h+3) = -12$. Rozborem podle dělitelů dvanácti zjistíme, že h může být pouze 1, 3, nebo 9. Protože M je jednoduchý, máme o něm nyní všechny informace. Vskutku pro čtyřstěn, krychli a dvanáctistěn nabývá h postupně těchto hodnot. □

Tvrzení. (Eulerův vzorec) *Pro trojrozměrný mnohostěn M platí*[7] $f_0(M) - f_1(M) + f_2(M) = 2$.

Důkaz. Nejprve tvrzení dokážeme pro jednoduchý trojrozměrný mnohostěn M. Zachovejme značení z předchozího tvrzení. Již víme, že $f_1(M) = 3h + 3$ a $f_2(M) = h + 3$. Podobně zjistíme

$$f_0(M) = \binom{3}{0} \cdot 1 + \binom{2}{0} \cdot h + \binom{1}{0} \cdot h + \binom{0}{0} \cdot 1 = 2h + 2.$$

Vskutku tedy $f_0(M) - f_1(M) + f_2(M) = 2$.

[7] Jak toto tvrzení souvisí s takzvanými rovinnými grafy můžeš zjistit ve třetím díle seriálu o kombinatorické geometrii ze 42. ročníku: *https://prase.cz/archive/42/uvod3s.pdf*.

Z obecného mnohostěnu M vyrobíme jednoduchý mnohostěn a ukážeme, že se tím hodnota $f_0(M) - f_1(M) + f_2(M)$ nezmění. Nechť v je vrchol M, z nějž vede příliš mnoho hran, označme jejich počet a. Potom v „usekneme“: Na každou hranu, která z v vede, umístíme nový vrchol tak, aby všechny tyto vrcholy ležely v jedné rovině. Poté v nahradíme těmito vrcholy, označme je $v_1, \ldots, v_a$. Tím jsme přidali mnohostěnu M stěnu tvořenou a-úhelníkem $v_1 v_2 \ldots v_a$. Přidali jsme tedy jednu stěnu, a hran, a vrcholů a jeden vrchol jsme odebrali. Dohromady se tedy hodnota $f_0(M) - f_1(M) + f_2(M)$ nezmění. Zároveň z každého z vrcholů $v_1, \ldots, v_a$ vedou tři hrany. Takto můžeme postupně „useknout“ všechny vrcholy, které mají příliš mnoho hran. Protože méně než tři hrany z vrcholu vést nemohou, získáme jednoduchý mnohostěn. □

Závěr

Zazvonil zvonec a seriálu je konec. Děkujeme Ti a gratulujeme, že jsi se s námi dočetl(a) až sem. Doufáme, že Tě náš cestopis světem polynomů bavil a něčemu novému Tě přiučil.

Seriál pro Tebe psali Majda, Matěj a Tom. Rádi bychom zde poděkovali všem, kteří nám s tím byli nápomocni, především Klárce a Michalovi.

Měj se fajn a užij si úlohy třetí seriálové série!

Návody ke cvičením

1. $\sum_{j=0}^{k} 1 \cdot 1$.

2. Podívej se na nejmenší členy s nenulovými koeficienty.

3. $k^2 = 2\binom{k+2}{2} - 3\binom{k+1}{1} + \binom{k+0}{0}$, $k^3 - k = 6\binom{(k-2)+3}{3}$.

4. Většina by měla být snadná. Pro (vi) se podívej na (v) s $c = -1$. Pro (vii) násob $1+x+x^2+\cdots$

5. Prostě to spočítej a dosaď.

Návody k úlohám

1. Spočítej všechny podmnožiny.

2. Přepiš $\binom{k}{k} = \binom{k+1}{k+1}$ a poté sčítej v Pascalově trojúhelníku.

3. Kolikrát použijeme který tah?

4. Vybírej, kdy změnit sáček.

5. Opět převeď na součin řad z binomické věty.

6. $(1+x)^a \cdot (1+x)^b$.

