Cvičení k předmětu MB154 Diskrétní matematika

přednášející: doc. Lukáš Vokřínek, Ph. D.
cvičící: Mgr. Jan Procházka

podzim 2024

Obsah

Kapitola 1

Dělitelnost v $\mathbb{Z}$, největší společný dělitel, Bézoutova rovnost

1.1 Opakování z přednášky

Nechť d, $n \in \mathbb{Z}$. Řekneme, že d *dělí* n, pokud $\exists k \in \mathbb{Z}$ takové, že $n = d \cdot k$. Píšeme $d \mid n$ Také říkáme, že n je *dělitelné* d. Snadno se vidí, že $n \mid n$ a pokud $d \mid n$ a $n \mid m$, pak $d \mid m$. Jedná se tedy o předuspořádání na množině celých čísel. Dále platí, že pokud $a \mid b$ a $b \mid a$, pak $b = \pm a$. Až na znaménko se tedy jedná o uspořádání.

Největším společným dělitelem dvou čísel a, $b \in \mathbb{Z}$ rozumíme takové $d \in \mathbb{Z}$, že $d \mid a$, $d \mid b$ a každé $c \in \mathbb{Z}$ splňující $c \mid a$ a $c \mid b$ splňuje také $c \mid d$. Jedná se o společného dělitele největšího vzhledem k relaci $\mid$.

Věta. *Pro a, $b \in \mathbb{Z}$ existuje jejich největší společný dělitel.*

Tohoto dělitele zapisujeme $\mathrm{nsd}(a, b)$, $\gcd(a, b)$ nebo jen (a, b). Je určen jednoznačně až na znaménko.

Důkaz – Eukleidův algoritmus. Dělíme větší číslo menším se zbytkem. V následujícím kroku vždy vezmeme za nový dělenec dělitel z předchozího kroku a za nový dělitel zbytek z předchozího kroku. Protože se zbytky zmenšují (vůči dělitelnosti), po konečném počtu kroků dostaneme za zbytek nulu a algoritmus se zastaví. Poslední nenulový zbytek je největším společným dělitelem.

Protože při získávání zbytku se odečítají násobky dělence, nemění se společní dělitelé, tedy ani největší společný dělitel. □

Pokud $(a, b) = 1$, nazýváme tato čísla *nesoudělnými*. Uvedeme některé vlastnosti největšího společného dělitele:

$$(a, b) = (b, a) \tag{1.1}$$

$$(a, b) = (a, b + a\,k) \tag{1.2}$$

$$(a, b) = 1 \Rightarrow (a, b\,c) = (a, c) \tag{1.3}$$

Vlastnost (1.2) vlastně odpovídá Eukleidovu algoritmu.

Věta (Bézoutova rovnost)**.** *Nechť m, $n \in \mathbb{Z}$. Označme $d := (m, n)$. Poté existují p, $q \in \mathbb{Z}$ takové, že $p\,m + q, n = d$.*

Poznámka. Koeficienty p a q, nazývané Bézoutovými, nejsou určeny jednoznačně. Existuje totiž nekonečně mnoho dvojic čísel r a s takových, že $r\,m + s\,n = 0$ (například $r = k\,n$, $s = -k\,m$ pro $k \in \mathbb{Z}$). Pak $d = (p + r)\,m + (q + s)\,n$.

Důkaz. Koeficienty lze zjistit zpětným dosazováním do Eukleidova algoritmu. Největší společný dělitel si vyjádříme jako rozdíl dělence a násobku dělitele. Poté si vyjadřujeme dělence pomocí předchozích kroků algoritmu. □

Největšího společného dělitele i Bézoutovy koeficienty pro čísla m, n lze spočítat také úpravou matice

$$\begin{pmatrix} 1 & 0 & m \\ 0 & 1 & n \end{pmatrix}$$

elementárními řádkovými úpravami (nad $\mathbb{Z}$! – tedy jen přičtením k-násobku jednoho řádku k druhému, prohozením řádků a vynásobením jednoho řádku *invertibilním* číslem, tedy ± 1) do tvaru

$$\begin{pmatrix} p & q & d \\ r & s & 0 \end{pmatrix}$$

kde $p\,m + q\,n = d = (m, n)$ a $r\,m + s\,n = 0$. Během provádění úprav ve třetím sloupci provádíme vlastně Eukleidův algoritmus, tudíž d je skutečně (m, n). Navíc elementární řádkové úpravy zachovávají tu vlastnost, že součtem m-násobku prvního sloupce a n-násobku druhého sloupce dostaneme třetí sloupec, z čehož je vidět, že p a q jsou skutečně Bézoutovy koeficienty.

1.2 Příklady řešené na cvičení

Příklad 1.1. Dokažte, že pro všechna celá čísla n platí

- n^2 dává zbytek 0 nebo 1 po dělení 4,
- n^2 dává zbytek 0, 1 nebo 4 po dělení 8.

Řešení. Obecně máme-li určovat zbytek výrazu $f(n)$ po dělení d, musíme uvažovat $n = d\,k$, $n = d\,k + 1$, …, $n = d\,k + (d - 1)$. V některých případech si můžeme situaci zjednodušit znalostí výrazu $f(n)$. Protože $(d\,k + c)^2 = d^2\,k^2 + 2d\,k\,c + c^2$, stačí uvažovat d' takové, že d'^2 i $2d'$ jsou dělitelné d.

- Stačí uvažovat $n = 2\,k$ nebo $n = 2\,k + 1$. Pak

$$n^2 = (2\,k)^2 = 4\,k^2$$

nebo

$$n^2 = (2\,k+1)^2 = 4\,k^2 + 4\,k + 1 = 4\,(k^2+k) + 1$$

tedy zbytek n^2 po dělení 4 je skutečně 0 nebo 1.

- Z předchozího bodu bychom mohli již vyvodit, že zbytek n^2 po dělení 8 je 0, 1, 4 nebo 5. Na důkaz budeme potřebovat uvažovat $n = 4\,k$, $n = 4\,k+1$, $n = 4\,k+2$ nebo $n = 4\,k-1$ (poslední protože $4\,k+3 = 4\,(k+1)-1$). Pak

$$\begin{aligned} n^2 &= (4\,k)^2 = 16\,k^2 = 8\,(2\,k^2), \\ n^2 &= (4\,k+1)^2 = 16\,k^2 + 8\,k + 1 = 8\,(2\,k^2+k) + 1, \\ n^2 &= (4\,k+2)^2 = 16\,k^2 + 16\,k + 4 = 8\,(2\,k^2+2\,k) + 4 \end{aligned}$$

nebo

$$n^2 = (4\,k-1)^2 = 16\,k^2 - 8\,k + 1 = 8\,(2\,k^2-k) + 1.$$

Zbytek po dělení n^2 osmi je tedy skutečně 0, 1 nebo 4. △

Příklad 1.2. Najděte největšího společného dělitele čísel 89, 55 a čísel 157, 58.

Řešení. Použijeme Eukleidův algoritmus. Dělíme postupně se zbytkem.

$$\begin{aligned} 89 &= 55\cdot 1 + 34 \\ 55 &= 34\cdot 1 + 21 \\ 34 &= 21\cdot 1 + 13 \\ 21 &= 13\cdot 1 + 8 \\ 13 &= 8\cdot 1 + 5 \\ 8 &= 5\cdot 1 + 3 \\ 5 &= 3\cdot 1 + 2 \\ 3 &= 2\cdot 1 + 1 \\ 2 &= 1\cdot 2 + 0 \end{aligned} \qquad \begin{aligned} 157 &= 58\cdot 2 + 41 \\ 58 &= 41\cdot 1 + 17 \\ 41 &= 17\cdot 2 + 7 \\ 17 &= 7\cdot 2 + 3 \\ 7 &= 3\cdot 2 + 1 \\ 3 &= 1\cdot 3 + 0 \end{aligned}$$

Vidíme, že $(89, 55) = 1$ a $(157, 58) = 1$. Obě dvojice čísel jsou nesoudělné. △

Poznámka. Výpočet Eukleidova algoritmu je někdy možné zkrátit užitím záporných zbytků. Vždy pak vybíráme zbytek s menší absolutní hodnotou. V případě čísel 89 a 55 se výpočet zkrátí výrazně.

$$\begin{aligned} 89 &= 55\cdot 2 - 21 \\ 55 &= 21\cdot 3 - 8 \\ 21 &= 8\cdot 3 - 3 \\ 8 &= 3\cdot 3 - 1 \\ 3 &= 1\cdot 3 + 0 \end{aligned}$$

Příklad 1.3. Nejděte největšího společného dělitele a Bézoutovy koeficienty pro dvojice čísel 157, 58 a 123, 91.

Řešení. Vezměme si výpočet $(157, 58)$ Eukleidovým algoritmem a vyjádříme si zbytky.

$$\begin{aligned} 157 &= 58 \cdot 2 + 41 & &\rightsquigarrow & 41 &= 157 - 2 \cdot 58 \\ 58 &= 41 \cdot 1 + 17 & &\rightsquigarrow & 17 &= 58 - 41 \\ 41 &= 17 \cdot 2 + 7 & &\rightsquigarrow & 7 &= 41 - 2 \cdot 17 \\ 17 &= 7 \cdot 2 + 3 & &\rightsquigarrow & 3 &= 17 - 2 \cdot 7 \\ 7 &= 3 \cdot 2 + 1 & &\rightsquigarrow & 1 &= 7 - 2 \cdot 3 \end{aligned}$$

Následně počítáme

$$\begin{aligned} (157, 58) = 1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 = \\ = 5 \cdot (41 - 2 \cdot 17) - 2 \cdot 17 = 5 \cdot 41 - 12 \cdot 17 = \\ = 5 \cdot 41 - 12 \cdot (58 - 41) = 17 \cdot 41 - 12 \cdot 58 = \\ = 17 \cdot (157 - 2 \cdot 58) - 12 \cdot 58 = 17 \cdot 157 - 46 \cdot 58. \end{aligned}$$

Můžeme také počítat metodou úpravy matic.

$$\begin{pmatrix} 1 & 0 & 157 \\ 0 & 1 & 58 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 41 \\ 0 & 1 & 58 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 41 \\ -1 & 3 & 17 \end{pmatrix} \sim \begin{pmatrix} 3 & -8 & 7 \\ -1 & 3 & 17 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 3 & -8 & 7 \\ -7 & 19 & 3 \end{pmatrix} \sim \begin{pmatrix} 17 & -46 & 1 \\ -7 & 19 & 3 \end{pmatrix} \sim \begin{pmatrix} 17 & -46 & 1 \\ -58 & 157 & 0 \end{pmatrix}$$

Vidíme, že $17 \cdot 157 - 46 \cdot 58 = 1 = (157, 58)$ a $-58 \cdot 157 + 157 \cdot 58 = 0$. Pro druhou dvojici čísel 123 a 91 počítáme již jen úpravou matic.

$$\begin{pmatrix} 1 & 0 & 123 \\ 0 & 1 & 91 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 32 \\ 0 & 1 & 91 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 32 \\ -3 & 4 & -5 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} -17 & 23 & 2 \\ -3 & 4 & -5 \end{pmatrix} \sim \begin{pmatrix} -17 & 23 & 2 \\ -37 & 50 & -1 \end{pmatrix} \sim \begin{pmatrix} -91 & 123 & 0 \\ -37 & 50 & -1 \end{pmatrix} \sim \begin{pmatrix} 37 & -50 & 1 \\ -91 & 123 & 0 \end{pmatrix}$$

Tudíž $37 \cdot 123 - 50 \cdot 91 = 1 = (123, 91)$ a $-91 \cdot 123 + 123 \cdot 91 = 0$. △

Příklad 1.4. Zjistěte, pro která $n \in \mathbb{N}$ je číslo $n^3 - n^2 + 2\,n + 1$ dělitelné číslem $n - 2$.

Řešení. Díváme se na výrazy jako na polynomy. Pak můžeme využít metodu dělení polynomu se zbytkem. Platí

$$n^3 - n^2 + 2\,n + 1 = (n - 2)\,(n^2 + n + 4) + 9.$$

Jistě $n - 2 \mid (n - 2)\,(n^2 + n + 4)$. Má-li $n - 2$ dělit $n^3 - n^2 + 2\,n + 1$, musí dělit také rozdíl $n^3 - n^2 + 2\,n + 1 - (n - 2)\,(n^2 + n + 4) = 9$. Tedy hledáme, kdy $n - 2$ dělí 9. Pro $n - 2 > 9$

to jistě neplatí ($a \mid b \Rightarrow a \leq b$), stačí tedy uvažovat $n \leq 11$. Vidíme, že pak to je jen pro $n \in \{1, 3, 5, 11\}$.

Pokud bychom uvažovali úlohu pro všechna celá čísla, mohli bychom získat podobně omezení zdola ($n \geq -7$) a n by mohlo být ještě -1 nebo -7. △

Příklad 1.5. Zjistěte pro která $n \in \mathbb{N}$ je $7n + 1$ dělitelné $3n + 4$.

Řešení. Předpokládejme, že $3n + 4 \mid 7n + 1$. Jistě $3n + 4 \mid -6n - 8$. Pak $3n + 4 \mid (7n + 4) - (6n + 8) = n - 7$. Posloupnosti $3n + 4$ a $n - 7$ jsou aritmetické, přičemž $3n + 4$ roste rychleji než $n - 7$. Pokud budou obě kladné a $3n + 4 > n - 7$ pak $n - 7$ (a tudíž ani $7n + 1$) nebude dělitelné $3n + 4$. To nastane pro $n \geq 8$. Stačí otestovat dělitelnost pro $n = 1, \ldots, 7$. Zapíšeme si hodnoty do tabulky.

n	1	2	3	4	5	6	7
$3n + 4$	7	10	13	16	19	22	25
$n - 7$	-6	-5	-4	-3	-2	-1	0

Vidíme, že pouze pro $n = 7$ bude $3n+4$ dělit $7n+1$. Skutečně $3 \cdot 7+4 = 25$ dělí $7 \cdot 7+1 = 50$.

Uvažovali-li bychom úlohu pro celá čísla, získali bychom podobně i omezení zdola (musí být $n \geq -5$) a zjistili bychom, že n může být ještě -1 nebo -3. △

Příklad 1.6. Najděte největšího společného dělitele čísel $2^{63} - 1$ a $2^{28} - 1$.

Řešení. Počítání s čísly by bylo náročné, můžeme však úlohu zobecnit a počítat největšího společného dělitele polynomů $n^{63} - 1$ a $n^{28} - 1$. Jejich hodnoty v 2 jsou totiž právě naše čísla.[1] Hodnota největšího společného dělitele těchto polynomů v 2 bude tak největším společným dělitelem těchto čísel. Počítáme Eukleidovým algoritmem

$$\begin{aligned} n^{63} - 1 &= (n^{28} - 1)\,(n^{35} + n^7) + n^7 - 1 \\ n^{28} - 1 &= (n^7 - 1)\,(n^{21} + n^{14} + n^7 + 1) + 0 \end{aligned}$$

přičemž druhá rovnost je vlastně vzorečkem pro částečný součet geometrické řady s kvocientem n^7. Platí tedy $n^7 - 1 = (n^{63} - 1, n^{28} - 1)$ a tedy $(2^{63} - 1, 2^{28} - 1) = 127$. Navíc máme i koeficienty Bézoutovy rovnosti: $127 = (2^{63} - 1) - (2^{35} + 2^7)\,(2^{28} - 1)$. △

Příklad 1.7. Označme F_n členy Fibonacciho posloupnosti, tj. $F_0 := 0$, $F_1 := 1$ a $F_n = F_{n-1} + F_{n-2}$ pro $n \geq 2$. Spočítejte (F_n, F_{n-1}), (F_n, F_{n-2}), (F_n, F_{n-3}), (F_n, F_{n-4}).

Řešení. $(F_n, F_n - 1)$ určíme indukcí vůči n. Pokud $n = 1$, máme $(F_1, F_0) = (1, 0) = 1$. Předpokládejme, že $n \geq 2$ a pro všechna $m < n$ je $(F_m, F_{m-1}) = 1$. Můžeme použít rekurentní vztah.

$$(F_n, F_{n-1}) = (F_{n-1} + F_{n-2}, F_{n-1}) \overset{(1.2)}{=} (F_{n-2}, F_{n-1}) \overset{\text{I. P.}}{=} 1 \tag{1.4}$$

[1] Samozřejmě bychom mohli počítat rovnou s číselnými výrazy stejně jako s polynomy,

Dva po sobě jsoucí členy Fibonacciho posloupnosti jsou tedy nesoudělné. Aby dávaly ostatní výrazy smysl, musí být $n \geq 2$, takže můžeme rovnou použít rekurentní vztah.

$$(F_n, F_{n-2}) = (F_{n-1} + F_{n-2}, F_{n-2}) \overset{(1.2)}{=} (F_{n-1}, F_{n-2}) \overset{(1.4)}{=} 1$$

Dále počítáme podobně

$$(F_n, F_{n-3}) = (F_{n-1} + F_{n-2}, F_{n-3}) = (2\,F_{n-2} + F_{n-3}, F_{n-3}) \overset{(1.2)}{=}$$
$$= (2\,F_{n-2}, F_{n-3}) \overset{(1.3),\,(1.4)}{=} (2, F_{n-3}) = \begin{cases} 2 & F_{n-3} \text{ sudé} \\ 1 & F_{n-3} \text{ liché} \end{cases} \tag{1.5}$$

a

$$(F_n, F_{n-4}) \overset{(1.5)}{=} (2\,F_{n-2} + F_{n-3}, F_{n-4}) = (3\,F_{n-3} + 2\,F_{n-4}, F_{n-4}) \overset{(1.2)}{=}$$
$$= (3\,F_{n-3}, F_{n-4}) \overset{(1.3),\,(1.4)}{=} (3, F_{n-4}) = \begin{cases} 3 & 3 \mid F_{n-4} \\ 1 & \text{jinak} \end{cases} \qquad \triangle$$

Dodatková úloha. Dokažte, že pro m, $n \in \mathbb{N}$ platí $(F_m, F_n) = F_{(m,n)}$.

