

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 vybíráme prvky do podmnožiny postupně: první můžeme vybrat n způsoby, druhý $n-1$ způsoby, $\dots$, 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. $\square$

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 :-).

$$\begin{array}{ccccccc}
 & & \binom{0}{0} & & & & 1 \\
 & & \binom{1}{0} & \binom{1}{1} & & & 1 & 1 \\
 & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & 1 & 2 & 1 \\
 & & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & 1 & 3 & 3 & 1 \\
 & & \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & 1 & 4 & 6 & 4 & 1 \\
 & & \binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & 1 & 5 & 10 & 10 & 5 & 1
 \end{array}$$

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 $P(x) = a_0 + a_1x + a_2x^2 = 2 + 3x + 4x^2$.

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. Pojdme 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

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

²Bylo 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 $1, x, \dots, x^n$. 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 $\{1, 2, \dots, n\}$, 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 $(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$. $\square$

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

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 způsoby³. Dobrá tedy, zkusme další ukázkou.

³Pokud 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 $1, \dots, 6$. 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 $1, \dots, 6$ (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 přičíst 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 konečné mnoha možností, ale můžeme si ještě trochu pomoci. 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 zkoušet 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 jejich prvků. Urči, kolik má $\{1, 2, \dots, n\}$ 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 nezni 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 nepřišla dostatečně k srdci, klidně si místo nich představuj ta reálná či racionální.

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

$$F(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{k=0}^{\infty} a_k x^k,$$

kde *koefficienty* $a_0, a_1, a_2, \dots$ 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 $F(x)^2$.

⁴Přes 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 vyhýbáme.

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

$$(1-x) \cdot (1+x+x^2+x^3+x^4+\dots) = (1+x+x^2+x^3+x^4+\dots) + (-x-x^2-x^3-x^4-\dots)$$

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 $1+x+x^2+x^3+x^4+\dots$ je totéž jako „dělit“ polynomem $1-x$. (Anebo též naopak, „dělit“ řadou $1+x+x^2+x^3+x^4+\dots$ je totéž jako násobit polynomem $1-x$.) Z tohoto důvodu si dovolíme psát

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

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 učené 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 $a_0, a_1, a_2, \dots$ podaří vyjádřit jako racionální funkci $R(x)$, nazveme ji *generující funkcí* posloupnosti $(a_0, a_1, a_2, \dots)$.⁵

Příklad s $1+x+x^2+x^3+x^4+\dots$ 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

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

⁵Obecněji 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. $\square$

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. $\square$

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:

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

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 $a_0, a_1, a_2, \dots$. Namísto ní uvážíme její generující funkci, mocninou 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 mocninou řadu a znovu přechít 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 závislejícím pouze na k .

Řešení. Uvážíme mocninou 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

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

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

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

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

Kromě manipulace s posloupnostmi můžeme nahlížet i o něco nápaditější úločky. 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 $d_1, \dots, d_k$. Dokaž, že musí platit $\frac{1}{d_1} + \dots + \frac{1}{d_k} = 1$.

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

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

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 $1-x^d = (1-x)(1+x+\dots+x^{d-1})$, dostaneme

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

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

Úloha 10. Nahlédni hokejkovou identitu $\sum_{n=k}^{\infty} \binom{n}{k} = \binom{m+1}{k+1}$ (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 Fibonaccioho čísla splňují pro každé $n \geq 0$ vztah

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

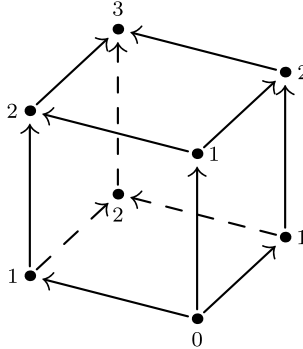
Úloha 14. V chlívků bydlí 30 růžových PraSátek, 40 černých a 50 flekatých, přičemž PraSátka se stejným barevným schématem jsou od sebe nerozlišitelná. Kolika způsoby můžeme z chlívků vybrat 70hlavě podstádo?

Úloha 15. (těžší) Nezáporná celá čísla jsou rozdělena do několika (alespoň dvou) disjunktních nekonečných aritmetických posloupností s diferencemi $d_1, \dots, d_k$. 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 špičce“ a na každou hranu nakreslí 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:

$$\begin{aligned} 8 &= 1 \cdot 1 + 1 \cdot 3 + 1 \cdot 3 + 1 \cdot 1 = \binom{3}{0} \cdot 1 + \binom{2}{0} \cdot 3 + \binom{1}{0} \cdot 3 + \binom{0}{0} \cdot 1, \\ 12 &= 3 \cdot 1 + 2 \cdot 3 + 1 \cdot 3 + 0 \cdot 1 = \binom{3}{1} \cdot 1 + \binom{2}{1} \cdot 3 + \binom{1}{1} \cdot 3 + \binom{0}{1} \cdot 1, \\ 6 &= 3 \cdot 1 + 1 \cdot 3 + 0 \cdot 3 + 0 \cdot 1 = \binom{3}{2} \cdot 1 + \binom{2}{2} \cdot 3 + \binom{1}{2} \cdot 3 + \binom{0}{2} \cdot 1. \end{aligned}$$

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 označme 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 obsažena. 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. $\square$

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 $(f_0(M), \dots, f_d(M))$, můžeme z těchto rovnic naopak dopočítat $(h_0(M), \dots, h_d(M))$:

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

To znamená, že jakýkoli poznatek o $(f_0(M), \dots, f_d(M))$ umíme přeložit do jazyka $(h_0(M), \dots, h_d(M))$ 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 $(f_0(M), \dots, f_d(M))$ na natočení nezávisí, nezávisí na něm ani $(h_0(M), \dots, h_d(M))$.