7. Vzpomeň si na derivace z minulého dílu a zderivuj binomickou větu.

8. Začni s $P(x) = (1+x)(1+x^2)(1+x^3)\cdots(1+x^n)$.

9. Zakóduj do polynomů $P_{n+1}(x) = (1+x)P_n(x)$, akorát se na koeficienty dívej modulo 2.

10. Vynásob $\frac{1}{(1-x)^{k+1}} \cdot \frac{1}{1-x}$.

11. $(1+x)^m \cdot \frac{1}{(1+x)^m}$.

12. $\frac{x^5-1}{x-1} \cdot (1+x) \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^5}$.

13. Generující funkci $F(x)$ Fibonacciho čísel už známe. Součty Fibonacciho čísel pak značí $\frac{F(x)}{1-x}$.

14. Koeficient u x^{70} v polynomu $\frac{x^{31}-1}{x-1} \cdot \frac{x^{41}-1}{x-1} \cdot \frac{x^{51}-1}{x-1}$. Lépe se Ti bude počítat, když rozvineš $\frac{1}{(x-1)^3}$ do mocninné řady.

15. Zkus použít kořeny některého $x^{d_i} - 1$.

Řešení cvičení

1. $F(x)$ má za koeficienty samé jedničky. Když se proto podíváme, jak má vypadat koeficient u x^k v součinu dvou takových řad, dostaneme sumu součinů jedniček s jedničkami: $\sum_{j=0}^{k} 1 \cdot 1 = k+1$. Tedy $F(x)^2 = \sum_{k=0}^{\infty}(k+1)x^k = 1 + 2x + 3x^2 + 4x^3 + \cdots$

2. Ať se naše řady spolu se svými koeficienty jmenují $F(x) = \sum_{k=0}^{\infty} a_k x^k$ a $G(x) = \sum_{k=0}^{\infty} b_k x^k$. Jelikož $F \neq 0$, nějaké a_i je nenulové – uvažujme nejmenší i s touto vlastností. Podobně ať j je nejmenší index takový, že $b_j \neq 0$. Potom je koeficient u x^{i+j} v $F(x) \cdot G(x)$ roven $a_i b_j \neq 0$, protože všechny ostatní nenulové členy z F a G se spolu znásobí na něco s vyšším exponentem u x než $i+j$. Tudíž i řada $F(x) \cdot G(x)$ má alespoň jeden nenulový koeficient, čili je nenulová.

3. (a) Abychom se dostali na kvadratický polynom, použijeme $\binom{k+2}{2} = \frac{(k+2)(k+1)}{2} = \frac{k^2+3k+2}{2}$. Čili vezmeme dvojnásobek a posléze se s pomocí $\binom{k+1}{1} = k+1$ a $\binom{k+0}{0} = 1$ chceme zbavit lineárního a absolutního členu. Po chvilce snažení bychom se měli dobrat ke $k^2 = 2\binom{k+2}{2} - 3\binom{k+1}{1} + \binom{k+0}{0}$, což odpovídá

$$\sum_{k=0}^{\infty} k^2 x^k = 2\sum_{k=0}^{\infty}\binom{k+2}{2}x^k - 3\sum_{k=0}^{\infty}\binom{k+1}{1}x^k + \sum_{k=0}^{\infty}\binom{k+0}{0}x^k = \frac{2}{(1-x)^3} - \frac{3}{(1-x)^2} + \frac{1}{1-x}.$$

(b) Vyjádříme třeba $k^3 - k = 6\binom{k+1}{3} = 6\binom{(k-2)+3}{3}$. Chceme pak vzít šestinásobek řady $\frac{1}{(1-x)^4}$ posunuté o dvě pozice, tudíž $\frac{6x^2}{(1-x)^4}$.

4. Mělo by vyjít postupně:
(i) $cR(x)$, (ii) $xR(x)$, (iii) $\frac{R(x)-a_0}{x}$, (iv) $R(x^2)$, (v) $R(cx)$, (vi) $\frac{R(x)+R(-x)}{2}$, (vii) $\frac{R(x)}{1-x}$.