Řešení podle [2]. Nejprve dokážeme pomocná tvrzení.

i) Platí
$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$$
což dokážeme indukcí. Pro $n = 1$ tvrzení platí. Předpokládejme platnost pro n, dokážeme ji pro $n+1$.

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n+1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \overset{\text{I. P.}}{=} \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} F_n & F_{n-1} + F_n \\ F_{n+1} & F_n + F_{n+1} \end{pmatrix} = \begin{pmatrix} F_n & F_{n+1} \\ F_{n+1} & F_{n+2} \end{pmatrix}$$

ii) Platí $F_{m+n} = F_{m-1}\,F_n + F_m\,F_{n+1} = F_{m+1}\,F_n + F_m\,F_{n-1}$. Toto dokážeme z i). Máme totiž

$$\begin{pmatrix} F_{m+n-1} & F_{m+n} \\ F_{m+n} & F_{m+n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{m+n} \overset{\text{i)}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^m \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \overset{\text{i)}}{=}$$
$$= \begin{pmatrix} F_{m-1} & F_m \\ F_m & F_{m+1} \end{pmatrix} \cdot \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} = \begin{pmatrix} F_{m-1}\,F_{n-1} + F_m\,F_n & F_{m-1}\,F_n + F_m\,F_{n+1} \\ F_m\,F_{n-1} + F_{m+1}\,F_n & F_m\,F_n + F_{m+1}\,F_{n+1} \end{pmatrix}$$

přičemž požadované rovnosti najdeme na antidiagonále.

[2] `https://www.cut-the-knot.org/arithmetic/algebra/FIbonacciGCD.shtml`

iii) F_m dělí $F_{m\,k}$. Toto dokážeme indukcí vůči k. Pro $k = 1$ (nebo $k = 0$) tvrzení platí – $F_m \mid F_m \mid 0$. Předpokládejme, že $F_m \mid F_{m\,k}$ a počítejme

$$F_{m\,(k+1)} = F_{m\,k+m} \overset{\text{ii)}}{=} F_{m\,k}\,F_{m+1} + F_m\,F_{m\,k-1}$$

přičemž F_m dělí oba sčítance vpravo podle indukčního předpokladu.

iv) $(F_m, F_{m\,k+1}) = 1$. Toto je důsledkem iii), máme tedy $F_{m\,k} = F_m \cdot d$ pro nějaké d. Dále máme podle (1.4) Bézoutovu rovnost $(F_{m\,k}, F_{m\,k+1}) = 1 = k \cdot F_{m\,k+1} + l \cdot F_{m\,k} = k \cdot$ $\cdot F_{m\,k+1} + l \cdot d \cdot F_m$.

Bez újmy na obecnosti položme $n = m\,k + r$. Počítejme

$$(F_m, F_n) = (F_m, F_{m\,k+r}) \overset{\text{ii)}}{=} (F_m, F_{m\,k+1}\,F_r + F_{m\,k}\,F_{r-1}) \overset{\text{iii), (1.2)}}{=}$$
$$= (F_m, F_{m\,k+1}\,F_r) \overset{\text{iv), (1.3)}}{=} (F_m, F_r)$$

což je vlastně Eukleidův algoritmus pro indexy Fibonacciho posloupnosti. Po konečně mnoha krocích bychom tedy dospěli k tomu, že $(F_m, F_n) = (F_{(m,n)}, F_0) = F_{(m,n)}$, což jsme měli dokázat.

Z dokázeného bychom mohli vyřešit předchozí (mírně pozměněnou) úlohu. Můžeme například říct, že $(F_n, F_{n+1}) = F_{(n,n+1)} = F_{(n,1)} = F_1 = 1$. Podobně $(F_n, F_{n+2}) = F_{(n,2)} = 1$, jelikož $F_1 = F_2 = 1$. $(F_n, F_{n+3}) = F_{(n,3)}$ což je $F_1 = 1$ nebo $F_3 = 2$. $(F_n, F_{n+4}) = F_{(n,4)}$, což je $F_1 = F_2 = 1$ nebo $F_4 = 3$. Dále můžeme například říct, že $(F_n, F_{2\,n}) = F_n$. △

1.3 Příklady k procvičení

Příklad 1.8. Doakžte, že pro všechna celá čísla n platí: n^3 dává zbytek 0, 1 nebo 8 po dělení 9. (Uvažujte $n = 3\,k$, $n = 3\,k + 1$ nebo $n = 3\,k + 2$.)

Příklad 1.9. Spočtěte Bézoutovy koeficienty pro největší společné dělitele $(85, 49)$ a $(109, 46)$. (Výsledky: například $15 \cdot 85 - 26 \cdot 49 = 1$, $19 \cdot 109 - 45 \cdot 46 = 1$.)

Příklad 1.10. Zjistěte, pro která přirozená čísla n je číslo $n^3 + 4\,n^2 - n + 5$ dělitelné číslem $n + 2$. (Výsledek: $n = 1$, 3, 13.)

Příklad 1.11. Zjistěte, pro která přirozená čísla n je číslo $n^3 - n^2 + n - 8$ dělitelné číslem $n^2 - 2\,n + 3$. (Výsledek: $n = 4$.)

Příklad 1.12. Posloupnost a_n je zadána rekurentně: $a_0 = 1$, $a_1 = 1$, $a_n = 3\,a_{n-1} + 2\,a_{n-2}$ pro $n \geq 2$. Dokažte prvně, že a_n je liché a pak spočtěte rekurentně (a_n, a_{n-1}). (Výsledek: $(a_n, a_{n-1}) = 1$.)

Kapitola 2

Kongruence, modulární inverze

2.1 Opakování z přednášky

Přirozené číslo n nazveme *prvočíslem*, jsou-li jeho děliteli pouze 1 a p. Číslo, které není prvočíslem nazýváme *složeným*. Množinu všech prvočísle značíme zpravidla $\mathbb{P}$.

Věta (Základní věta aritmetiky)**.** *Libovolné číslo $n \in \mathbb{N}$ lze rozložit na součin prvočísel, a to jednoznačně až na pořadí činitelů.*

Poznámka. Prvočíslo p je součinem jediného prvočísla, 1 je součinem prázdné množiny prvočísel.

Dávají-li a a b stejný zbytek po dělení m, nazýváme je *kongruentními modulo m*, což píšeme $a \equiv b \pmod m$. Máme následující charakterizaci kongruence.

$$a \equiv b \pmod m \iff a = b + m\,k \text{ pro nějaké } k \in \mathbb{Z} \iff m \mid a - b$$

Dále je kongruence modulo m *reflexivní*, tj. $a \equiv a$, *symetrická*, tj. $a \equiv b \Rightarrow b \equiv a$, a *tranzitivní*, tj. $a \equiv b$ a $b \equiv c$ dává $a \equiv c$. Jedná se tedy o relaci ekvivalence. Dále platí $a \equiv b \pmod m$ dává $a \equiv b + k \cdot m \pmod m$.

Kongruence podle téhož modulu lze sčítat a násobit stejným číslem, lze je násobit i umocnit na totéž číslo. Dále je-li $(m, k) = 1$, pak

$$a\,k \equiv b\,k \pmod m \Rightarrow a \equiv b \pmod m.$$

Pro $n \mid m$ nám kongruence modulo m dává kongruenci modulo m. Obráceně dostáváme m/n různých řešení, $a \equiv b$ nebo $a \equiv b + n$, …, $a \equiv b + (m/n - 1)n \pmod m$. Dále je-li $[m_1, m_2] = m1\,m_2/(m_1, m_2)$, máme

$$a \equiv b \pmod{m_1} \text{ i } \pmod{m_2} \iff a \equiv b \pmod{[m_1, m_2]}.$$

Stejným číslem můžeme násobit i dělit obě strany *a modul*, tj.

$$a \cdot k \equiv b \cdot k \pmod{m \cdot k} \iff a \equiv b \pmod m.$$

Číslo b nazýváme *inverzí* k číslu a *modulo m* (nebo také modulární inverzí), jestliže

$$a \cdot b \equiv 1 \pmod m.$$

Věta. *Modulární inverze k a modulo m existuje jediná právě tehdy, když $(a, m) = 1$.*

Důkaz. Zobrazení násobení a je díky vlastnosti dělení kongruencí injektivní, má tedy zbytková třída reprezentovatelná vzor. Protože je počet tříd m, jedná se o bijekci a vzor je jediný.

Obráceně, pokud jsou a a m soudělné, násobení a není injektivní a nulová třída má nenulový vzor. Existuje tedy nenulové b tak, že $a \cdot b \equiv 0 \pmod{m}$ a inverze nemůže existovat. □

Věta (Čínská zbytková věta (Sun-Tsu))**.** *Nechť $m_1, \ldots m_k \in \mathbb{N}$ jsou po dvou nesoudělné. Poté má soustava*

$$x \equiv c_i \pmod{m_i}$$

pro $i = 1, \ldots, k$, $c_i \in \mathbb{Z}$ jediné řešení modulo $m_1 \cdot \cdots \cdot m_k$.

2.2 Příklady řešené na cvičení

Příklad 2.1. Najděte zbytek po dělení čísla 5^{30} číslem 91, to samé pro $5^{3\,000\,000}$.

Řešení. Můžeme počítat mocniny 5 modulo 91. Máme $5^2 = 25$, dále

$$\begin{aligned}
5^3 &= 125 \equiv 34 & 5^8 &\equiv 47 \cdot 5 = 235 \equiv -38 \\
5^4 &\equiv 34 \cdot 5 = 170 \equiv -12 & 5^9 &\equiv -38 \cdot 5 = -190 \equiv -8 \\
5^5 &\equiv -12 \cdot 5 = -60 \equiv 31 & 5^{10} &\equiv -8 \cdot 5 = -40 \\
5^6 &\equiv 31 \cdot 5 = 155 \equiv 64 & 5^{11} &\equiv -40 \cdot 5 = -200 \equiv -18 \\
5^7 &\equiv 64 \cdot 5 = 320 \equiv 47 & 5^{12} &\equiv -18 \cdot 5 = -90 \equiv 1
\end{aligned}$$

vše modulo 91. Víme tedy, že $5^{12} \equiv 1 \pmod{91}$, tudíž

$$5^{30} = \left(5^{12}\right)^2 \cdot 5^6 \equiv 5^6 \equiv 64 \pmod{91}.$$

Jelikož 3 000 000 je dělitelné 12, máme rovnou $5^{3\,000\,000} \equiv 1 \pmod{91}$. △

Jiné řešení. Máme rozklad $91 = 7 \cdot 13$. Víme, že

$$\begin{aligned}
5^2 \equiv -1 \pmod{13} &\Rightarrow 5^{30} \equiv (-1)^{15} = -1 \pmod{13} \\
5 \equiv -2 \text{ a } 2^3 \equiv 1 \pmod{7} &\Rightarrow 5^{30} \equiv (-2)^{30} = 2^{30} \equiv 1^{10} = 1 \pmod{7}
\end{aligned}$$

Tudíž je 5^{30} kongruentní -1 modulo 13 a 1 modulo 7.

Předpokládejme $x \in \{0, \ldots, 90\}$ takové, že $5^{30} \equiv x \pmod{91}$. Poté $5^{30} \equiv x \pmod{13}$ i $\pmod{7}$. Podle Čínské zbytkové věty existuje jediné takové x mezi 0 a 90. Můžeme například procházet $7k + 1$ a hledat mezi nimi nějaké číslo kongruentní -1 modulo 13.

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$7k+1$	1	8	15	22	29	36	43	50	57	64	71	78	85

Vidíme, že $64 = 13 \cdot 5 - 1$, takže hledaným zbytkem je číslo 64.

U čísla $5^{3\,000\,000}$ je počítání jednodušší. Modulo 7 spočítáme stejně zbytek 1, zbývá spočítat zbytek modulo 13.

$$5^{3\,000\,000} \equiv (-1)^{1\,500\,000} = 1 \pmod{13}$$

Máme tedy hned (použijeme opět Čínskou zbytkovou větu) $5^{3\,000\,000} \equiv 1 \pmod{91}$. △

Příklad 2.2. Dokažte, že $25 \mid 72^{2n+2} - 47^{2n} + 28^{2n-1}$ pro každé $n \in \mathbb{N}$.

Řešení. Víme, že

$$\begin{aligned} 72 &\equiv -3 \pmod{25} \\ 47 &\equiv -3 \pmod{25} \\ 28 &\equiv 3 \pmod{25} \end{aligned}$$

tudíž

$$\begin{aligned} 72^{2n+2} - 47^{2n} + 28^{2n-1} &\equiv (-3)^{2n+2} - (-3)^{2n} + 3^{2n-1} = \\ &= 3^{2n+2} - 3^{2n} + 3^{2n-1} = 3^{2n-1}(27 - 3 + 1) = 3^{2n-1} \cdot 25 \equiv 0 \pmod{25} \end{aligned}$$

což jsme měli dokázat. △

Příklad 2.3. Spočtěte 35^{-1} modulo 132.

Řešení. Počítáme $(132, 35)$ a Bézoutovy koeficienty (například) pomocí úprav matice.

$$\begin{pmatrix} 1 & 0 & 132 \\ 0 & 1 & 35 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & 27 \\ 0 & 1 & 35 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & 27 \\ -1 & 4 & 8 \end{pmatrix} \sim \begin{pmatrix} 4 & -15 & 3 \\ -1 & 4 & 8 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 4 & -15 & 3 \\ -9 & 34 & 2 \end{pmatrix} \sim \begin{pmatrix} 13 & -49 & 1 \\ -9 & 34 & 2 \end{pmatrix} \sim \begin{pmatrix} 13 & -49 & 1 \\ -35 & 132 & 0 \end{pmatrix}$$

Máme tedy $13 \cdot 132 - 49 \cdot 35 = 1$, neboli $-49 \cdot 35 \equiv 1 \pmod{132}$. Hledanou modulární inverzí je tedy $-49 \equiv 83 \pmod{132}$. △

Jiné řešení. Víme, že $132 = 2^2 \cdot 3 \cdot 11$ a $35 = 5 \cdot 7$, takže $(35, 132) = 1$ a modulární inverze existuje. Použijeme metodu rozkladu. Hledáme tedy x takové, že

$$35\,x \equiv 1 \pmod{4}, \quad \pmod{3} \text{ i } \pmod{11}$$

Neboť $36 = 4 \cdot 9$, vidíme, že $x \equiv -1 \pmod{4}$. Rovněž $36 = 3 \cdot 12$, tedy také $x \equiv -1 \pmod{3}$. Nakonec $33 = 3 \cdot 11$, takže

$$\begin{aligned} 35\,x \equiv 2\,x \equiv 1 &\pmod{11} \mid \cdot 6 \\ 12\,x \equiv x \equiv 6 &\pmod{11} \end{aligned}$$

Z $(4, 3) = 1$ víme, že $x \equiv -1 \pmod{4 \cdot 3 = 12}$, tedy mezi čísly tvaru $12\,k - 1$ hledáme číslo tvaru $11\,l - 6$. Jinými slovy hledáme mezi čísly tvaru $11\,l + 7$ číslo dělitelné 12.

l	0	1	2	3	4	5	6	7	8	9	10	11
$11\,l+7$	7	18	29	40	51	62	73	84	95	106	117	128

Vidíme, že se jedná o číslo 84, hledanou modulární inverzí je tedy 83.

Při hledání x jsme si úlohu rozložili na řešení soustavy kongruencí

$$\begin{aligned} 35\,x &\equiv 1 \pmod 4 \\ 35\,x &\equiv 1 \pmod 3 \\ 35\,x &\equiv 1 \pmod{11} \end{aligned}$$

kterou jsme si převedli na

$$\begin{aligned} x &\equiv -1 \pmod{12} \\ x &\equiv 6 \pmod{11}. \end{aligned}$$

Tuto soustavu lze řešit také tak, že si z první kongruence vyjádříme $x = 12\,k - 1$, které následně dosadíme do druhé kongruence, kterou řešíme. Pak máme

$$\begin{aligned} 12\,k - 1 &\equiv 6 \pmod{11} \\ 12\,k &\equiv 7 \pmod{11} \\ k &\equiv 7 \pmod{11} \end{aligned}$$

tedy $k = 11\,l + 7$. Následně $x = 12\,k - 1 = 12 \cdot (11\,l + 7) - 1 = 132\,l + 83$, tedy $x \equiv 83 \pmod{132}$. △

Příklad 2.4. Spočítejte 55^{-1} modulo 132.

Řešení. Máme rozklady $132 = 2^2 \cdot 3 \cdot 11$ a $55 = 5 \cdot 11$. Tedy $(132, 55) = 11 > 1$ a modulární inverze neexistuje. Skutečně například $12 \not\equiv 0 \pmod{132}$, ale $55 \cdot 12 = 5 \cdot 132 \equiv 0 \pmod{132}$. △

Příklad 2.5. Dokažte, že $n = (893^5 + 4)^{20} - 1$ je dělitelné číslem $176 = 11 \cdot 16$.