Až do teď to nevypadá, že by tohle všechno nějak souviselo s polynomy. Pojdme 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

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

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:

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

V předposledním rovnítku jsme využili binomické věty. □

Posloupnost $(h_0(M), \dots, h_d(M))$ je hezčí než $(f_0(M), \dots, f_d(M))$, protože platí $h_k = h_{d-k}$ pro každé $k = 0, \dots, d$. Proč? V definici jsme nějak otočili mnohostěn M . Obrátme 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 $(h_0(M), \dots, h_d(M))$ 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

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

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 platí⁷ $f_0(M) - f_1(M) + f_2(M) = 2$.*

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

⁷Jak 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. Nechtě v je vrchol M , z něž 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 $v_1, \dots, v_a$. Tím jsme přidali mnohostěnu M stěnu tvořenou a -úhelníkem $v_1 v_2 \dots v_a$. 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 $v_1, \dots, v_a$ 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. $\square$

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 $1 + x + x^2 + \dots$.
5. Prostě to spočítej a dosad.

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 převed 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 $P(x) = (1+x)(1+x^2)(1+x^3) \dots (1+x^n)$.
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 $F(x)^2 = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + 4x^3 + \dots$

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 dostat 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 jednaprvkových 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:

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

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

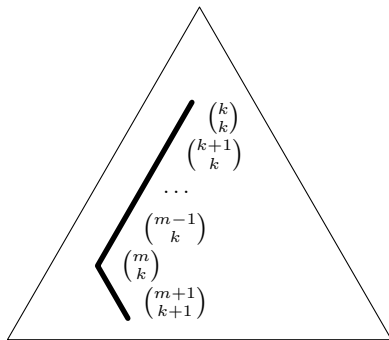
$$\binom{k+2}{k+1} + \binom{k+2}{k} + \binom{k+3}{k} + \dots$$

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

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

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 $(1 + x)^n = \sum_{k=0}^n \binom{n}{k} x^k$. Pojdme 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} zbudou dvojnásobek původního koeficientu. Nás zajímá součet původních koeficientů na sudých pozicích (to je počet sudých podmnožin), dobereme se ho proto dosazením jedničky a dělením 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 indukci 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 indukci 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 $P_{2^k}(x) \equiv (1+x^{2^k})P_0(x)$ 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 vynásobením $\frac{1}{1-x}$ 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 $1 + x^2 + x^4 + x^6 + \dots = \sum_{k=0}^{\infty} x^{2k} = \frac{1}{1 - x^2}$, zatímco ananasům analogicky odpovídá $1 + x^5 + x^{10} + \dots = \frac{1}{1 - x^5}$. 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 Fibonacchio 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 $\frac{F(x) - f_1 x - f_0}{x^2}$, 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 PraŠátek si můžeme vzít 0, 1, ..., nebo 30 kusů, což odpovídá polynomu $1 + x + \dots + x^{30} = \frac{x^{31} - 1}{x - 1}$. Stejnou interpretaci provedeme i s černými a flekatými PraŠátky. Součin odpovídajících tří polynomů nám pak v koeficientu u x^k říká, kolika způsoby lze vybrat k -hlavé stádo. Vyjádříme si součin a rozvíňme 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

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

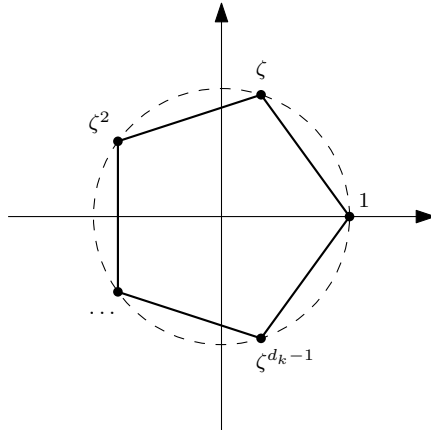
15. Stejně jako v ukázkovém příkladu se dobereme rovnosti

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

BÚNO at jsou difference seřazené vzestupně $d_1 \leq \dots \leq d_k$, pak dokážeme, že musí být $d_k = d_{k-1}$. Pro spor at není, tedy at 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 nejbliž k jedničce (takové mohou být dva, vybereme si kterýkoliv z nich), pak jsou kořeny $x^d - 1$ přesně $1, \zeta_d, \zeta_d^2, \dots, \zeta_d^{d-1}$, takže v $\mathbb{C}[x]$ rozložíme na součin

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



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 polynomm $x - \zeta$, 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 dvojnásobí $x - \zeta$ zkrátí se jmenovatelem a zbude $\frac{x^{a_k}}{-(x-1)(x-\zeta^2)(x-\zeta^3)\dots(x-\zeta^{d_k-1})}$. 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.

⁸Více se o nich můžeš dočíst třeba v tomto příspěvku:

<https://prase.cz/library/OdmocninyZJednickuLK/OdmocninyZJednickuLK.pdf>.