5. Pokud je M pravidelný čtyřstěn, $h_0(M) = h_1(M) = h_2(M) = h_3(M) = 1$. Zároveň

$$f_0(M) = 4 = 1 \cdot h_0(M) + 1 \cdot h_1(M) + 1 \cdot h_2(M) + 1 \cdot h_3(M),$$
$$f_1(M) = 6 = 3 \cdot h_0(M) + 2 \cdot h_1(M) + 1 \cdot h_2(M) + 0 \cdot h_3(M),$$
$$f_2(M) = 4 = 3 \cdot h_0(M) + 1 \cdot h_1(M) + 0 \cdot h_2(M) + 0 \cdot h_3(M).$$

Pokud je M dvanáctistěn, $h_0(M) = h_3(M) = 1$, $h_1(M) = h_2(M) = 9$. Na druhou stranu $f_0(M) = 20$, $f_1(M) = 30$ a $f_2(M) = 20$. Opět dosazením ověříme, že tvrzení platí.

Řešení úloh

1. Ať je M množina s n prvky. Pak suma levé straně představuje počet nulaprvkových podmnožin M, plus počet jednoprvkových podmnožin M, ..., plus počet n-prvkových podmnožin M. To ale musí dohromady dát počet všech podmnožin M. Když vybíráme podmnožinu M, můžeme se u každého z n prvků nezávisle rozhodnout, zda si ho do podmnožiny vzít, či nikoliv. Tedy n-krát vybíráme ze 2 možností, tudíž dostaneme 2^n.

2. Zkoumáme sumu, která začíná nějak takhle:

$$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots$$

Všimněme si, že první člen $\binom{k}{k} = 1$, což bychom klidně taky mohli přepsat na $\binom{k+1}{k+1}$. Podle sčítacího vzorečku z tvrzení pak můžeme na začátku sumy zjednodušit $\binom{k+1}{k+1} + \binom{k+1}{k} = \binom{k+2}{k+1}$. Tím dostáváme

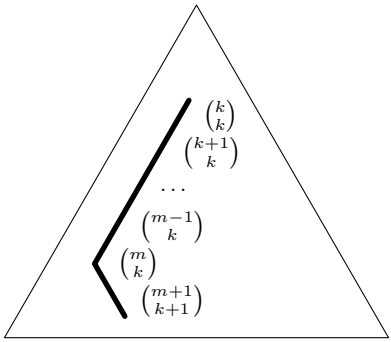
$$\binom{k+2}{k+1} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots$$

Zde ale stejně dobře můžeme sečíst $\binom{k+2}{k+1} + \binom{k+2}{k} = \binom{k+3}{k+1}$ a máme

$$\binom{k+3}{k+1} + \binom{k+3}{k} + \cdots$$

Tento proces bude pokračovat dál a dál, až na úplném konci sečteme $\binom{m}{k+1} + \binom{m}{k} = \binom{m+1}{k+1}$, což je přesně to, co jsme chtěli dostat.

Mimochodem, označení „hokejková identita“ se váže k tomu, jak jsou kombinační čísla v sumě a celkový výsledek rozmístěny v Pascalově trojúhelníku. Mnemotechnicky: součtem násady hokejky je její čepel.



3. Dohromady se potřebujeme posunout o 8 políček nahoru a 8 doprava. Zabere nám to tedy 12 tahů: 4 nahoru a 8 doprava. Cesta je určená tím, v jakém pořadí tahy použijeme, tedy které čtyři z dvanácti tahů budou nahoru. Počet způsobů je tedy $\binom{12}{4} = \frac{9 \cdot 10 \cdot 11 \cdot 12}{24} = 495$.