Řešení. Neboť $(11, 16) = 1$, stačí dokázat, že n je dělitelné 11 i 16. Díky $880 = 80 \cdot 11 = 55 \cdot 16$ víme, že $893 \equiv 2 \pmod{11}$ a $893 \equiv -3 \pmod{16}$. Poté

$$\begin{aligned} n &\equiv (2^5 + 4)^{20} - 1 = 36^{20} - 1 && \text{díky } 893 \equiv 2 \pmod{11} \\ &\equiv 3^{20} - 1 && \text{neboť } 36 \equiv 3 \pmod{11} \\ &\equiv (-2)^{10} - 1 = 2^{10} - 1 && \text{jelikož } 3^2 \equiv -2 \pmod{11} \\ &\equiv (-1)^2 - 1 = 0 \pmod{11} && \text{protože } 2^5 \equiv -1 \pmod{11}. \end{aligned}$$

Podobně

$$\begin{aligned} n &\equiv \Big((-3)^5 + 4\Big)^{20} - 1 && \text{kvůli } 893 \equiv -3 \pmod{16} \\ &\equiv (-3+4)^{20} - 1 = 1^{20} - 1 = 0 && \text{protože } (-3)^4 = 81 \equiv 1 \pmod{16}. \end{aligned}$$

Tudíž také $n \equiv 0 \pmod{176}$, což jsme měli dokázat. △

Příklad 2.6. Dokažte, že pro každé $n \in \mathbb{N}$ je $4^{2n+1} - 10n - 4$ dělitelné 25.

Nápověda. Použijte $16^n - 1 = (16-1)(1 + 16 + \cdots + 16^{n-1} \equiv 15n \pmod{25}$.

Řešení. Nejprve indukcí dokážeme tvrzení z nápovědy. Pro $n = 1$ máme $16 - 1 = 15 \equiv 15 \pmod{25}$. Předpokládejme nyní, že tvrzení platí pro n a počítejme pro $n+1$:

$$16^{n+1} - 1 = 16 \cdot (16^n - 1) + 16 - 1 \overset{\text{I. P.}}{\equiv} 16 \cdot 15n + 16 - 1 = \\ = 225n + 15 \cdot (n+1) \equiv 15 \cdot (n+1) \pmod{25}$$

neboť $25 \mid 225$. Pak je důkaz jednoduchý:

$$4^{2n+1} - 10n - 4 = 4 \cdot (16^n - 1) - 10n \equiv 4 \cdot 15n - 10n = 50n \equiv 0 \pmod{25}$$

tedy opravdu 25 dělí $4^{2n+1} - 10n - 4$ pro každé $n \in \mathbb{N}$. △

Příklad 2.7. Dokažte, že číslo $5^{20} + 2^{30}$ je složené.

Řešení. Chceme najít nějaké číslo (větší než 1), které dělí naše $5^{20} + 2^{30}$. Víme, že

$$5^2 \equiv -1 \pmod{13} \qquad\qquad 2^6 \equiv -1 \pmod{13}$$

(první kongruence je jasná, u druhé si vzpomeneme na cvičení 2.1). Pak

$$5^{20} + 2^{30} = \left(5^2\right)^{10} + \left(2^6\right)^5 \equiv (-1)^{10} + (-1)^5 = 1 - 1 = 0 \pmod{13}$$

a tedy $13 \mid 5^{20} + 2^{30}$ a jedná se skutečně o číslo složené. △

Jiné řešení. Protože $5^{20} + 2^{30} = (5^4)^5 + (2^6)^5$ je součet dvou lichých mocnin, můžeme si vzpomenout na vzoreček a říci, že jako součin se jedná o číslo složené.

Odvodíme tedy pro připomenutí vzorečky pro součty lichých a rozdíly libovolných mocnin. Máme částečný součet geometrické řady

$$q^n - 1 = (q-1) \cdot (1 + q + \cdots + q^{n-1}). \tag{2.1}$$

Napíšeme-li si $q = \frac{a}{b}$ pro nějaká a, $b > 0$ a vynásobíme-li následně (2.1) b^n s tím, že na pravé straně násobíme první závorku b a druhou b^{n-1}, dostaneme vzorec pro rozdíl mocnin:

$$a^n - b^n = (a-b) \cdot (b^{n-1} + a\,b^{n-2} + a^2\,b^{n-3} + \cdots + a^{n-3}\,b^2 + a^{n-2}\,b + a^{n-1}). \tag{2.2}$$

Vzorec pro součet *lichých* mocnin lze již odvodit z (2.2). Dosazením $a = -c$ a s využitím toho, že pro liché mocniny a máme minus a pro sudé mocniny plus, dostáváme

$$-c^n - b^n = (-c-b) \cdot (b^{n-1} - c\,b^{n-2} + c^2\,b^{n-3} - \cdots + c^{n-3}\,b^2 - c^{n-2}\,b + c^{n-1})$$

z čehož po vynásobení -1 máme

$$c^n + b^n = (c+b) \cdot (b^{n-1} - c\,b^{n-2} + c^2\,b^{n-3} - \cdots + c^{n-3}\,b^2 - c^{n-2}\,b + c^{n-1}).$$

V našem případě pak

$$5^{20} + 2^{30} = \left(5^4\right)^5 + \left(2^6\right)^5 = \left(5^4 + 2^6\right) \cdot \left(5^{16} - 5^{12}\,2^6 + 5^8\,2^{12} - 5^4\,2^{18} + 2^{24}\right)$$

tedy $5^{20} + 2^{30}$ je číslo složené. Všimněme si, že $5^4 + 2^6 = 689 = 13 \cdot 53$. △

Příklad 2.8. Odvoďte pravidla pro dělitelnost 11, 9, 7 pomocí dekadického zápisu.

Řešení. Vezměme číslo $n \in \mathbb{N}$ a zapišme si ho jako $n = \sum_{i=0}^{r} a_i \, 10^i$ pro $a_i \in \{0, \dots, 9\}$. Začneme s dělitelností devíti. Neboť je $10 \equiv 1 \pmod 9$, máme

$$n = \sum_{i=0}^{r} a_i \, 10^i \equiv \sum_{i=0}^{r} a_i \pmod 9$$

čímž dostáváme známé pravidlo – n je dělitelné devíti právě, když je dělitelný jeho ciferný součet. Iterací dostaneme, že je dělitelné n právě, když je dělitelný jeho superciferný součet. Protože $9 = 3^2$, platí tento důkaz i pro trojku. Dělitelnost jedenácti lze řešit podobně, jelikož $10 \equiv -1 \pmod{11}$. Následně

$$n = \sum_{i=0}^{r} a_i \, 10^i \equiv \sum_{i=0}^{r} a_i \, (-1)^i = \sum_{i \text{ sudé}} a_i - \sum_{i \text{ liché}} a_i \pmod{11}$$

a dostáváme, že n je dělitelné jedenácti právě tehdy, když je dělitelný rozdíl součtů jeho sudých cifer a jeho cifer lichých. Opět můžeme postup iterovat. Pro dělitelnost sedmi již nelze použít čistě dekadický zápis, nicméně můžeme použít následující pozorování. Máme $7 \cdot 11 \cdot 13 = 1\,001$. Zapíšeme-li si n jako $n = \sum_{j=0}^{s} b_j \cdot 1\,000^j$ pro $b_j \in \{0, \dots, 999\}$, můžeme díky $1\,000 \equiv -1 \pmod{1\,001}$ říct, že

$$n = \sum_{j=0}^{s} b_j \cdot 1\,000^j \equiv \sum_{j=0}^{s} b_j \, (-1)^j = \sum_{j \text{ sudé}} b_j - \sum_{j \text{ liché}} b_j \pmod{1\,001}$$

a tedy i modulo 7, 11 i 13. Můžeme tedy říci, že je n dělitelné 7, 11 nebo 13 právě tehdy, je-li dělitelný rozdíl součtů jejich sudých a lichých trojčíslí. I tento postup lze samozřejmě iterovat, abychom nakonec skončili mezi 0 a 999. △

2.3 Příklady k procvičení

Příklad 2.9. Najděte zbytky po dělení čísel 10^{50} a $10^{5\,000\,000}$ číslem 13. (Výsledek: zbytky se začnou opakovat s periodou 6, obojí proto vyjde 9.)

Příklad 2.10. Dokažte, že pro libovolné $n \in \mathbb{N}$ je $13^{3n} + 15^{2n+1} - 21^{n+2}$ dělitelné 17. (Výsledek: využije se $13^3 \equiv 15^2 \equiv 21 \equiv 4 \pmod{17}$.)

Příklad 2.11. Spočtěte 55^{-1} modulo 117. (Výsledek: 100.)

Příklad 2.12. Spočtěte 45^{-1} modulo 117. (Výsledek: inverze neexistuje.)

Příklad 2.13. Dokažte, že $n := (893^5 + 9)^{30} - 1$ je dělitelné číslem $91 = 7 \cdot 13$. (Počítejte zvlášť modulo 7 a modulo 13.)

Kapitola 3

Řešení lineárních kongruencí, primitivní kořeny, Eulerova funkce

3.1 Opakování z přednášky

Řešíme kongruenci $a'x \equiv b' \pmod{n'}$. Můžeme si ji vydělit $d := (a', b', n')$ a dostat kongruenci

$$a\,x \equiv b \pmod{n}$$

kterou si převedeme přidáním vždy platné kongruence na soustavu

$$\begin{aligned} a\,x &\equiv b \pmod{n} \\ n\,x &\equiv 0 \pmod{n} \end{aligned}$$

a tu ekvivalentními úpravami převedeme do tvaru

$$\begin{aligned} x &\equiv c \pmod{n} \\ 0\,x &\equiv e \pmod{n} \end{aligned}$$

kde následně máme dvě možnosti:

- $e \equiv 0 \pmod{n}$, pak $x \equiv c \pmod{n}$ je řešení, modulo n' pak máme d řešení: $x \equiv c$, $x \equiv c + n$, $c + 2\,n$, $\ldots$, $x \equiv c + (d-1)\,n \pmod{n'}$;
- $e \not\equiv 0 \pmod{n}$, pak původní kongruence nemá řešení.

Soustavu kongruencí (mají-li každá jednotlivě řešení) si můžeme podle předchozího vždy převést do tvaru

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \end{aligned}$$

$$\vdots$$
$$x \equiv c_k \pmod{n_k}$$

která má řešení právě tehdy, když $c_i \equiv c_j \pmod{(n_i, n_j)}$. Toto řešení je pak jediné modulo $[m_1, \ldots, m_k]$. Soustavu řešíme tak, že si (třeba) z první kongruence vyjádříme parametricky $x = n_1 t_1 + c_1$, což následně dosadíme do (třeba) druhé kongruence, kterou vyřešíme vzhledem k t_1, tedy $t_1 = m_2 t_2 + c_2'$, což následně dosadíme za x a dosadíme do (například) třetí kongruence a postup iterujeme.

Eulerova funkce φ je pro přirozené číslo n zadaná následujícím předpisem

$$\varphi(n) = \left|\{m \in \mathbb{N} \mid m \leq n \text{ a } (m, n) = 1\}\right|.$$

Je celkem zřejmé, že pro prvočíslo p je $\varphi(p) = p - 1$. Dále $\varphi(p^k) = p^{k-1} \cdot (p-1)$. Eulerova funkce je *multiplikativní*, tj. pro a, b taková, že $(a, b) = 1)$ máme $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Napíšeme-li si tedy n jako součin mocnin prvočísel

$$n = p_1^{k_1} \cdot \cdots \cdot p_l^{k_l}$$

můžeme spočítat

$$\varphi(n) = p_1^{k_1 - 1} \cdot (p_1 - 1) \cdot \cdots \cdot p_l^{k_l - 1} \cdot (p_l - 1).$$

Věta (Eulerova)**.** *Pro a, n taková, že $(a, n) = 1$ platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Věta (malá Fermatova)**.** *Pro prvočíslo p a a jím nedělitelné platí $a^{p-1} \equiv 1 \pmod{p}$.*

Pro a a n taková, že $(a, n) = 1$ číslo r nazveme *řádem a modulo n*, jestliže se jedná o nejmenší číslo takové, že $a^r \equiv 1 \pmod{n}$, neboli pokud $a^{r'} \equiv 1 \pmod{n}$, pak $r \mid r'$. Existence řádu je zaručená Eulerovou větou.

Věta (Lagrangeova[1])**.** *Řád čísla a modulo n dělí $\varphi(n)$.*

Číslo a je *primitivní kořen modulo n*, jestliže pro každé b existuje k takové, že $a^k \equiv b \pmod{n}$.

Věta. *Primitivní kořen modulo prvočíslo existuje.*

Při hledání primitivního modulo p je potřeba najít číslo, jehož řád je právě $\varphi(p) = p - 1$. Díky Lagrangeově větě si můžeme vypsat všechny dělitele $p - 1$ do Hasseovského diagramu (uspořádaného dělitelností), kde následně stačí testovat modulo p „submaximální“ mocniny čísel a, tj. takové, které v Hasseovském diagramu leží těsně pod $p - 1$. Pokud by totiž byla kongrentní jedné i menší mocnina a, byla by jedné kongruentní i některá „submaximální“ mocnina.

[1] Jedná se o speciální případ Lagrangeovy věty o konečných grupách. Ta říká, že řád prvku grupy dělí řád grupy.

3.2 Příklady řešené na cvičení

Příklad 3.1. Vyřešte kongruenci $74\,x \equiv 22 \pmod{168}$.

Řešení. Kongruenci si můžeme přepsat do tvaru $37\,x \equiv 11 \pmod{84}$. Protože $(37, 84) = 1$, má kongruence jediné řešení. Přidáme si platnou kongruenci $84\,x \equiv 0 \pmod{84}$ a ekvivalentními úpravami řešíme soustavu kongruencí.

$$\left.\begin{aligned} 37\,x &\equiv 10 \\ 84\,x &\equiv 0 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} 10\,x &\equiv -22 \\ 37\,x &\equiv 11 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} 10\,x &\equiv -22 \\ -3\,x &\equiv 15 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} x &\equiv 23 \\ -3\,x &\equiv 15 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} x &\equiv 23 \\ 0\,x &\equiv 84 \end{aligned}\right\} \pmod{84}$$

Vidíme, že $x \equiv 23 \pmod{84}$. Pak $x \equiv 23$ nebo $107 = 84 + 23 \pmod{168}$. Skutečně

$$74 \cdot 23 = 1\,702 = 1\,680 + 22 \equiv 22 \pmod{168}$$
$$74 \cdot 107 = 74 \cdot 84 + 74 \cdot 23 = 37 \cdot 168 + 74 \cdot 23 \equiv 22 \pmod{168}$$

tedy máme dvě řešení modulo 168. △

Příklad 3.2. Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 10 \pmod{25} \\ x &\equiv 6 \pmod{11}. \end{aligned}$$

Řešení. Jelikož $(25, 11) = 1$, má podle Čínské zbytkové věty soustava řešení, a to mezi 0 a $11 \cdot 25 = 275$ jediné. Jedním ze způsobů řešení je vypisovat si do tabulky čísla tvaru $25\,k + 10$ a čísla tvaru $11\,l + 6$. Máme hodnoty

$$x \in \{10, 35, 60, 85, 110, 135, 160, 185, 210, 235, 260\}$$

a

$$x \in \{6, 17, 28, 39, 50, 61, 72, 83, 94, 105, 127, 138, 149, 160, \dots\}$$

přičemž vidíme, že $x = 160$ a dále počítat nemusíme. Tento způsob je jednoduchý, nicméně procházet mnoho čísel bývá zdlouhavé. △

Jiné řešení. Jinou možností je spočítat si Bézoutovy koeficienty pro čísla 25 a 11. Máme $1 = 4 \cdot 25 - 9 \cdot 11$ (ověřte sami), takže můžeme říci, že $4 \cdot 25 \equiv 1 \pmod{11}$ a $-9 \cdot 11 \equiv 1 \pmod{25}$. Můžeme v obou rovnicích představit jedničku, tedy

$$\begin{aligned} x &\equiv -9 \cdot 11 \cdot 10 \pmod{25} \\ x &\equiv 4 \cdot 25 \cdot 6 \pmod{11} \end{aligned}$$

přičemž každá z hodnot je kongruentní nule vůči druhému modulu. Vidíme tedy, že

$$x \equiv -9 \cdot 10 \cdot 11 + 4 \cdot 25 \cdot 6 = -390 \equiv 160$$

modulo 25 i modulo 11, tedy také modulo $11 \cdot 25 = 275$. △

Jiné řešení. Třetí metodou řešení je vyjádřit si z první rovnice x parametricky a dosadit do rovnice druhé. Z první rovnice vidíme, že $x = 25\,k + 10$. Poté řešíme

$$\begin{aligned} 25\,k + 10 &\equiv 6 \pmod{11} \\ 3\,k - 1 &\equiv 6 \pmod{11} \end{aligned}$$

neboť $25 \equiv 3$ a $10 \equiv -1 \pmod{11}$, pak

$$\begin{aligned} 3\,k &\equiv 7 \pmod{11} \\ k &\equiv 6 \pmod{11} \end{aligned}$$

kde v posledním kroku jsme si vynásobili kongruenci 4, jelikož $3 \cdot 4 = 12 \equiv 1$ a $7 \cdot 4 = 28 \equiv 6 \pmod{11}$, a tedy $k = 11\,l + 6$. Celkem

$$x = 25\,k + 10 = 25\,(11\,l + 6) + 10 = 275\,l + 160,$$

čímž dostáváme řešení $x \equiv 160 \pmod{275}$. △

Příklad 3.3. Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{15} \\ x &\equiv 4 \pmod{21} \\ x &\equiv 6 \pmod{25}. \end{aligned}$$

Řešení. Řešíme pouze metodou parametrického dosazování. Z první kongruence vyjádříme $x = 15\,k + 1$, dosazením do druhé kongruence získáme

$$\begin{aligned} 15\,k + 1 &\equiv 4 \pmod{21} \\ 15\,k &\equiv 3 \pmod{21} \end{aligned}$$

odtud zkrácením obou stran kongruence i modulu třemi

$$5\,k \equiv 1 \pmod{7}$$

$$k \equiv 3 \pmod 7$$

čímž dostáváme tři řešení, $k \equiv 3$, $k \equiv 10$ a $k \equiv 17 \pmod{21}$, nicméně všechna tato řešení lze psát dohromady jako $k = 7\,l + 3$. Máme tedy

$$x = 15\,k + 1 = 15\,(7\,l + 3) + 1 = 105\,l + 46$$

což dosadíme do třetí kongruence

$$\begin{aligned} 105\,l + 46 &\equiv 6 \pmod{25} \\ 105\,l &\equiv -40 \pmod{25} \\ 5\,l &\equiv 10 \pmod{25} \end{aligned}$$

neboť $105\,l \equiv 105\,l - 25 \cdot 4\,l = 5\,l$ a $-40 \equiv -40 + 2 \cdot 25 = 10 \pmod{25}$, dále zkrácením obou stran kongruence i modulu pěti

$$l \equiv 2 \pmod 5$$

takže máme řešení. Modulo 25 bychom dostali 5 řešení, $l \equiv 2$, 7, 12, 17 nebo $22 \pmod{25}$, nicméně všechna lze psát jako $l = 5\,t + 2$. Dosadíme tedy do x

$$x = 105\,l + 46 = 105\,(5\,t + 2) + 46 = 525\,t + 256$$

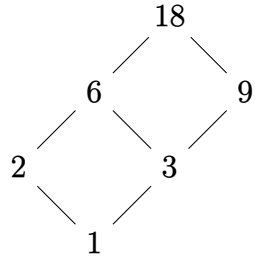
a máme řešení $x \equiv 256 \pmod{525}$, přičemž $525 = [15, 21, 25]$. Skutečně

$$\begin{aligned} 256 &= 1 + 15 \cdot 17 \\ &= 4 + 21 \cdot 12 \\ &= 6 + 25 \cdot 10 \end{aligned}$$

a jedná se o řešení. △

Příklad 3.4. Najděte primitivní kořen modulo 19 a modulo 53. Poté popište *všechny* primitivní kořeny.