4. Představme si řadu složenou z 10 bonbónů a dvou oddělovačů – první mezi bonbóny z prvního a druhého sáčku, druhý mezi bonbóny z druhého a třetího. Množství bonbónů v jednotlivých sáčcích je určeno pozicemi oddělovačů, tedy tím, na kterých dvou z dvanácti pozic v řadě oddělovače jsou. Díky tomu je počet možných rozdělení $\binom{10}{2} = 45$.

5. Když v binomické větě nahradíme x za $-x$, přibudou nám do sumy znaménka v podobě $(1-x)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^k$, což se nám pro vyjádření zadané sumy hodí. Naproti tomu podobně jako ve vzorovém příkladu přepíšeme $\binom{n}{k} = \binom{n}{n-k}$, načež můžeme sumu $\sum_{k=0}^{n} (-1)^k \binom{n}{k}\binom{n}{n-k}$ interpretovat jako koeficient u x^n v polynomu $(1-x)^n \cdot (1+x)^n = (1-x^2)^n$. Ten má zjevně jen členy sudého stupně, takže pro lichá n je výsledek nula, zatímco pro sudá n je to (použitím binomické věty) $(-1)^{n/2}\binom{n}{n/2}$.

6. Sumu interpretujeme jako koeficient u x^n v

$$\left(\sum_{i=0}^{a} \binom{a}{i} x^i\right) \cdot \left(\sum_{j=0}^{b} \binom{b}{j} x^j\right) = (1+x)^a \cdot (1+x)^b = (1+x)^{a+b},$$

což je opětovným použitím binomické věty rovno $\binom{a+b}{n}$.

7. Binomická věta nám dává v $\mathbb{C}[x]$ rovnost polynomů $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$. Pojďme obě strany rovnice zderivovat (vzpomeň si na formální derivace z minulého dílu). Derivace součtu je součet derivací a derivace konstantního násobku je konstantní násobek derivace, takže na pravé straně získáme

$$\sum_{k=0}^{n} \binom{n}{k} (x^k)' = \sum_{k=0}^{n} \binom{n}{k} \cdot k x^{k-1}.$$

Když pak dosadíme $x = 1$, dostaneme přesně sumu, která nás zajímá. Naproti tomu na levé straně dostaneme derivaci $n(1+x)^{n-1}$ (všimni si, že n je ze zadání kladné, takže $n-1$ je nezáporné, takže tohle dává smysl) – to umíme zdůvodnit dvěma způsoby: buďto opakovaně použijeme pravidlo pro součin $(P\cdot Q)' = P'\cdot Q + P\cdot Q'$, anebo použijeme pravidlo pro skládání $(P(Q(x)))' = P'(Q(x))\cdot Q'(x)$ s volbou $P(x) = x^n$, $Q(x) = 1 + x$. Na levé straně tedy dosazením $x = 1$ dostaneme $n2^{n-1}$, což je tak výsledek kýžené sumy.

8. Uvažme polynom $P(x) = (1 + x)(1 + x^2)(1 + x^3)\cdots(1 + x^n)$. Závorka $1 + x^j$ kóduje, že si do podmnožiny buďto prvek j vzít můžeme, anebo nemusíme. Pak po roznásobení každý člen x^k odpovídá podmnožině se součtem k, takže celkem v $P(x)$ koeficient u x^k představuje počet podmnožin se součtem k. My si chceme nechat jen ty se sudým součtem.

K tomu poslouží dosadit $-x$: tím se převrátí znaménko přesně u členů s lichým stupněm. Když proto vezmeme $P(x) + P(-x)$, členy lichého stupně zmizí a u každého x^{2k} zbude dvojnásobek původního koeficientu. Nás zajímá součet původních koeficientů na sudých pozicích (to je počet sudých podmnožin), dobereme se ho proto dosazením jedničky a podělením dvěma. Počítáme tak $\frac{P(1)+P(-1)}{2}$. Přitom $P(-1)$ bude nula, protože v součinu, kterým jsme $P(x)$ původně zadefinovali, bude závorka $(1-1)$. Naopak dosazením 1 v součinu dostaneme součin samých dvojek, takže hledaný výsledek bude $\frac{2^n+0}{2} = 2^{n-1}$.

9. Tvrdíme, že fungují všechna n, která jsou mocniny dvojky větší než největší prvek S_0.

Každou S_n zakódujeme jako polynom $P_n(x) = \sum_{a\in S_n} x^a$, přičemž na koeficienty se budeme dívat modulo 2; pokud se kamarádíš s obory $\mathbb{Z}_p$, pak jen říkáme, že budeme brát $P_n \in \mathbb{Z}_2[x]$. V tomto duchu pak vztah, kterým konstruujeme nové S_{n+1}, říká jen $P_{n+1}(x) \equiv (1 + x)P_n(x)$, kde se stále díváme modulo 2: koeficient u x^a v P_{n+1} bude lichý přesně tehdy, když byl v P_n lichý právě jeden z koeficientů u x^a a u x^{a-1}.

Triviální indukcí plyne $P_n(x) \equiv (1 + x)^n P_0(x)$. Zvolme nyní $n = 2^k$ pro nějaké k. Modulo 2 platí $(1 + x)^2 = 1 + 2x + x^2 \equiv 1 + x^2$, z čehož indukcí plyne $(1 + x)^{2^k} \equiv 1 + x^{2^k}$. Jakmile bude k dost velké na to, aby $2^k > \max S_0 = \deg(P_0)$, pak už v $P_{2^k}(x) \equiv \left(1 + x^{2^k}\right) P_0(x)$ roznásobením vznikne hromádka členů, každý s jiným stupněm – nic se proto modulo 2 nevyruší a členy v P_n budou odpovídat prvkům S_0 a jejich kopiím posunutým o $n = 2^k$, což je přesně to, co jsme chtěli.

10. Nejprve sumu přeznačme tak, aby nezačínala od k, ale od nuly. Označme $j = n-k$ a $a = m-k$, pak chceme ukázat $\sum_{j=0}^{a} \binom{j+k}{k} = \binom{a+k+1}{k+1}$.

Pojďme vynásobit $\frac{1}{(1-x)^{k+1}} \cdot \frac{1}{1-x}$. Na jednu stranu víme, že $\frac{1}{(1-x)^{k+1}} = \sum_{j=0}^{\infty} \binom{j+k}{k} x^j$ a vynásobení $\frac{1}{1-x}$ vyrobí v koeficientech částečné součty (viz Cvičení 4(vii)), takže u x^a v $\frac{1}{(1-x)^{k+1}} \cdot \frac{1}{1-x}$ dostaneme koeficient $\sum_{j=0}^{a} \binom{j+k}{k}$.

Naproti tomu ale víme, že $\frac{1}{(1-x)^{k+1}} \cdot \frac{1}{1-x} = \frac{1}{(1-x)^{k+2}}$, což se rozvine v řadu, kde koeficient u x^a je $\binom{a+k+1}{k+1}$. Dohromady jsme tedy ukázali

$$\sum_{j=0}^{a} \binom{j+k}{k} = \binom{a+k+1}{k+1},$$

což jsme přesně chtěli.

11. Kombinační čísla $\binom{m+k-1}{k} = \binom{k+m-1}{m-1}$ jsou koeficienty generující funkce $\frac{1}{(1-x)^m}$. Když nahradíme x za $-x$, dostaneme $\frac{1}{(1+x)^m}$ s koeficienty $(-1)^k\binom{k+m-1}{m-1}$. Naproti tomu $\binom{m}{k}$ jsou koeficienty $(1 + x)^m$, takže suma

$$\sum_{k=0}^{n} (-1)^k \binom{k+m-1}{m-1} \cdot \binom{m}{n-k}$$

vyjadřuje koeficient u x^n v $\frac{1}{(1+x)^m} \cdot (1 + x)^m = 1$. Výsledek tedy bude 1 pro $n = 0$, zatímco pro $n > 0$ obdržíme 0.