Řešení. Protože 19 i 53 jsou prvočísla, v obou případech primitivní kořeny existují. Nejprve počítejme modulo 19. Podle Fermatovy věty pro každé $k \in \mathbb{N}$ máme $k^{18} \equiv 1 \pmod{19}$. Máme právě $18 = \varphi(19)$ čísel nesoudělných s 19, takže mají-li různé mocniny primitivního kořene dát všechny třídy kongruence, musí mít primitivní kořen řád 18. Řád obecného čísla modulo 19 je dělitelem 18 (Lagrangeova věta), tedy čísla mohou mít řád 1, 2, 3, 6, 9 nebo 18. Nakreslíme si Hasseovský diagram dělitelů 18 uspořádaný dělitelností



(3.1)

odkud vidíme, že stačí najít a takové, že a^6 ani a^9 není kongruentní 1 modulo 19. Pokud by totiž byla kongruentní jedné menší (v diagramu (3.1)) mocnina a, byla by 1 kongruentní i mocnina šestá nebo devátá. Hledáme tedy takové a. Jedna to nebude, zkusíme dvojku:

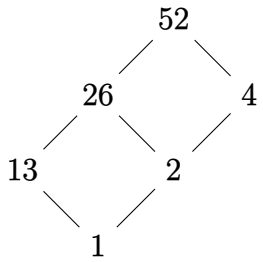
$$2^6 = 64 \equiv 7 \pmod{19}$$

neboť $19 \cdot 3 = 57$, dále

$$2^9 = 2^{6+3} = 2^6 \cdot 2^3 \equiv 7 \cdot 8 = 56 \equiv -1 \pmod{19}$$

kde jsme využili předchozího. Má tedy 2 řád 18 a je primitivním kořenem modulo 19. Ostatní primitivní kořeny jsou ty mocniny 2, kde je exponent nesoudělný s 18. Dále jsou primitivními kořeny tedy $2^5 \equiv 13$, $2^7 \equiv 14$, $2^{11} \equiv 15$, $2^{13} \equiv 3$ a $2^{17} \equiv 10 \pmod{19}$. Obecně počet primitivních kořenů bude $\varphi(18) = 6$.

Pro primitivní kořen modulo 53 hledáme číslo řádu 52, obecně mohou mít čísla řád 1, 2, 4, 13, 26 nebo 52. Nakreslíme si opět Hasseovský diagram dělitelů $52 = 13 \cdot 4$.



(3.2)

a vidíme, že stačí ověřovat čtvrtou a 26. mocninu. Můžeme zkoušet různá čísla, začneme opět dvojkou:

$$2^4 = 16$$

což není kongruentní 1, dále $2^6 = 64 \equiv 11 \pmod{53}$, tudíž

$$2^{26} = 2^{6\cdot 4+2} = (2^6)^4 \cdot 2^2 \equiv 11^4 \cdot 4 = (11^2)^2 \cdot 4 \pmod{53}$$

s využitím $11^2 = 121 \equiv 15 \pmod{53}$ máme

$$2^{26} \equiv 15^2 \cdot 4 = 15 \cdot (15 \cdot 4) = 15 \cdot 60 \equiv 15 \cdot 7 = 105 \equiv -1 \pmod{53}$$

kde jsme využili, že $60 \equiv 7 \pmod{53}$ a $2 \cdot 53 = 106$. Tudíž 2 má řád 52 a je primitivním kořenem modulo 53. Ostatní primitivní kořeny jsou právě ty mocniny 2, kde exponent je nesoudělný s 52. Je jich $\varphi(52) = 24$. △

Příklad 3.5. Určete $\varphi(10)$, $\varphi(100)$, $\varphi(1\,000)$ a $\varphi(256)$.

Řešení. Počítáme podle vzorců

$$\varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4,$$

u 10 by to šlo i odhadnout, nesoudělná jsou 1, 3, 7 a 9,

$$\begin{aligned}\varphi(100) &= \varphi(2^2)\cdot\varphi(5^2) = 1\cdot 2\cdot 4\cdot 5 = 40,\\ \varphi(1\,000) &= \varphi(2^3)\cdot\varphi(5^3) = 1\cdot 4\cdot 4\cdot 25 = 400,\\ \varphi(256) &= \varphi(2^8) = 1\cdot 2^7 = 128.\end{aligned}$$ △

Příklad 3.6. Nalezněte všechna $m \in \mathbb{N}$ taková, že $\varphi(m) = 38$, respektive $\varphi(m) = 16$.

Řešení. Máme rozklad $38 = 2\cdot 19$. Má-li $p \mid m$, musí $p-1 \mid 38$. Protože $19+1 = 20$ není prvočíslo, musí být $p-1 = 2$, tedy $p = 3$. Pak by mělo být $m = 3^k$, nicméně pak

$$\varphi(m) = 2\cdot 3^{k-1} = 2\cdot 19$$

přičemž 19 není mocnina 3. Tudíž takové m neexistuje.

Pro $\varphi(m) = 16$ máme $p \mid m \Rightarrow p-1 \mid 16$, a pokud by p dělilo m i ve vyšší mocnině, muselo by pak i $p \mid 16$. Děliteli 16 jsou 1, 2, 4, 8 a 16, mezi nimiž hledáme $p-1$. Pak p může být 2, 3, 5 nebo 17 (9 není prvočíslo), přičemž jedině 2 se může vyskytovat i ve vyšší mocnině. Můžeme si tedy rozepsat $m = 2^a\cdot 3^b\cdot 5^c\cdot 17^d$, kde b, c, $d \in \{0,1\}$. Procházíme všechny případy.

I) Nejprve vyřešme případ $17 \mid m$. Poté $m = 17\,k$ a $\varphi(m) = \varphi(17)\cdot\varphi(k) = 16\,\varphi(k) = 16$, tedy $\varphi(k) = 1$, tudíž $k = 1$ nebo 2. Máme tedy $m = 17$ nebo 34.

II) Pokud 17 nedělí m, máme $m = 2^a\cdot 3^b\cdot 5^c$, kde b, $c \in \{0,1\}$, tedy máme čtyři možnosti kombinací b a c, podle nichž vždy dopočítáme a. Pak máme

   i) $b = c = 0$: $m = 2^a$ a $\varphi(m) = 1\cdot 2^{a-1} = 16 = 2^4$, tedy $a = 5$ a $m = 32$;

   ii) $b = 1$, $c = 0$: $m = 2^a\cdot 3$ a $\varphi(m) = 2\cdot 2^{a-1} = 16$, pak $a = 4$ a $m = 48$;

   iii) $b = 0$, $c = 1$: $m = 2^a\cdot 5$ a $\varphi(m) = 2^{a-1}\cdot 4 = 16$, $a = 3$ a $m = 40$;

   iv) $b = c = 1$: $m = 2^a\cdot 3\cdot 5$ a $\varphi(m) = 2^{a-1}\cdot 8 = 16$, tudíž $a = 2$ a $m = 60$.

Dohromady pak může být $m \in \{17, 32, 34, 40, 48, 60\}$. △

3.3 Příklady k procvičení

Příklad 3.7. Vyřešte kongruenci $75\,x \equiv 21 \pmod{168}$. (Výsledek: $x \equiv 7 \pmod{56}$, případně $x \equiv 7$, 63 nebo 119 $\pmod{168}$.

Příklad 3.8. Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 10 \pmod{20}\\ x &\equiv 7 \pmod{13}.\end{aligned}$$

(Výsledek: $x \equiv 150 \pmod{260}$.)

Příklad 3.9. Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 4 \pmod 9 \\ x &\equiv 1 \pmod{15} \\ x &\equiv 16 \pmod{35}. \end{aligned}$$

(Výsledek: $x \equiv 121 \pmod{315}$.)

Příklad 3.10. Najděte primitivní kořen modulo 31. (Výsledek: $\varphi(31) = 2 \cdot 3 \cdot 5$, takže je potřeba zkontrolovat a^6, a^{10} a a^{15}; nevyjde sice 2, ale vyjde 3.)

Příklad 3.11. Určete $\varphi(45)$, $\varphi(90)$. (Výsledek: $\varphi(45) = \varphi(90) = 24$.)

Příklad 3.12. Nalezněte všechna $m \in \mathbb{N}$ taková, že $\varphi(m) = 28$, respektive taková, že $\varphi(m) = 18$. (Výsledek: $\varphi(m) = 28$ pro $m \in \{29, 58\}$, $\varphi(m) = 18$ pro $m \in \{19, 27, 38, 54\}$.)

Kapitola 4

Kongruence, kvadratické zbytky, Legendreův symbol

4.1 Opakování z přednášky

Definice. Číslo a nazveme *kvadratickým zbytkem modulo* n, pokud kongruence

$$x^2 \equiv a \pmod{n}$$

má řešení.

Věta (27 z přednášky)**.** *Buď p liché prvočíslo a a číslo s ním nesoudělné. Pak kongruence $x^2 \equiv a \pmod{p}$ má řešení právě tehdy, když $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Definice. Pro prvočíslo p a číslo a definujeme *Legendreův symbol* předpisem

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ je kvadratický zbytek modulo } p, \\ -1 & a \text{ není kvadratický zbytek modulo } p, \\ 0 & a \text{ je soudělné s } p. \end{cases}$$

Čteme „a vzhledem k p“.

Jednoduchým důsledkem Věty je, že pro liché prvočíslo p a a s ním nesoudělné máme $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$. Nyní uvedeme další vlastnosti Legendreova symbolu.

i) Pokud $a \equiv b \pmod{p}$, pak $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

ii) $\left(\frac{a\,b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

iv) pro liché prvočíslo q platí $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$.

Pomocí těchto vlastností je možné Legendreův symbol dopočítat.

Zastavme se na chvíli u vlastnosti iii). U nich počítáme znaménko, jehož výpočet si můžeme zjednodušit. Vzpomeňme si na Příklad 1.1. Tam jsme dokázali, že pro libovolné n je zbytek n^2 po dělení osmi 0, 1, nebo 4. To jsme dokazovali tak, že jsme uvažovali n zbytkové třídy po dělení 4. Vzhledem k tomu, že p je liché prvočíslo, máme $p = 4k \pm 1$ pro nějaké $k \in \mathbb{N}$. Pak

$$p^2 - 1 = (4k \pm 1)^2 - 1 = 16k^2 \pm 8k + 1 - 1 = 8(2k^2 + k).$$

Tudíž $\frac{p^2-1}{8}$ bude tvaru $2k^2 \pm k$. Pak

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{2k^2 \pm k} = (-1)^{\pm k} = (-1)^k$$

a vidíme, že stačí najít k p nejbližší násobek 4 a podívat se na paritu podílu. Ten bude sudý, pouze pokud bude tento nejbližší násobek 4 dělitelný osmi, jinými slovy $p \pm 1 = 8l$, neboli $p \equiv \pm 1 \pmod 8$. Pokud bude podíl lichý, bude pak $p \pm 1 \equiv 4 \pmod 8$, neboli $p \equiv 3$ nebo $5 \pmod 8$. Tudíž máme pro p liché

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1 \text{ nebo } 7 \pmod 8, \\ -1 & p \equiv 3 \text{ nebo } 5 \pmod 8. \end{cases}$$

Podobně můžeme řešit i vlastnost iv). Zde bude exponent lichý pouze tehdy, pokud bude $\frac{p-1}{2}\frac{q-1}{2}$ liché, neboli pokud nebudou ani $p-1$ ani $q-1$ dělitelné 4, neboli pokud p i q budou kongruentní 3 modulo 4. Tedy můžeme napsat opět

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & p \equiv q \equiv 3 \pmod 4, \\ \left(\frac{p}{q}\right) & \text{jinak.} \end{cases}$$

4.2 Příklady řešené na cvičení

Příklad 4.1. Určete poslední cifru čísla $3^{7^{11^5}}$ a poslední dvě cifry čísla 13^{2024}.

Řešení. Hledáme vlastně (kladný) zbytek po dělení čísla $3^{7^{11^5}}$ desíti. Víme, že $3^2 = 9 \equiv -1 \pmod{10}$. Tudíž $3^4 \equiv 1 \pmod{10}$. Můžeme si napsat exponent $7^{11^5} = 4k + l$. Pak

$$3^{7^{11^5}} = 3^{4k+l} = (3^4)^k \cdot 3^l \equiv 1^k \cdot 3^l = 3^l \pmod{10}. \tag{4.1}$$

Musíme tedy určit l. Hledáme zbytek 7^{11^5} po dělení 4. Víme, že $7^2 = 49 \equiv 1 \pmod 4$. Napíšeme-li si exponent $11^5 = 2m + n$, uvidíme, že

$$7^{11^5} = 7^{2m+n} = (7^2)^m \cdot 7^n \equiv 1^m \cdot 7^n = 7^n \pmod 4. \tag{4.2}$$

Stačí tedy určit zbytek 11^5 po dělení 2. Ovšem 11 je liché číslo, 11^5 tedy také a $m = 1$. Pak, díky (4.2), máme

$$7^{11^5} \equiv 7^1 = 7 \equiv 3 \pmod 4,$$

tedy $l = 3$. Dosazením do (4.1) dostáváme

$$3^{7^{11^5}} \equiv 3^3 = 9 \cdot 3 \equiv -1 \cdot 3 = -3 \equiv 7 \pmod{10}$$

a poslední cifra čísla $3^{7^{11^5}}$ je 7.

Hledáme zbytek 13^{2024} po dělení 100. Víme, že $\varphi(100) = 40$, tedy $13^{40} \equiv 1 \pmod{100}$. Poté

$$13^{2024} = 13^{40 \cdot 50 + 24} = (13^{40})^{50} \cdot 13^{24} \equiv 13^{24} \pmod{100},$$

tedy stačí počítat mocniny 13 modulo 100. Máme

$$\begin{aligned} 13^2 &\equiv 69 && \pmod{100} \\ 13^4 \equiv 69^2 &\equiv 61 && \pmod{100} \\ 13^8 \equiv 61^2 &\equiv 21 && \pmod{100} \\ 16^{16} \equiv 21^2 &\equiv 41 && \pmod{100} \end{aligned}$$

a odtud $13^{24} = 13^{16} \cdot 13^8 \equiv 41 \cdot 21 \equiv 61 \pmod{100}$. Také bychom mohli zjistit, že $13^{20} = = 13^{16} \cdot 13^4 \equiv 41 \cdot 61 \equiv 1 \pmod{100}$, takže bychom viděli, že řád 13 modulo 100 je nejvýše 20 (ve skutečnosti je to 20, ověřte sami), takže pak bychom měli rovnou $13^{2024} = = 13^{101 \cdot 20 + 4} \equiv 13^4 \equiv 61 \pmod{100}$. Poslední dvě cifry čísla 13^{2024} jsou tedy 61.

Jiná, lepší, metoda je počítat zvlášť modulo 4 a modulo 25. Protože $13 \equiv 1 \pmod{4}$, máme rovnou, že $13^{2024} \equiv 1 \pmod{4}$. Jelikož $\varphi(25) = 5 \cdot 4 = 20$, máme $13^{20} \equiv 1 \pmod{25}$. (Odtud bychom viděli, že řád 13 modulo 100 je 20.) Pak $13^{2024} \equiv 13^4 \pmod{25}$, takže počítáme

$$\begin{aligned} 13^2 = 169 &\equiv -6 && \pmod{25}, \\ 13^4 \equiv (-6)^2 = 36 &\equiv 11 && \pmod{25}, \end{aligned}$$

tudíž 13^{2024} je kongruentní 1 modulo 4 a 11 modulo 25. Řešením soustavy lineárních kongruencí pak dostaneme, že $13^{2024} \equiv 61 \pmod{100}$. △

Příklad 4.2. Určete všechna $n \in \mathbb{N}$ taková, že

a) $5^{3n+4} \equiv 8 \pmod{13}$;

b) $5^{2^{3n+1}} \equiv -7 \pmod{22}$.