12. Sestavíme si pro každé ovoce řadu, která má 1 u každého x^k takového, že si můžeme vzít k kusů daného ovoce, a 0 všude jinde. Poté součin čtyř takových řad bude kódovat v koeficientu u x^n počet způsobů, jak vybrat salát s n kusy ovoce za daných podmínek.

Nejjednodušší je hruška: prostě buď bude, nebo nebude, takže máme řadu (resp. dokonce polynom) $1+x$. Podobně jablka dají $1+x+x^2+x^3+x^4 = \frac{x^5-1}{x-1}$. Sudý počet pomerančů odpovídá $1+x^2+x^4+x^6+\cdots = \sum_{k=0}^{\infty} x^{2k} = \frac{1}{1-x^2}$, zatímco ananasům analogicky odpovídá $1+x^5+x^{10}+\cdots = \frac{1}{1-x^5}$. Znásobením dostáváme řadu

$$\frac{x^5-1}{x-1}\cdot(1+x)\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^5} = \frac{1+x}{(1-x)(1-x^2)} = \frac{1}{(1-x)^2}.$$

Tuto řadu už ale známe a víme, že jejím koeficientem u x^n je $\binom{n+1}{1} = n+1$. Jolča tedy může salát poskládat $n+1$ způsoby.

13. V ukázkovém příkladu už jsme odvodili generující funkci Fibonacciho čísel, je to $F(x) = \frac{x}{1-x-x^2}$. Abychom dokázali kýženou rovnost, vyrobíme z levé a pravé strany dvě mocninné řady a dokážeme, že jsou si navzájem rovné – když se rovnají řady, rovnají se i odpovídající koeficienty. Na levé straně máme posloupnost částečných součtů, takže podle Cvičení 4(vii) víme, že vznikne generující funkce $\frac{F(x)}{1-x}$. Na pravé straně nejprve f_{n+2} znamená posunout posloupnost doleva o dvě pozice, což dá generující funkci $\frac{F(x)-f_1x-f_0}{x^2}$, a poté -1 znamená generující funkci $\frac{-1}{1-x}$.

Dohromady tak chceme dokázat rovnost

$$\frac{F(x)}{1-x} = \frac{F(x)-x}{x^2} - \frac{1}{1-x}.$$

K tomu už stačí rozepsat $F(x) = \frac{x}{1-x-x^2}$, zbavit se jmenovatelů a ověřit rovnost polynomů:

$$\begin{aligned}\frac{x}{(1-x)(1-x-x^2)} &= \frac{1}{x(1-x-x^2)} - \frac{1}{x} - \frac{1}{1-x},\\ x^2 &= (1-x) - (1-x)(1-x-x^2) - x(1-x-x^2),\\ x^2 &= x^2.\end{aligned}$$

14. Od růžových PraSátek si můžeme vzít 0, 1, …, nebo 30 kusů, což odpovídá polynomu $1+x+\cdots+x^{30} = \frac{x^{31}-1}{x-1}$. Stejnou interpretaci provedeme i s černými a flekatými PraSátky. Součin odpovídajících tří polynomů nám pak v koeficientu u x^k říká, kolika způsoby lze vybrat k-hlavé stádo. Vyjádřeme si součin a rozviňme v něm jmenovatel do nekonečné řady pomocí $\frac{1}{(1-x)^{d+1}} = \sum_{k=0}^{\infty}\binom{k+d}{d}x^k$:

$$\begin{aligned}\frac{x^{31}-1}{x-1}\cdot\frac{x^{41}-1}{x-1}\cdot\frac{x^{51}-1}{x-1} &= -\frac{1}{(1-x)^3}\cdot(x^{123}-x^{92}-x^{82}-x^{72}+x^{51}+x^{41}+x^{31}-1) =\\ &= -\left(\sum_{k=0}^{\infty}\binom{k+2}{2}x^k\right)\cdot(x^{123}-x^{92}-x^{82}-x^{72}+x^{51}+x^{41}+x^{31}-1).\end{aligned}$$