Řešení. Začneme a). Nejprve zjistíme řád 5 modulo 13. Víme, že $5^2 = 25 \equiv -1 \pmod{13}$, tedy $5^4 \equiv 1 \pmod{13}$ a řád 5 je 4. Tudíž si můžeme výraz upravit

$$5^{3n+4} \equiv 5^{3n} = (5^3)^n = (5^2 \cdot 5)^n \equiv (-1 \cdot 5)^n = (-5)^n \pmod{13}.$$

Následně zjistíme, že $-5 \equiv 8 \pmod{13}$, tudíž kongruence platí pro $n = 1$. Jelikož řád 5 modulo 13 je 4, budou se kongruence opakovat s periodou 4. Dostáváme tedy, že tak bude pro $n = 4k + 1$, neboli $n \equiv 1 \pmod{4}$.

Řešíme b). Upravujeme si výraz

$$5^{2^{3\,n+1}} = 5^{2\cdot 2^{3\,n}} = (5^2)^{2^{3\,n}} \equiv 3^{(2^3)^n} = 3^{8^n} \pmod{22}$$

neboť $25 \equiv 3 \pmod{22}$. Následně můžeme počítat rekurentně $3^{8^{n+1}} = \left(3^{8^n}\right)^8$ modulární mocniny. Pak

- $n = 1$:
$$3^8 = (3^4)^2 = 81^2 \equiv (-7)^2 = 49 \equiv 5 \pmod{22}$$
- $n = 2$:
$$3^{8^2} = 3^{8\cdot 8} = \left(3^8\right)^8 \equiv 5^8 = 25^4 \equiv 3^4 = 81 \equiv -7 \pmod{22}$$
(Zde vidíme, že pro $n = 2$ kongruence platí.)
- $n = 3$:
$$3^{8^3} = \left(3^{8^2}\right)^8 \equiv (-7)^8 = 7^8 = 49^4 \equiv 5^4 = 25^2 \equiv 3^2 = 9 \pmod{22}$$
- $n = 4$:
$$3^{8^4} = \left(3^{8^3}\right)^8 \equiv 9^8 = 3^{16} = \left(3^8\right)^2 \equiv 5^2 \equiv 3 \pmod{22}$$

takže pro $n \geq 5$ můžeme využít rekurentního vztahu, posloupnost bude periodická (jelikož $3^{8^5} = \left(3^{8^4}\right)^8 \equiv 3^8$ atd.). Celkem tedy máme

$$5^{2^{3\,n+1}} \equiv 3^{8^n} \equiv \begin{cases} 3 & n \equiv 0 \pmod 4 \\ 5 & n \equiv 1 \pmod 4 \\ -7 & n \equiv 2 \pmod 4 \\ 9 & n \equiv 3 \pmod 4 \end{cases} \pmod{22},$$

takže řešením jsou všechna n kongruentní 2 modulo 4. △

Příklad 4.3. Určete, zda je 7 kvadratickým zbytkem modulo 13.

Řešení. Jinými slovy řešíme, jestli má kongruence $x^2 \equiv 7 \pmod{13}$ řešení. Použijeme Větu 27 z přednášky. Kongruence má řešení právě tehdy, když $7^{\frac{13-1}{2}} \equiv 1 \pmod{13}$. Počítáme tedy 7^6 modulo 13. $7^2 = 49 \equiv -3 \pmod{13}$, takže

$$7^6 = \left(7^2\right)^3 \equiv (-3)^3 = -27 \equiv -1 \not\equiv 1 \pmod{13}$$

a 7 není kvadratickým zbytkem modulo 13. Skutečně, můžeme si do tabulky s využitím toho, že $x \equiv 13 - x \pmod{13}$, napsat do tabulky hodnoty druhých mocnin modulo 13

x	± 1	± 2	± 3	± 4	± 5	± 6
x^2 modulo 13	1	4	-4	3	-1	-3

odkud vidíme, že jedinými kvadratickými zbytky modulo 13 jsou ± 1, ± 3 a ± 4. △

Příklad 4.4. Řešte kongruenci $3\,x^2 + x - 5 \equiv 0 \pmod{13}$.

Řešení. Polynom $3\,x^2 + x - 5$ nemá v $\mathbb{Z}$ kořeny, dále postupujeme podobně jako bychom řešili kvadratickou rovnici v $\mathbb{C}$, totiž úpravou na čtverec, kde ovšem počítáme modulo 13, tedy místo dělení násobíme modulární inverzí.[1]

Nejprve si polynom vynásobíme modulární inverzí k 3. Jelikož $3{\cdot}4 = 12 \equiv -1 \pmod{13}$, máme

$$3\,x^2 + 4 - 5 \equiv x^2 - 4\,x + 20 \equiv x^2 - 4\,x + 7.$$

Nyní již přímo upravujeme na čtverec, protože 4 se dá vydělit dvěma. Neboť $(x-2)^2 = x^2 - 4\,x + 4$, $x^2 - 4\,x = (x-2)^2 - 4$, a tudíž je původní polynom kongruentní $(x-2)^2 + 3$, tedy původní kongruence je ekvivalentní kongruenci

$$(x-2)^2 \equiv -3 \pmod{13}.$$

Tato má řešení, neboť -3 je kvadratický zbytek modulo 13 (viz konec řešení Příkladu 4.3, odkud také vidíme, že $x - 2 \equiv \pm 6 \pmod{13}$), neboli $x \equiv 8$ nebo $9 \pmod{13}$. △

Příklad 4.5. Řešte kongruence $x^2 - 3\,x - 10 \equiv 0$ a $x^2 - 3\,x - 14 \equiv 0 \pmod{49}$.

Řešení. Nejprve řešíme kongruenci $x^2 - 3\,x - 10 \equiv 0 \pmod{49}$. V $\mathbb{Z}[x]$ máme rozklad $x^2 - 3\,x - 10 = (x+2)\,(x-5)$, tedy automaticky $x \equiv -2$ nebo $5 \pmod{49}$ je řešením kongruence. Zjistíme, zda existují i jiná řešení metodou úpravy na čtverec.[2]

Zjistíme modulární inverzi k 2. Máme $2 \cdot 25 = 50 \equiv 1 \pmod{49}$. Pak naše verze „$\frac{3}{2}$“ je $3 \cdot 25 = 75 \equiv 26 \pmod{49}$. Pak máme $2 \cdot 26 \equiv 3 \pmod{49}$, tedy můžeme doplnit na čtverec, pouze dopočítáme 26^2 modulo 49. Máme

$$26^2 = 2^2 \cdot 13^2 = (4 \cdot 13) \cdot 13 = 52 \cdot 13 \equiv 3 \cdot 13 = 39 \equiv -10 \pmod{49},$$

tedy

$$(x - 26)^2 \equiv x^2 - 3\,x - 10 \pmod{49}.$$

Vidíme, že 26 také řeší naši kongruenci. Máme tedy $x^2 - 3\,x - 10 \equiv 0$ pro $x \equiv -2$, 5 nebo $26 \pmod{49}$.[3]

Polynom $x^2 - 3\,x - 14$ nad $\mathbb{Z}$ nerozložíme (ověřte sami), ale můžeme si jej díky předchozímu vyjádřit jako

$$x^2 - 3\,x - 14 = x^2 - 3\,x - 10 - 4 \equiv (x - 26)^2 - 4 \pmod{49}$$

[1] Ve skutečnosti fakt, že 13 je prvočíslo, dává, že zbytkové třídy modulo 13 spolu se sčítáním a násobením tvoří těleso, takže polynomiální kongruence může mít nejvýše tolik řešení, kolik je stupeň polynomu.

[2] 49 není prvočíslo, tudíž zbytkové třídy modulo 49 netvoří těleso a může se stát, že polynomy mohou mít více „kořenů“ (tj. čísel, kde hodnota je dělitelná 49), než je stupeň polynomu. Kupříkladu kongruence $x^2 - 1 \equiv 0 \pmod{8}$ má čtyři kořeny, ± 1 a ± 3, i když je stupeň polynomu pouze 2.

[3] Zde si všimněte $26 \equiv -2 \equiv 5 \pmod{7}$. $49 = 7^2$ je mocnina prvočísla. Pokud bychom uvažovali projekci řešení úlohy modulo 7 (což je prvočíslo, takže máme maximálně dvě řešení), budou všechna kongruentní (modulo 7 bychom dostali polynom $(x+2)^2$). Podobně, u polynomu $x^2 - 1$ modulo 8 jsou všechna řešení kongruentní modulo 2.

kde na pravé straně máme rozdíl druhých mocnin, takže si jej můžeme napsat jako

$$(x-26)^2 - 2^2 = (x-26-2)\,(x-26+2) = (x-28)\,(x-24),$$

tudíž řešeními kongruence $x^2 - 3\,x - 14 \equiv 0$ jsou pouze $x \equiv 24$ nebo $28 \pmod{49}$. △

Příklad 4.6. Řešte kongruenci $x^2 \equiv 58 \pmod{163}$.

Řešení. Nejprve zjistíme, jestli je 58 kvadratickým zbytkem modulo 163 (sami ověřte, že je to prvočíslo). Využijeme k tomu Legendreův symbol. Máme rozklad $58 = 2 \cdot 29$ Počítáme

$$\left(\frac{58}{163}\right) = \left(\frac{2}{163}\right) \cdot \left(\frac{29}{163}\right)$$

díky vlastnosti ii),

$$= (-1)^{\frac{163^2-1}{8}} \cdot \left(\frac{163}{29}\right) \cdot (-1)^{\frac{163-1}{2}\,\frac{29-1}{2}}$$

díky vzorcům z vlastností iii) a iv), kde $(-1)^{\frac{163^2-1}{8}} = -1$, neboť $163 \equiv 3 \pmod 8$, a $(-1)^{\frac{163-1}{2}\,\frac{29-1}{2}} = 1$, jelikož $29 \equiv 1 \pmod 4$,

$$= -\left(\frac{18}{29}\right) = -\left(\frac{2}{29}\right) \cdot \left(\frac{3}{29}\right)^2 = -(-1)^{\frac{29^2-1}{8}} = 1$$

díky vlastnostem i) a ii, přičemž trojku máme ve druhé mocnině, takže druhá mocnina Legendreova symbolu bude jistě 1 ($(3, 29) = 1$), a pro dvojku použijeme stejný vzoreček a $(-1)^{\frac{29^2-1}{8}} = -1$, jelikož $29 \equiv 5 \pmod 8$. 58 tedy je kvadratický zbytek modulo 163 a můžeme přejít k řešení kongruence. Máme

$$58^{\frac{163-1}{2}} = 58^{81} \equiv \left(\frac{58}{163}\right) = 1 \pmod{163}$$

tedy si celou rovnici můžeme vynásobit jedničkou, zleva psanou jako 1 a zprava jako 58^{81}. Dostaneme

$$x^2 \equiv 58^{82} \pmod{163}$$

tedy odmocněním získáme $x \equiv \pm 58^{41} \pmod{163}$. Zbývá spočítat modulární mocniny 58. Máme

$$\begin{aligned} 58^2 &= 3\,364 \equiv 104 \equiv -59 && \pmod{163} \\ 58^3 &\equiv -59 \cdot 58 = -3\,422 \equiv 1 && \pmod{163} \end{aligned}$$

tudíž vidíme, že $58^{41} \equiv 58^2 \equiv -59$, tedy vidíme, že řešeními jsou $x \equiv 59$ nebo $104 \pmod{163}$. △

Příklad 4.7. Řešte kongruenci $x^2 \equiv 58 \pmod{157}$.

Řešení. Opět nejprve s pomocí Legendreova symbolu ověříme, že má kongruence řešení (sami ověřte, že je 157 prvočíslo). Máme

$$\left(\frac{58}{157}\right) = \left(\frac{2}{157}\right) \cdot \left(\frac{29}{157}\right) = (-1)^{\frac{157^2-1}{8}} \cdot \left(\frac{157}{29}\right) \cdot (-1)^{\frac{157-1}{2}\,\frac{29-1}{2}}$$

díky vlastnostem ii), iii) a iv), přičemž $(-1)^{\frac{157^2-1}{8}} = -1$, jelikož $157 \equiv 5 \pmod 8$, a $(-1)^{\frac{157-1}{2}\,\frac{29-1}{2}} = 1$, protože $29 \equiv 1 \pmod 4$,

$$= -\left(\frac{12}{29}\right) = -\left(\frac{3}{12}\right) \cdot \left(\frac{2}{29}\right)^2 = -\left(\frac{3}{29}\right) = -\left(\frac{29}{3}\right) \cdot (-1)^{\frac{29-1}{2}\,\frac{3-1}{2}}$$

díky vlastnostem i), ii) a iv), dále se 2 vyskytuje v druhé mocnině a $(-1)^{\frac{29-1}{2}\,\frac{3-1}{2}} = 1$, protože $29 \equiv 1 \pmod 4$,

$$= -\left(\frac{2}{3}\right) = 1$$

díky vlastnosti i) a tomu, že 2 není kvadratický zbytek modulo 3 (všechny druhé mocniny dávají zbytek 0 nebo 1). Kongruence tedy má řešení. Můžeme přistoupit k samotnému řešení. Již nemůžeme použít trik s násobením $58^{78} \equiv 1 \pmod{157}$, protože bychom na pravé straně dostali lichou mocninu. Odmocněním $58^{78} \equiv 1$ dostaneme $58^{39} \equiv \pm 1 \pmod{157}$, zbývá určit znaménko. (Pokud by to byla jednička, mohli bychom rovnici vynásobit 58^{39}, pokud -1, musíme vymyslet něco jiného.) Například modulárním umocňováním získáme

$$\begin{aligned} 58^1 &= 58 & 58^8 &\equiv 14 \\ 58^2 &\equiv 67 & 58^{16} &\equiv 39 \\ 58^4 &\equiv 93 & 58^{32} &\equiv 108 \end{aligned}$$

tedy $58^{39} = 58^{32+4+2+1} \equiv (108 \cdot 93) \cdot (67 \cdot 58) \equiv -4 \cdot 118 \equiv -1 \pmod{157}$. Dále víme, že 2 není kvadratický zbytek modulo 157 (spočítali jsme výše), tedy $2^{78} \equiv \left(\frac{2}{157}\right) = -1$, tím pádem $4^{39} = 2^{78} \equiv -1 \pmod{157}$. Pak $4^{39} \cdot 58^{39} \equiv (-1) \cdot (-1) = 1 \pmod{157}$. Vynásobíme-li si kongruenci $x^2 \equiv 58 \pmod{157}$ čtyřmi, ovšem psáno vlevo jako 4 a vpravo jako $4^{40} \cdot 58^{39}$, dostaneme

$$4\,x^2 \equiv 4^{40} \cdot 58^{40} \pmod{157}$$

odkud odmocněním získáme $2\,x \equiv \pm 2^{40} \cdot 58^{20}$. Vynásobením modulární inverzí k dvojce, tedy $\frac{158}{2} = 79$ dostaneme

$$x \equiv \pm (4 \cdot 58)^{20} \cdot 79 \pmod{157}.$$

Zbývá určit modulární třídu výrazu napravo. $4 \cdot 58 = 232 \equiv 75 \pmod{157}$, dále

$$\begin{aligned} 75^2 &\equiv -27 && \pmod{157} \\ 75^4 &\equiv (-27)^2 \equiv -56 && \pmod{157} \\ 75^8 &\equiv (-56)^2 \equiv -4 && \pmod{157} \\ 75^{16} &\equiv (-4)^2 = 16 && \pmod{157} \\ 75^{20} &= 75^{16} \cdot 75^4 \equiv -56 \cdot 16 \equiv 46 && \pmod{157} \end{aligned}$$

a vynásobením modulární inverzí ke dvojce, 79, dostaneme, že $(4 \cdot 58)^{20} \cdot 79 \equiv 23 \pmod{157}$. Tudíž máme řešení $x \equiv 23$ nebo $134 \pmod{157}$. △

4.3 Příklady k procvičení

Příklad 4.8. Určete poslední dvě cifry čísla $7^{11^{2023}}$. (Vyjde postupně $2023 \equiv 7 \pmod{16}$, $7^{2023} \equiv 7^7 \equiv 23 \pmod{40}$ a $11^{7^{2023}} \equiv 11^2 3 \equiv 31 \pmod{100}$.)

Příklad 4.9. Určete, pro která $n \in \mathbb{N}$ platí a) $5^{3^{n+1}} \equiv 3 \pmod{11}$; b) $4^{5^{6^{n+1}}} \equiv 10 \pmod{13}$. (Výsledek: a) řád 5 modulo 11 vyjde 5, řešením je pak $n \equiv 2 \pmod{5}$; b) řád 4 modulo 13 vyjde 6, řád 5 modulo 6 vyjde 2, řešením je pak libovolné n.)

Příklad 4.10. Řešte konruenci $4x^2 - 5x - 4 \equiv 0 \pmod{11}$. (Výsledek: $x \equiv 6$ nebo $-2 \pmod{11}$.)

Příklad 4.11. Řešte kongruenci $x^2 + 11x + 3 \equiv 0 \pmod{35}$. (Výsledek: $x \equiv 6$, 11, 13 nebo $18 \pmod{35}$.)

Příklad 4.12. Rozhodněte, zda je 58 kvadratický zbytek modulo 151. Vyřešte kongruenci $x^2 \equiv 58 \pmod{151}$. (Výsledek: $x \equiv \pm 80 \pmod{151}$.)

Kapitola 5

Jacobiho symbol, testování prvočíselnosti, šifrování

5.1 Opakování z přednášky

Definice. Buďte čísla n *liché* a a libovolné. Nechť dále $n = p_1 \cdot \cdots \cdot p_k$, kde p_i, $i = 1, \ldots, k$, jsou (ne nutně různá) prvočísla. Definujeme *Jacobiho symbol*, čteno „a vzhledem k n“, vztahem

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \cdot \cdots \cdot \left(\frac{a}{p_k}\right),$$

kde na pravé straně jsou Legendreovy symboly.

Jacobiho symbol má podobné vlastnosti jako Legendreův symbol, což zjednodušuje jeho výpočet. Uveďme je nyní.

i) Pokud $a \equiv b \pmod{n}$, pak $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

ii) $\left(\frac{a\,b}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$;

iii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;

iv) pro liché m platí $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}$.

Opět máme u vlastností iii) a iv) vzorečky

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & n \equiv 1 \text{ nebo } 7 \pmod 8, \\ -1 & n \equiv 3 \text{ nebo } 5 \pmod 8. \end{cases}$$

a

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & m \equiv n \equiv 3 \pmod 4, \\ \left(\frac{n}{m}\right) & \text{jinak.} \end{cases}$$

jelikož při důkazu jsme využívali jen to, že jsme počítali s lichými čísly a nikoli nutně s prvočísly. Jacobiho symbol nemá nutně stejný vztah ke kvadratickým zbytkům, respektive máme pouze jednostrannou implikaci, tj. je-li a kvadratický zbytek modulo n, pak $\left(\frac{a}{n}\right) = 1$, jelikož a musí být kvadratický zbytek modulo všechna prvočísla v rozkladu n. Druhá implikace však neplatí. Například 2 není kvadratickým zbytkem modulo $15 = 3 \cdot 5$, ale $\left(\frac{2}{15}\right) = 1$. To je dáno tím, že se jedná o součin dvou prvočísel, modulo ani jednoho z nichž 2 není kvadratickým zbytkem.

Máme různé testy pro testování prvočíslenosti.

Věta (Fermatův test prvočíselnosti)**.** *Je-li p prvočíslo a a s ním nesoudělné, pak*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Věta (Eulerův test prvočíselnosti)**.** *Je-li p prvočíslo a a s ním nesoudělné, pak*

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Věta (Eulerův-Jacobiho test prvočíselnosti)**.** *Je-li p prvočíslo a a s ním nesoudělné, pak*

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

Při asymetrickém šifrování potřebuje každý účastník *veřejný klíč* V, sloužící k šifrování, a *soukromý klíč* S, který slouží k dešifrování. Pro asymetrické šifrování máme k disposici různé algoritmy.

RSA Pro generování klíčů zvolí účastník dvě *velká* prvočísla p a q, spočítá $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$, dále zvolí e nesoudělné s $\varphi(n)$ a spočítá (například pomocí Eukleidova algoritmu) modulární inverzi d, tedy $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Veřejným klíčem je pak $V = (n, e)$, soukromým klíčem je $S = d$. Pří šifrování zprávy M spočítáme $C := V(M) \equiv M^e \pmod{n}$. Při dešifrování šifrované zprávy C pak účastník spočítá $M \equiv C^d \pmod{n}$.

protokol na výměnu klíčů DH Obě strany komunikace se dohodnou na prvočísle p a primitivním kořenu g modulo p pak každý z účastníků vybere a, respektive b, a pošle druhé straně g^a, resp. g^b modulo p. Společným klíčem pro komunikaci je pak $g^{a\,b} = (g^a)^b = (g^b)^a$, což mohou oba účastníci spočítat bez toho, aby jej mohl zjistit kdokoli jiný.

ElGamal Systém je odvozen z protokolu DH. Účastník zvolí prvočíslo p, primitivní kořen g modulo p, náhodné a a spočítá $h \equiv g^a \pmod{p}$. Veřejným klíčem pak je $V = (p, g, h)$ a soukromým klíčem je pak $S = a$. Při šifrování zprávy M zvolíme náhodné b a spočítáme $C_1 \equiv g^b \pmod{p}$ a $C_2 \equiv M \cdot h^b \pmod{p}$; následně pošleme $C = (C_1, C_2)$. Pro dešifrování pak účastník spočítá $M \equiv C_2 / C_1^a \pmod{p}$.

Rabinův kryptosystém Pro generování klíčů zvolí účastník dvě *podobně velká* prvočísla $p \equiv q \equiv 3 \pmod 4$ a spočítá $n = p \cdot q$. Veřejným klíčem je $V = n$, soukromým klíčem je $S = (p, q)$. Při šifrování zprávy M spočítáme $C \equiv M^2 \pmod n$. Pro dešifrování účastník spočítá (čtyři) modulární odmocniny z C (dvě modulo p, dvě modulo q, pak dopočítá) a následně zjistí, která byla původní zprávou (například dohodou na kódu).

5.2 Příklady řešené na cvičení

Příklad 5.1. Ukažte, že $p = 1\,105 = 5 \cdot 13 \cdot 17$ projde Fermatovým testem $a^{p-1} \equiv 1 \pmod p$ pro libovolné a nesoudělné s p.

Řešení. Nechť a je nesoudělné s 1 105 libovolné. Pak a je nesoudělné i s 5, 13 i 17, o nichž víme, že jsou to prvočísla. Z malé Fermatovy věty proto máme

$$\begin{aligned} a^4 &\equiv 1 \pmod 5 \\ a^{12} &\equiv 1 \pmod{13} \\ a^{16} &\equiv 1 \pmod{17} \end{aligned}$$

Jelikož $[4, 12, 16] = 48$, máme dále $a^{48} \equiv 1 \pmod 5$, $\pmod{13}$ i $\pmod{17}$. Pak tedy je $a^{48} \equiv 1 \pmod{1\,105}$. Jenže $1\,104 = 48 \cdot 23$, díky čemuž $a^{1\,104} \equiv 1 \pmod{1\,105}$. △

Příklad 5.2. Ukažte, že $p = 1\,105$ neprojde Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ pro vhodné a nesoudělné s p, například pro $a = 7$.

Řešení. Z příkladu 5.1 víme, že pro libovolné a nesoudělné s 1 105 je $a^{48} \equiv 1$. Protože

$$\frac{1\,105 - 1}{2} = 552 = 48 \cdot 11 + 24,$$

máme $a^{552} \equiv a^{24} \pmod{1\,105}$. Hledáme některé a takové, že $a^{24} \not\equiv \pm 1 \pmod{1\,105}$. Opět z příkladu 5.1 víme, že $a^{24} \equiv 1 \pmod 5$ i $\pmod{13}$, navíc také, že $a^{24} \equiv a^8 \pmod{17}$. Hledáme tedy takové a nesoudělné s 5 a 13, že $a^8 \equiv -1 \pmod{17}$. Pak totiž $x := a^{552}$ splňuje soustavu kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{13} \\ x &\equiv -1 \pmod{17} \end{aligned}$$

Sami ověřte, že jediným řešením je $x \equiv 781 \pmod{1\,105}$.

Vzhledem k tomu, že exponent 8 je sudý, víme, že kongruence budou platit pro $\pm a$. Modulo 17 tedy stačí zkoušet $a = 2$, 3, 4, 5, 6 a 7. Máme

$$2^8 = (2^4)^2 = 16^2 \equiv (-1)^2 = 1 \pmod{17},$$

$$
\begin{aligned}
3^8 &= (3^3)^2 \cdot 3^2 \equiv 10^2 \cdot 3^2 = 30^2 \equiv (-4)^2 = 16 \equiv -1 \pmod{17},\\
4^8 &= 2^{16} \equiv 1 \pmod{17},\\
5^8 &= (5^2)^4 = 25^4 \equiv 8^4 = 2^{12} \equiv 2^4 = 16 \equiv -1 \pmod{17},\\
6^8 &= 2^8 \cdot 3^8 \equiv 1 \cdot (-1) = -1 \pmod{17},\\
7^8 &= (7^2)^4 = 49^4 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}.
\end{aligned}
$$

Máme tedy na výběr $a \in \{\pm 3, \pm 5, \pm 6, \pm 7\}$. Celkem tedy lze říci, že pro každé a kongruentní ± 3, ± 5, ± 6 nebo ± 7 modulo 17 nesoudělné s 5 i s 13 platí, že $a^{552} \equiv 781 \not\equiv 1 \pmod{1\,105}$. Například tedy pro $a = 3$, 6 nebo 7 číslo 1 105 neprojde Eulerovým testem. △

Příklad 5.3. Ukažte, že $p = 341$ projde Eulerovým testem pro $a = 2$, ale nikoli Eulerovým-Jacobiho testem pro $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ pro $a = 2$.

Řešení. Počítejme mocniny 2 modulo 341. Nejmenší mocnina, která se zkrátí je $2^9 = 512 \equiv 171 \pmod{341}$, pak $2^{10} \equiv 171 \cdot 2 = 342 \equiv 1 \pmod{341}$. Vidíme tedy, že

$$2^{\frac{341-1}{2}} = 2^{170} = (2^{10})^{17} \equiv 1 \pmod{341}.$$

Spočítejme nyní Jacobiho symbol $\left(\frac{2}{341}\right)$. Podle vlastnosti iii) máme

$$\left(\frac{2}{341}\right) = (-1)^{\frac{341^2-1}{8}} = -1$$

jelikož $341 = 42 \cdot 8 + 5$. Vidíme tedy, že $2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$, tudíž 341 není prvočíslo. Skutečně máme rozklad $341 = 11 \cdot 31$, jedná se tedy o součin dvou prvočísel. To, že $\left(\frac{2}{341}\right) = -1$ pak znamená, že 2 je kvadratickým zbytkem modulo *právě jednoho* z prvočísel z rozkladu. Konkrétně $8^2 = 64 \equiv 2 \pmod{31}$. Navíc bychom z rozkladu mohli vidět, že $2^{10} \equiv 1 \pmod{11}$ a $2^{10} = 32^2 \equiv 1^2 = 1 \pmod{31}$, tedy i $2^{10} \equiv 1 \pmod{341}$. △

Příklad 5.4. Zpráva M byla zašifrována pomocí RSA s veřejným klíčem $(51, 13)$ (tj. $e = 13$, $n = 51$) do tvaru 7, 48, 11. Pokuste se šifru prolomit a najít M.

Řešení. Víme, že $n = 17 \cdot 3$. Pak $\varphi(n) = 2 \cdot 16 = 32$. Zjišťujeme tedy modulární inverzi k 13 modulo 32 pomocí hledání koeficientů Bézoutovy rovnosti.

$$\begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & 32 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 13 \\ -2 & 1 & 6 \end{pmatrix} \sim \begin{pmatrix} 5 & -2 & 1 \\ -32 & 13 & 0 \end{pmatrix}$$

a vidíme, že $d = 5$ Poté stačí dešifrovat

$$
\begin{aligned}
7^5 &= (7^2)^2 \cdot 7 \equiv (-2)^2 \cdot 7 = 4 \cdot 7 = 28 && \pmod{51}\\
48^5 &\equiv (-3)^5 = -3 \cdot 81 \equiv -3 \cdot 30 \equiv -90 \equiv 12 && \pmod{51}\\
11^5 &= 11^2 \cdot 11^3 = 121 \cdot 1\,331 \equiv 19 \cdot 5 = 95 \equiv 44 && \pmod{51}
\end{aligned}
$$

neboť $121 = 2 \cdot 51 + 19$ a $1331 = 26 \cdot 56 + 5$. Původní zpráva byla tedy 28, 12, 34. △

Příklad 5.5. Pomocí šifry RSA s veřejným klíčem $(551, 95)$, tj. $n = 551 = 19 \cdot 29$, $e = 95$, zašifrujte a poté dešifrujte zprávu $M = 25$.

Řešení. Zprávu $M = 25$ zašifrujeme tak, že počítáme

$$C \equiv M^{95} = 25^{95} = 25^{81+9+3+2}.$$

Máme $25^1 = 25$ a $25^2 = 625 \equiv 74 \pmod{551}$. Dále

$$\begin{aligned} 25^3 &\equiv 74 \cdot 25 = 1\,850 \equiv 197 && \pmod{551} \\ 25^9 &\equiv 197^3 = 7\,645\,373 \equiv 248 && \pmod{551} \\ 25^{27} &\equiv 248^3 = 15\,252\,992 \equiv 210 && \pmod{551} \\ 25^{81} &\equiv 210^3 = 9\,261\,000 \equiv 343 && \pmod{551} \end{aligned}$$

tedy

$$\begin{aligned} 25^{95} &\equiv 343 \cdot 248 \cdot 197 \cdot 74 = \\ &= 85\,064 \cdot 14\,578 \equiv 210 \cdot 252 = \\ &= 52\,920 \equiv 24 && \pmod{551} \end{aligned}$$

a vidíme, že $C \equiv 24 \pmod{551}$.

Pro dešifrování musíme zjistit soukromý klíč. Máme $\varphi(551) = 28 \cdot 18 = 504$, hledáme d – modulární inverzi k 95 modulo 504 – pomocí nalezení Bézoutových koeficientů.

$$\begin{pmatrix} 1 & 0 & 504 \\ 0 & 1 & 95 \end{pmatrix} \sim \begin{pmatrix} 1 & -5 & 29 \\ 0 & 1 & 95 \end{pmatrix} \sim \begin{pmatrix} 1 & -5 & 29 \\ -3 & 16 & 8 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 13 & -69 & -3 \\ -3 & 16 & 8 \end{pmatrix} \sim \begin{pmatrix} 13 & -69 & -3 \\ 23 & -122 & 2 \end{pmatrix} \sim \begin{pmatrix} -36 & 191 & 1 \\ -95 & 504 & 0 \end{pmatrix}$$

Vidíme, že $d = 191$. Při dešifrování počítáme $C^d = 24^{191}$ modulo 551. (Již víme, že to vyjde 25.) Protože $24^2 = 576 \equiv 25 \pmod{551}$, máme hned

$$M \equiv 24^{191} = 24^{2 \cdot 95 + 1} = (24^2)^{95} \cdot 24 \equiv 25^{95} \cdot 24 \equiv 24 \cdot 24 \equiv 25 \pmod{551}$$

a nemuseli jsme počítat vyšší mocniny. △

5.3 Příklady k procvičení

Příklad 5.6. Ukažte, že $p = 1\,729 = 7 \cdot 13 \cdot 19$ projde Fermatovým testem $a^{p-1} \equiv 1 \pmod{p}$ pro libovolné a nesoudělné s p. (Počítejte zvlášť modulo 7, 13, 19 a zjistíte, že řád každého takového čísla a je dělitelem $36 \mid 1\,728$.)

Dodatková úloha. Ukažte, že p projde i Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ pro libovolné a nesoudělné s p.

Příklad 5.7. Ukažte, že $p = 2\,821 = 7 \cdot 13 \cdot 31$ neprojde Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ pro vhodné a nesoudělné s p, například pro $a = 2$. (Výsledek $2^{1\,410} \equiv 1\,520 \pmod{2\,821}$.)

Příklad 5.8. Ukažte, že $p = 217$ projde Eulerovým testem pro $a = 5$, ale nikoliv Eulerovým-Jacobiho testem $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ pro $a = 5$. (Výsledek: levá strana 1, pravá strana -1.)

Příklad 5.9. Zpráva M byla zašifrována pomocí RSA s veřejným klíčem $(55, 23)$, tj. $n = 55$, $e = 23$, do tvaru 8, 9, 17. Pokuste se šifru prolomit a najít M. (Výsledek: dešifrovací exponent $d = 7$, dešifrované zprávy 2, 4, 8.)

Příklad 5.10. Pomocí RSA s veřejným klíčem $(323, 151)$, tj. $n = 323 = 17 \cdot 19$, $e = 151$, zašifrujte a poté dešifrujte zprávu $M = 21$. (Výsledek: dešifrovací exponent $d = 103$, zašifrovaná zpráva 166.)

Kapitola 6

Šifrování, diofantické rovnice

6.1 Opakování z přednášky

Při asymetrickém šifrování potřebuje každý účastník *veřejný klíč* V, sloužící k šifrování, a *soukromý klíč* S, který slouží k dešifrování. Pro asymetrické šifrování máme k disposici různé algoritmy.

RSA Pro generování klíčů zvolí účastník dvě *velká* prvočísla p a q, spočítá $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$, dále zvolí e nesoudělné s $\varphi(n)$ a spočítá (například pomocí Eukleidova algoritmu) modulární inverzi d, tedy $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Veřejným klíčem je pak $V = (n, e)$, soukromým klíčem je $S = d$. Pří šifrování zprávy M spočítáme $C := V(M) \equiv M^e \pmod{n}$. Při dešifrování šifrované zprávy C pak účastník spočítá $M \equiv C^d \pmod{n}$.

protokol na výměnu klíčů DH Obě strany komunikace se dohodnou na prvočísle p a primitivním kořenu g modulo p pak každý z účastníků vybere a, respektive b, a pošle druhé straně g^a, resp. g^b modulo p. Společným klíčem pro komunikaci je pak $g^{a\,b} = (g^a)^b = (g^b)^a$, což mohou oba účastníci spočítat bez toho, aby jej mohl zjistit kdokoli jiný.

ElGamal Systém je odvozen z protokolu DH. Účastník zvolí prvočíslo p, primitivní kořen g modulo p, náhodné a a spočítá $h \equiv g^a \pmod{p}$. Veřejným klíčem pak je $V = (p, g, h)$ a soukromým klíčem je pak $S = a$. Při šifrování zprávy M zvolíme náhodné b a spočítáme $C_1 \equiv g^b \pmod{p}$ a $C_2 \equiv M \cdot h^b \pmod{p}$; následně pošleme $C = (C_1, C_2)$. Pro dešifrování pak účastník spočítá $M \equiv C_2 / C_1^a \pmod{p}$.

Rabinův kryptosystém Pro generování klíčů zvolí účastník dvě *podobně velká* prvočísla $p \equiv q \equiv 3 \pmod{4}$ a spočítá $n = p \cdot q$. Veřejným klíčem je $V = n$, soukromým klíčem je $S = (p, q)$. Při šifrování zprávy M spočítáme $C \equiv M^2 \pmod{n}$. Pro dešifrování účastník spočítá (čtyři) modulární odmocniny z C (dvě modulo p, dvě modulo q, pak dopočítá) a následně zjistí, která byla původní zprávou (například dohodou na kódu).