Zajímá nás koeficient u x^{70}, čili v poslední závorce můžeme ignorovat členy s vyšším exponentem. Pak se dobereme výsledku

$$\binom{70+2}{2} - \binom{70-51+2}{2} - \binom{70-41+2}{2} - \binom{70-31+2}{2} = 1061.$$

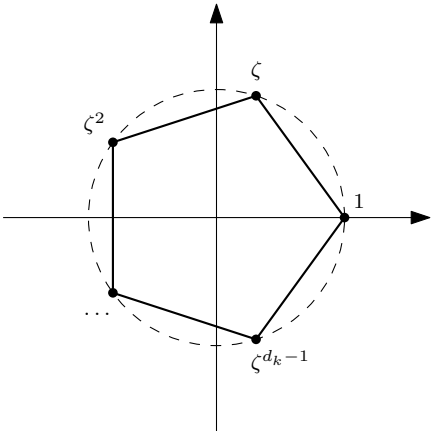
15. Stejně jako v ukázkovém příkladu se dobereme rovnosti

$$\frac{1}{1-x} = \frac{x^{a_1}}{1-x^{d_1}} + \cdots + \frac{x^{a_k}}{1-x^{d_k}}. \qquad (*)$$

BÚNO ať jsou diference seřazené vzestupně $d_1 \leq \cdots \leq d_k$, pak dokážeme, že musí být $d_k = d_{k-1}$. Pro spor ať není, tedy ať je d_k ostře větší než všechna ostatní d_i.

Kterýkoliv polynom tvaru $x^d - 1$ má d komplexních kořenů. Říká se jim *d-té odmocniny z jedničky*[8] a v komplexní rovině představují vrcholy pravidelného d-úhelníku vepsaného do kružnice $|z| = 1$; speciálně jsou tedy navzájem různé. Pokud označíme jako ζ_d ten z nich, který je při cestě po kružnici nejblíž k jedničce (takové mohou být dva, vybereme si kterýkoliv z nich), pak jsou kořeny $x^d - 1$ přesně $1, \zeta_d, \zeta_d^2, \ldots, \zeta_d^{d-1}$, takže v $\mathbb{C}[x]$ rozložíme na součin

$$x^d - 1 = (x-1)(x-\zeta_d)(x-\zeta_d^2)\cdots(x-\zeta_d^{d-1}).$$



Klíčovým pozorováním je, že pokud je d_k ostře větší než všechna ostatní d_i a zvolíme $\zeta = \zeta_{d_i}$, pak ζ nebude kořenem žádného dalšího $x^{d_i} - 1$. V rovnici $(*)$ nyní nalezneme spor tím, že nejprve vynásobíme obě strany vynásobit polynomem $x - \zeta$, a poté dosadíme $x = \zeta$. V členech $\frac{1}{1-x}$ ani $\frac{x^{a_i}}{1-x^{d_i}}$ pro $i < k$ se pak nic nezkrátí, protože ζ nebyl kořen příslušných jmenovatelů. To znamená, že po dosazení $x = \zeta$ všechny tyto členy zmizí. Naproti tomu v $\frac{x^{a_k}}{1-x^{d_k}}$ se dvojčlen $x - \zeta$ zkrátí se jmenovatelem a zbude $\frac{x^{a_k}}{-(x-1)(x-\zeta^2)(x-\zeta^3)\cdots(x-\zeta^{d_k-1})}$. Tím pádem ζ už nebude kořenem jmenovatele a není ani kořenem čitatele, proto dosazením ζ nutně vznikne nenulové číslo. Dohromady tak z rovnice $(*)$ zbude jen to, že se nula rovná něčemu nenulovému, což je spor, který jsme hledali.

[8] Více se o nich můžeš dočíst třeba v tomto příspěvku:
https://prase.cz//library/OdmocninyZJednickyLK/OdmocninyZJednickyLK.pdf.