6.2 Příklady řešení na cvičení

Příklad 6.1. Najděte primitivní kořen modulo 23 a demonstrujte DH protokol pro $a = 7$ a $b = 13$.

Řešení. Máme $\varphi(23) = 22 = 2 \cdot 11$. Zkoušíme různé mocniny čísel.

$$\begin{aligned}
2^2 &= 4 \\
2^{11} &= (2^5)^2 \cdot 2 \equiv 9^2 \cdot 2 = 9 \cdot 18 \equiv 9 \cdot -5 = -45 \equiv 1 \pmod{23} \\
3^2 &= 9 \\
3^{11} &= (3^3)^3 \cdot 9 \equiv 4^3 \cdot 9 = 2^5 \cdot 2 \cdot 9 \equiv 9^2 \cdot 2 \equiv 1 \pmod{23} \\
5^2 &= 25 \equiv 2 \pmod{23} \\
5^{11} &\equiv 25^5 \cdot 5 \equiv 2^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1 \pmod{23}
\end{aligned}$$

Tudíž 5 je primitivní kořen modulo 23. Jiné primitivní kořeny jsou ty mocniny 5, kde exponent je nesoudělný s 22. Artem si zvolil exponent $a = 7$. Pošle tedy Barboře

$$5^7 = (5^2)^3 \cdot 5 \equiv 2^3 \cdot 5 = 40 \equiv -6 \pmod{23}.$$

Barbora si zvolila číslo $b = 13$. Pošle Artemovi

$$5^{13} = 25^6 \cdot 5 \equiv 2^6 \cdot 5 \equiv 9 \cdot 10 = 90 \equiv -2 \pmod{23}.$$

Společným klíčem pro komunikaci bude $5^{7\cdot 13} = (5^{13})^7 \equiv (-2)^7 = -2^7 \equiv -9 \cdot 4 = -36 \equiv 10 \pmod{23}$. △

Příklad 6.2. Tomáš a Petr chtějí komunikovat šifrou ElGamal. Tomáš si zvolil prvočíslo $p = 31$, primitivní kořen $g = 12$ a číslo $x = 6$. Zveřejnil pak trijici $(31, 12, h)$, kde $h \equiv 12^6 \pmod{31}$. Petr mu poslal dvojici $(21, 27)$. Jakou zprávu poslal Petr Tomášovi?

Řešení. Nejprve spočítáme h. S využitím $2^5 \equiv 1$ a $3^3 \equiv -4 \pmod{31}$ máme

$$h \equiv 12^6 = 2^{12} \cdot 3^6 = 2^2 \cdot (-4)^2 = 2^6 \equiv 2 \pmod{31}.$$[1]

Musíme dešifrovat zprávu $(21, 27) \equiv (-10, -4) \pmod{31}$. Tomášův soukromý klíč je 6. Počítáme $(-10)^6 = 2^6 \cdot 5^6 \equiv 2 \cdot 1 = 2 \pmod{31}$. Inverze k 2 modulo 31 je 16 (ověřte sami), takže Petrova původní zpráva byla $-4 \cdot 16 = -64 \equiv -2 \equiv 29 \pmod{31}$. △

Příklad 6.3. V Rabinově kryptosystému zvolila Alice svůj soukromý klíč $p = 19$, $q = 23$, veřejným klíčem je pak $n = p \cdot q = 437$. Zašifrujte pro Alici zprávu $m \equiv 327 \pmod{437}$ a ukažte, jak bude Alice tuto zprávu dešifrovat.

[1] K dešifrování vlastně nepotřebujeme znát číslo h, nicméně je dobré procvičení si jej spočítat.

Řešení. Šifrou je $C \equiv M^2 \pmod{n}$, tedy v našem případě je

$$M^2 = 327^2 = 106\,929 \equiv 301 =: C \pmod{437}.$$

Pro dešifrování spočítáme odmocniny modulo p a modulo q. Hledáme r a s tak, že

$$r^2 \equiv 301 \pmod{19} \qquad\qquad s^2 \equiv 301 \pmod{23}.$$

Z řešení kvadratických kongruencí (viz příklady 4.6 a 4.7) máme

$$r \equiv \pm 301^{\frac{19+1}{4}} \pmod{19} \qquad\qquad s \equiv \pm 301^{\frac{23+1}{4}} \pmod{23}.$$

Zbývá tedy spočítat mocniny 301^5 modulo 19 a 301^6 modulo 23. Máme

$$301 \equiv -3 \pmod{19} \qquad\qquad 301 \equiv 2 \pmod{23},$$

tudíž díky $\pm$ u odmocnin vidíme, že

$$r \equiv \pm 3^5 = \pm 9 \cdot 27 \equiv \pm 9 \cdot 8 = \pm 72 \equiv \mp 4 \pmod{19}$$

a

$$s \equiv \pm 2^6 = 64 \equiv \mp 5 \pmod{23}.$$

Pak pro každou dvojici (ze čtyř) r a s hledáme M takové, že $M \equiv r \pmod{19}$ a $M \equiv s \pmod{23}$. Tedy řešíme čtyři soustavy kongruencí

$$\begin{aligned} M &\equiv \pm 4 \pmod{19}, \\ M &\equiv \pm 5 \pmod{23}. \end{aligned}$$

Například pro $r = 4$ a $s = 5$ máme z první kongruence $M = 19\,k + 4$, dosazením do druhé kongruence dostaneme

$$\begin{aligned} 19\,k + 4 &\equiv 5 \pmod{23} \\ 19\,k &\equiv 1 \pmod{23} \\ -4\,k &\equiv 1 \pmod{23} \\ 4\,k &\equiv -1 \pmod{23} \end{aligned}$$

odkud vynásobením 6 dostaneme

$$24\,k \equiv k \equiv -6 \pmod{23}$$

tedy $k = 23\,l - 6$ a $M = 437\,l - 110$, tedy $M \equiv -110 \equiv 327 \pmod{437}$. Je jasné, že pro dvojici $r = -4$ a $s = -5$ bychom dostali $M \equiv 110 \pmod{437}$. (Mohli jsme si z první kongruence vyjádřit $M = -19\,k - 4$, dosazením do druhé by se opět řešení jen vynásobilo

-1.) Pro dvojici $r = 4$, $s = -5$ bychom dostali z první kongruence opět $M = 19\,k + 4$, následně bychom řešili kongruenci

$$\begin{aligned} 19\,k + 4 &\equiv -5 \pmod{23} \\ 19\,k &\equiv -9 \pmod{23} \\ -4\,k &\equiv -9 \pmod{23} \\ 4\,k &\equiv 9 \pmod{23} \end{aligned}$$

a opět vynásobením 6 dostaneme

$$24\,k \equiv k \equiv 54 \equiv 8 \pmod{23}$$

tedy $k = 23\,\ell + 8$ a $M = 437\,\ell + 156$, tedy $M \equiv 156 \pmod{437}$. Opět volbou $r = -4$, $s = 5$ bychom jednoduše dostali $M \equiv -156 \equiv 281 \pmod{437}$. Tedy máme 4 kandidáty pro původní zprávu, $M \equiv 110$ nebo 156 nebo 281 nebo 327 $\pmod{437}$. Například domluvou (nebo kódem) bychom pak zjistili, že $M \equiv 327 \pmod{437}$. △

Příklad 6.4. Vyřešte diofantickou rovnici $21\,x + 34\,y = 1\,597$, prvně nad $\mathbb{Z}$, pak nad $\mathbb{N}_0$.

Řešení. Nejprve si vyjádříme x. Máme

$$21\,x = 1\,597 - 34\,y.$$

Vidíme, že rovnice má nad $\mathbb{Z}$ řešení, pokud bude pravá strana dělitelná 21, neboli platí-li kongruence $34\,y \equiv 1\,597 \pmod{21}$. Tuto si můžeme zjednodušit a dále řešit

$$13\,y \equiv 1 \pmod{21}$$

vynásobením 5 dostaneme

$$2\,y \equiv 5 \pmod{21}$$

neboť $65 \equiv 2 \pmod{21}$, z čehož následně vynásobením 11 máme

$$y \equiv 13 \pmod{21}$$

protože $22 \equiv 1$ a $55 \equiv 13 \pmod{21}$. Tedy $y = 21\,k + 13$. Dosazením do původní rovnice řešíme vzhledem k x.

$$\begin{aligned} 21\,x + 34\,(21\,k + 13) &= 1\,597 \\ 21\,(x + 34\,k) &= 1\,155 \\ x + 34\,k &= 55 \\ x &= 55 - 34\,k \end{aligned}$$

Vidíme tedy, že řešeními jsou všechny dvojice

$$(x, y) = (55 - 34\,k, 13 + 21\,k), \quad k \in \mathbb{Z}.$$

Chceme-li řešit rovnici nad $\mathbb{N}_0$, uvažujeme ještě omezující podmínky $x \geq 0$, $y \geq 0$. Podmínka pro x je tvaru

$$55 - 34\,k \geq 0,$$

neboli

$$k \leq \frac{55}{34} < \frac{68}{34} = 2.$$

Podmínka pro y dává

$$13 + 21\,k \geq 0,$$

neboli

$$k \geq -\frac{13}{21} > -\frac{21}{21} = -1.$$

Tedy k může být jedině 0 nebo 1. Dostáváme tedy jediná dvě řešení nad $\mathbb{N}_0$ (i nad $\mathbb{N}$), dvojice $(55, 13)$ nebo $(21, 34)$. △

Příklad 6.5. Vyřešte diofantickou rovnici $50\,x + 70\,y + 57\,z = 1\,234$, nejprve nad $\mathbb{Z}$, pak nad $\mathbb{N}_0$.

Řešení. Můžeme si rovnici psát jako

$$10\,(5\,x + 7\,y) = 1\,234 - 57\,z,$$

odkud vidíme, že pravá strana rovnice musí být dělitelná 10, neboli musí být $57\,z \equiv 1\,234 \pmod{10}$. Po zjednodušení řešíme kongruenci $7\,z \equiv 4 \pmod{10}$. Vynásobením 3 dostaneme $z \equiv 2 \pmod{10}$ ($3 \cdot 7 = 21 \equiv 1$ a $3 \cdot 4 = 12 \equiv 2 \pmod{10}$), neboli $z = 10\,k + 2$. Dosazením do původní rovnice dostaneme rovnici

$$\begin{aligned} 50\,x + 70\,y + 570\,k + 114 &= 1\,234 \\ 50\,x + 70\,y + 570\,k &= 1\,120 \end{aligned}$$

což můžeme vydělit 10

$$5\,x + 7\,y + 57\,k = 112 \tag{6.1}$$

přičemž nyní můžeme rovnou počítat modulo 5 (opět $112 - 57\,k - 7\,y$ musí být dělitelné 5). Dostaneme kongruenci

$$2\,y + 2\,k \equiv 2 \pmod{5}$$

kterou můžeme vydělit 2 (protože $(2, 5) = 1$) a získat vyjádření $y \equiv 1 - k \pmod{5}$, neboli $y = 1 - k + 5\,l$. Dosazením do (6.1) vyřešíme pro x.

$$5\,x + 7 - 7\,k + 35\,l + 57\,k = 112$$

$$5\,(x + 10\,k + 7\,l) = 105$$

což můžeme vydělit 5

$$\begin{aligned} x + 10\,k + 7\,l &= 21 \\ x &= 21 - 10\,k - 7\,l. \end{aligned}$$

Nad $\mathbb{Z}$ jsou tedy řešeními všechny trojice tvaru

$$(x, y, z) = (21 - 10\,k - 7\,l, 1 - k + 5\,l, 2 + 10\,k), \quad k,\, l \in \mathbb{Z}.$$

Nad $\mathbb{N}_0$ musíme opět važovat omezení $x \geq 0$, $y \geq 0$, $z \geq 0$. Vzhledem k tomu, že z je parametricky vyjádřeno jen pomocí k, máme ihned omezení $10\,k + 2 \geq 0$, neboli

$$k \geq -\frac{1}{5} > -1,$$

tedy $k \geq 0$. Poté z omezení pro y dostaneme

$$1 \geq k - 5\,l \geq,$$

neboli

$$l \geq \frac{k-1}{5} \geq -\frac{1}{5} > -1$$

kde poslední nerovnost platí, protože je $k \geq 0$. Vidíme, že musí být $l \geq 0$. Jedná se však o dolní odhad pro l, nicméně vždy musí být $l \geq \left\lceil \frac{k-1}{5} \right\rceil$. Musíme tedy kontrolovat, jestli je v daném řešení skutečně $y \geq 0$.

Omezení pro x je ekvivalentní nerovnosti $10\,k + 7\,l \leq 21$. Vidíme, že pro $k \geq 3$ nebo $l \geq 4$ jistě neplatí, jelikož k i l jsou nezáporná. Můžeme postupně procházet například všechny možnosti k a dívat se na omezení pro l.

- $k = 0$: Zde dostaneme $7\,l \leq 21$, neboli $l \leq 3$. Máme tak dvojice parametrů $(0, 0)$, $(0, 1)$, $(0, 2)$ nebo $(0, 3)$, odpovídající trojicím $(21, 1, 2)$, $(14, 6, 2)$, $(7, 11, 2)$, $(0, 16, 2)$, přičemž všechna tato řešení jsou nad $\mathbb{N}_0$.

- $k = 1$: Máme omezení $7\,l \leq 11 < 14$, neboli $l < 2$. Máme možné parametrické dvojice $(1, 0)$ a $(1, 1)$, které odpovídají trojicím řešení $(10, 0, 12)$ a $(4, 5, 12)$, obě nad $\mathbb{N}_0$.

- $k = 2$: Dostaneme omezení $7\,l \leq 1$, tedy může být jedině $l = 0$. Dosteneme trojici řešení $(1, -1, 22)$, přičemž toto řešení již není nad $\mathbb{N}_0$. To je proto, že není splněna podmínka pro y, jelikož zde $5\,l = 0$ a $k = 2$, tedy $y = 1 - 2 = -1 < 0$.

Nad $\mathbb{N}_0$ tedy máme jen 6 řešení, jsou to trojice (x, y, z) tvaru $(21, 1, 2)$, $(14, 6, 2)$, $(7, 11, 2)$, $(0, 16, 2)$, $(10, 0, 12)$ nebo $(4, 5, 12)$. (Nad $\mathbb{N}$ bychom dostali 4 řešení – $(21, 1, 2)$, $(14, 6, 2)$, $(7, 11, 2)$ a $(4, 5, 12)$.) $\triangle$

6.3 Příklady k procvičení

Příklad 6.6. Najděte primitivní kořen modulo 19 a demonstrujte DH protokol pro $a = 5$ a $b = 7$. (Vyjde hned $g = 2$, Alena pošle $2^5 \equiv 13$, Bohuslav pošle $2^7 \equiv 14$, společný soukromý klíč vyjde $2^{5\cdot 7} \equiv 10 \pmod{19}$.)

Příklad 6.7. Taras a Přemysl chtějí komunikovat šifrou ElGamal. Taras si zvolil prvočíslo $p = 29$, primitivní kořen $g = 10$ a číslo $x = 7$. Zveřejnil pak trojici $(29, 10, h)$, kde $h \equiv 10^7 \pmod{29}$. Přemysl mu poslal dvojici $(2, 27)$. Jakou zprávu poslal Přemysl Tarasovi? (Společný soukromý klíč je $2^7 \equiv 12$, dešifrovaná zpráva je $M \equiv 12^{-1} \cdot 27 \equiv 24 \pmod{29}$.)

Příklad 6.8. V Rabinově kryptosystému Adéla zvolila za svůj soukromý klíč $p = 11$ a $q = 19$, veřejným klíčem je pak $n = p \cdot q = 209$. Zašifrujte pro Adélu zprávu $M = 42 \pmod{209}$ a ukažte, jak bude Adéla tuto zprávu dešifrovat. (Zašifrování $C \equiv 92$, dešifrování $M \equiv \pm 42, \pm 52 \pmod{209}$.)

Příklad 6.9. Vyřešte diofantickou rovnici $23\,x + 41\,y = 1\,693$, prvně nad $\mathbb{Z}$, pak se pokuste odpovědět nad $\mathbb{N}_0$. (Vyjde $x = -41\,t + 54$, $y = 23\,t + 11$, $t \in \mathbb{Z}$; nezáporná x, y vyjdou pro $t = 0,\ 1$.)

Příklad 6.10. Vyřešte diofantickou rovnici $36\,x + 60\,y + 35\,z = 93$, prvně nad $\mathbb{Z}$, pak se pokuste odpovědět nad $\mathbb{N}_0$. (Například $x = -5\,s - 15\,t + 28$, $y = 3\,s + 2\,t$, $z = 12\,t - 1$ pro $s,\ t \in \mathbb{Z}$; nad $\mathbb{N}_0$ máme čtyři řešení: $(13, 2, 11)$, $(8, 5, 11)$, $(3, 8, 11)$ a $(3, 1, 23)$.)

Kapitola 7

Kódování

7.1 Opakování z přednášky

Pracujeme nad abecedou $\{0,1\}$. Při použití (n,k)-kódu přenášíme slova o k bitech, kde (na začátek) přidáváme $n-k$ kódových bitů abychom dostali kódová slova o n bitech. *Hammingovou vzdáleností* dvou slov (stejné délky) rozumíme počet bitů, ve kterých se liší.

Věta (28 z přednášky)**.** *Kód* odhaluje r *a méně chyb právě tehdy, když je minimální Hammingova vzdálenost kódových slov alespoň* $r+1$*. Kód* opravuje r *a méně chyb právě tehdy, když je Hammingova vzdálenost kódových slov alespoň* $2\,r+1$*.*

Lineárním (n,k)*-kódem* rozumíme injektivní lineární zobrazení $g\colon (\mathbb{Z}/2)^k \to (\mathbb{Z}/2)^n$. Ve standardních bázích je reprezentováno $n \times k$ maticí G, které říkáme *generující matice kódu* g. Pokud přidáváme kódové bity na začátek slova, bude mít matice blokový tvar

$$G = \begin{pmatrix} P \\ \mathrm{I}_k \end{pmatrix}. \tag{7.1}$$

Matice P je rozměrů $(n-k) \times k$. Lineární zobrazení $h\colon (\mathbb{Z}/2)^n \to (\mathbb{Z}/2)^{n-k}$, zadané ve standardních bázích maticí

$$H := \begin{pmatrix} \mathrm{I}_{n-k} & P \end{pmatrix} \tag{7.2}$$

o rozměrech $k \times n$, nazýváme *zobrazením kontroly parity* kódu zadaného zobrazením g, matici H pak *maticí kontroly parity* tohoto kódu.

Věta (29 z přednášky)**.** *Nechť lineární kód* g *s generující maticí* G *má zobrazení, respektive matici, kontroly parity* h*, resp.* H*. Potom kódová slova kódu* g *jsou právě* $\ker h$*, tedy slovo* $\mathbf{v}$ *je kódové právě tehdy, když* $h(\mathbf{v}) = 0$*.*

Pro dané slovo $\mathbf{v} \in (\mathbb{Z}/2)^n$ nazýváme $\mathbf{s} := h(\mathbf{v}) \in (\mathbb{Z}/2)^{n-k}$ *syndromem slova* $\mathbf{v}$, který používáme při dekódování.

Pro dekódování přijatého slova $\mathbf{v}$ si spočítáme jeho syndrom $\mathbf{s}$. Na konec přidáme nuly (počátek $(\mathbb{Z}/2)^k$), získáme slovo $\mathbf{s}|0\ldots0$, které můžeme považovat za bod $(\mathbb{Z}/2)^n$. Přičtením kódových slov získáme afinní podprostor $(\mathbb{Z}/2)^n$ všech chybových slov odpovídajících

syndromu $\mathbf{s}$. Pokud předpokládáme, že při přenosu došlo k nejmenšímu množství chyb, hledáme v tomto podprostoru slovo s nejmenším počtem jedniček, jedničky totiž znamenají odchylku od kódových slov. Hledaným kódovým slovem je pak slovo, z něhož vzniklo přičtením syndromu naše slovo s nejmenším počtem jedniček. Je-li takových slov více, znamená to, že danou chybu neumíme opravit a máme více možností pro kódové slovo a tím i pro původní zprávu.

Jiný způsob dekódování je zakódovat informační bity přijaté zprávy $\mathbf{z}$, čímž vznikne kódové slovo $\mathbf{u}$. Rozdílem $\mathbf{z}-\mathbf{u}$ získáme chybu $\mathbf{e}$. Následně minimalizujeme počet jedniček v $\mathbf{e}$ pomocí sloupců generující matice G. Oba postupy jsou ekvivalentní, jelikož sloupce matice G zadávají bázi $\operatorname{im} g$, tudíž se přičítáním těchto vektorů k bodu $\mathbf{e}$ pohybujeme uvnitř afinního podprostoru chybových slov prináležících syndromu $\mathbf{s}$.

Jedním ze způsobů, jak zadat lineární kód je pomocí polynomů. Polynomy zde zapisujeme seřazené od absolutního členu ke členu vedoucímu. Buď $p(x) = a_0 + a_1\,x + \cdots + {} + a_{n-k}\,x^{n-k}$ polynom stupně $n-k$ nad $\mathbb{Z}/2$. *Polynomiálním kódem* generovaným polynomem p je kód, pro nějž je zobrazením kontroly parity dělení polynomem p se zbytkem. Jedná se o lineární (n,k)-kód. Jeho vstupní slova jsou polynomy nad $\mathbb{Z}/2$ stupně menšího než k, zobrazením g je pak $f \mapsto p \cdot f$, kde f je daný vstupní polynom. Kódovými slovy jsou pak tedy polynomy stupně menšího než n dělitelné polynomem p.

Chceme najít generující matici a matici kontroly parity. Polynomy stupně menšího než $n-k$ lze chápat jako zbytky po dělení polynomem p, tudíž je na nich zobrazení h identita. Matice H je, zapisujeme-li polynomy jako n-tice koeficientů vzestupně vzhledem ke stupni, skutečně tvaru (7.2). Zbývá zjistit, jak vypadá matice P. Sloupce matice H jsou zbytky po dělení polynomů x^i polynomem p, totéž bude platit i pro sloupce matice P. První sloupec bude právě zbytek po dělení p polynomu x^{n-k}, je to tedy sloupec koeficientů členů nižších stupňů polynomu p psaný *zdola nahoru*. Další sloupce jsou zbytky po dělení p monomů vyššího stupně. Ty však dostaneme ze zbytku x^{n-k} vynásobením x, kde případně monom x^{n-k} nahradíme příslušným zbytkem. V praxi tedy posouváme předchozí sloupec *dolů*, na první místo přidáme nulu a při přetečení jedničky nahoře přičítáme *první* sloupec matice P. Je jasné, že pak generující matice bude tvaru (7.1).[1]

7.2 Příklady řešené na cvičení

Příklad 7.1. Množinu čtyř slov chceme přenášet binárním kódem

a) rozpoznávajícím jednoduché chyby;

b) opravujícím jednoduché chyby.

Jakou nejmenší délku slov (chceme pro všechna slova stejnou) můžeme mít? Dejte příklad takových čtyř slov.

[1] Mohli bychom psát matici P i *shora dolů*, ale pak bychom dostali jinou generující matici. Jednalo by se o náš polynomiální kód nikoli ve standardní bázi prostoru polynomů, ale v permutované bázi.

Řešení. Máme slova 00, 01, 10 a 11. Nejprve řešíme a). Potřebujeme, aby minimální Hammingova vzdálenost kódových slov byla 2. Vidíme, že stačí například kód zajišťující sudý počet jedniček. Na začátek přidáme 0 nebo 1 tak, aby byl počet jedniček ve slově vždy sudý. Kódová slova pak budou 000, 101, 110 a 011. Je zřejmé, že se budou lišit minimálně na třech pozicích. Tento kód bude generovaný maticí

$$G_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

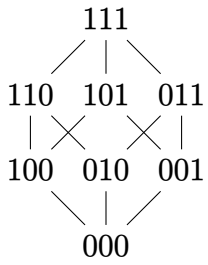
což je lineární $(3, 2)$-kód.

Pro b) potřebujeme, aby byla vzdálenost kódových slov minimálně 3. Jednou možností je opakovat každý bit třikrát. Dostali bychom $(6, 2)$ kód, nicméně přidáváme mnoho bitů. Zkusíme tedy najít nějaký kód, který přidává méně bitů. Můžeme vypozorovat, že vstupní slova mají mezi sebou minimální Hammingovu vzdálenost 1 a kódová slova kódu z a) mají minimální vzdálenost 2. Dáme-li je tedy za sebe kódové slovo z a a vstupní slovo, uvidíme, že se budou nová kódová slova lišite minimálně ve dvou bitech na prvních třech pozicích a v jednom bitu na posledních dvou pozicích, tedy celkem minimálně ve třech bitech. Máme tedy kódová slova 00000, 10101, 11010 a 01111. Jedná se o kódová slova lineárního $(5, 2)$-kódu daného maticí

$$G_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ověřme, že jsou pětibitová kódová slova skutečně minimální délky. Předpokládejme pro spor, že existuje kód s čtyřmístnými kódovými slovy. Bez újmy na obecnosti můžeme předpokládat, že tento kód přidává na bity na začátek kódových slov. Buď $ab00$ kódové slovo odpovídající 00. Pak, má-li se od něj kódové slovo odpovídající 01 lišit na třech pozicích, musí jím být $a'b'01$, kde $(\cdot)'$ značí opačný bit. Tutéž argumentaci lze použít i pro slovo 10, tudíž jsou od sebe kódová slova pro 01 a 10 vzdálena o 1.

Jinak lze řešit úlohu pomocí grafů. Na množinu všech slov délky n se můžeme dívat jako na graf, kde hrana spojuje každé dva vrcholy, které se od sebe liší jen v jednom bitu. Z každého vrcholu tak bude vycházet právě n hran. Graf bude mít tvar n-rozměrné krychle, nebo se na něj můžeme dívat jako na Hasseovský diagram podmnožin n-prvkové množiny (pak n-tice nul a jedniček odpovídají charakteristickým funkcím daných podmnožin). Například pro $n = 3$ budeme mít následující diagram.



Je vidět, že vrcholy 000, 100, 101 a 011 jsou od sebe odděleny vždy minimálně dvěma hranami. Odtud bychom mohli vyřešit a). Vidíme, že pro $n = 3$ máme v krychli dost vrcholů na to, abychom byli schopni najít čtveřici tak, že mezi každými dvěma vrcholy je minimální délka cesty alespoň 2.

Pokud chceme jednoduché chyby i opravovat, potřebujeme minimální délku cest mezi dvěma slovy alespoň 3. To si můžeme přeformulovat na tvrzení: „Pro žádné dva vrcholy v naší čtveřici neexistují jim incidentní hrany se společným druhým vrcholem.“ Pokud $n = 4$, máme celkem 16 vrcholů, 4 z nich jsou naše slova, takže zbývá 12 vrcholů. Jenže z každého z našich vrcholů vedou čtyři hrany do celkem 16 vrcholů, tudíž musí druhé vrcholy některých z nich být společné. Pro $n = 5$ máme celkem 32 vrcholů, 4 kódové, z každého z nich vede 5 hran do celkem 20 vrcholů. Zbývá 28 vrcholů, tedy je jich dost na to, abychom byli schopni najít čtveřici s požadovanou vlastností.

Tento grafový přístup nám umožňuje úlohu zobecnit. Pro dané 2^k hledáme minimální 2^n tak,[2] aby kódová slova délky n odhalovala / opravovala jednoduché chyby. Hledáme minimální n takové, že v n-rozměrné krychli lze najít 2^k vrcholů tak, aby minimální počet hran mezi nimi byl 2, resp. 3.

Má-li být minimální vzdálenost vrcholů 2, stačí vzít $n = k + 1$. To je proto, že $(k+1)$--rozměrná krychle je vlastně dvojice k-rozměrných krychlí, kde „odpovídající si“ vrcholy jsou spojeny hranou. Vezmeme pak z první krychle polovinu vrcholů (od sebe oddělených minimálně 2 hranami), z druhé krychle pak druhou polovinu.

Pro opravování chyb hledáme podobně minimální n tak, abychom v n-rozměrné krychli byli schopni najít 2^k vrcholů tak, že nemají společné žádně druhé vrcholy hran z nich vycházející. Máme celkem 2^n vrcholů, kódových vrcholů je 2^k, z každého z nich vychází n hran. Zbylých vrcholů je $2^n - 2^k$. Potřebujeme, aby mezi nimi bylo alespoň $2^k \cdot n$ vrcholů, neboli

$$2^k \cdot n \leq 2^n - 2^k$$

což odpovídá

$$n - \log_2(n+1) \geq k.$$

Protože je $\mathbb{N}$ dobře uspořádaná množina, má nerovnice pro dané k jediné řešení.[3] △

[2] Vstupní slova musí být nějaké délky, řekněme k, stačí tady úlohu uvažovat v závislosti na délce vstupních a kódových slov.

[3] Alternativně bychom se na nerovnici mohli dívat z druhé strany. Ze slov délky n lze vytvořit kód opravující jednoduché chyby ve slovech maximálně délky $n - \log_2(n+1)$.

Příklad 7.2. Pomocí lineárního kódu daného maticí

$$\left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

zakódujte zprávu 101.

Řešení. Zpráva 101 je sloupcovým vektorem $\mathbf{z} = (1, 0, 1)^{\mathrm{T}}$. Kódování probíhá tak, že daný vektor $\mathbf{z}$ vynásobíme zleva generující maticí G, kde dostaneme vektor

$$\mathbf{k} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

a hledané kódové slovo je 10101. △

Poznámka. Místo násobení sloupcových vektorů zleva jsme mohli také násobit řádkové vektory zprava transponovanou maticí.

Příklad 7.3. Určete všechna kódová slovy $(3, 2)$-kódu generovaného polynomem $x + 1$. Určete generující matici tohoto polynomiálního kódu.

Řešení. Máme polynom $p(x) = 1 + x$. Kód g je dán násobením polynomem p. Vstupní slova budou polynomy $f(x) = a_0 + a_1\, x$, kde a_i, $i \in \{0, 1\}$. Pak

$$g(f)(x) = (p \cdot f)(x) = a_0 + (a_0 + a_1)\, x + a_1\, x^2.$$

Máme čtyři možnosti pro polynom f:

1. $f(x) = 0$: $(p \cdot f)(x) = 0$,
2. $f(x) = 1$: $(p \cdot f)(x) = 1 + x$,
3. $f(x) = x$: $(p \cdot f)(x) = x + x^2$,
4. $f(x) = 1 + x$: $(p \cdot f)(x) = 1 + x + x + x^2 = 1 + x^2$.

Polynom f reprezentuje slovo $a_0 a_1$, podobně pro kódový polynom. Vstupní i kódová slova si můžeme zapsat do následující tabulky

vstupní slovo	00	01	10	11
kódové slovo	000	011	110	101

Vidíme, že všechna kódová slova obsahují sudý počet jedniček. Kód g je skutečně kódem zajišťujícím sudý počet jedniček. Nám zvyklé vyjádření, kde kódový bit přidáváme na začátek slova má pak tento kód například v bázi $(x, 1, x^2)$.

Zobrazení h přiřazuje polynomu stupně 2 zbytek po dělení $p(x) = 1 + x$. Hledáme zbytek po dělení p polynomu $x^{3-2} = x$. Platí

$$x = (1 + x) \cdot 1 + 1$$

tedy zbytek je 1. Zbytek polynomu x^2 je pak x, které si nahradíme 1. Máme tedy matici

$$P = \begin{pmatrix} 1 & 1 \end{pmatrix},$$

matici kontroly parity

$$H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

a generující matici

$$G = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}. \qquad \triangle$$

Příklad 7.4. Určete generující matici a matici kontroly parity $(7, 2)$-kódu generovaného polynomem $p(x) = x^5 + x^4 + x^2 + 1$. Dekódujte přijaté slovo 00101|11 za předpokladu, že při přenosu došlo k nejmenšímu možnému množství chyb.

Řešení. Nejprve si zjistíme matici P. Jejím prvním sloupcem bude (vzestupně seřazený) zbytek po dělení x^5 polynomem p. Je vidět, že to bude $x^4 + x^2 + 1$, neboli $(1\,0\,1\,0\,1)^{\mathrm{T}}$. Druhým sloupcem pak bude $(x^4 + x^2 + 1) \cdot x = x^5 + x^3 + x$, kde si x^5 nahradíme zbytkem, tedy vyjde $x^4 + x^3 + x^2 + x + 1$. Pak vyjde matice

$$P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix},$$

z čehož získáme matici H přidáním I_5 blokově na první sloupec, tedy

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

a matici G přidáním I_2 blokově na druhý řádek, tedy

$$G = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dekódujme zprávu 00101|11, která odpovídá vektoru $\mathbf{v} = (0\,0\,1\,0\,1\,1\,1)^{\mathrm{T}}$. Máme dvě možnosti, jak úlohu řešit. Informační bity přijaté zprávy jsou 11. Zakódujeme si zprávu $(1\,1)^{\mathrm{T}}$. Dostaneme kódové slovo $\mathbf{u} = (0\,1\,0\,1\,0\,1\,1)^{\mathrm{T}}$, následně si spočítáme chybu přenosu $\mathbf{e} = \mathbf{v} - \mathbf{u} = (0\,1\,1\,1\,1\,0\,0)^{\mathrm{T}}$. Prvních 5 bitů chybového vektoru je totožných se syndromem zprávy $\mathbf{v}$:

$$\mathbf{s} = H \cdot \mathbf{v} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Nyní se snažíme minimalizovat počet jedniček chyby $\mathbf{e}$ pomocí sloupců generující matice G. Přičtením druhého sloupce G získáme nový chybový vektor $\mathbf{e}' = (1000001)^{\mathrm{T}}$. Je vidět, že přičtením prvního nebo druhého sloupce matice G k $\mathbf{e}'$ by se počet jedniček zvýšil. Původní zprávu získáme přičtením minimální chyby $\mathbf{e}'$ k přijaté zprávě $\mathbf{v}$, dostaneme zprávu $(1\,0\,1\,0\,1\,1\,0)^{\mathrm{T}}$, tedy původní odeslaná informace byla 10.

Jinou možností je použít metody lineární geometrie. Již jsme si spočítali syndrom $\mathbf{s}$ zprávy $\mathbf{v}$. V $(\mathbb{Z}/2)^7$ si spočítáme obraz kódu g (sestávající z kódových slov). Píšeme-li vstupní slova jako sloupce matice, bude její násobek zleva G odpovídat matici kódových slov. Složenými závorkami značíme, že sloupce matice jsou právě vstupní / kódová slova, jedná se tedy spíše o množinu / prostor sloupcových vektorů, než o matici.

$$G \cdot \left\{ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \left\{ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\},$$

Obraz kódu g tvoří vektorový podprostor v $(\mathbb{Z}/2)^7$. Afinní podprostor chybových slov se syndromem $\mathbf{s}$ dostaneme přičtením vektoru $(\mathbf{s}\,0\,0)^{\mathrm{T}}$, což dává (s přihlédnutím k notaci se

složenými závorkami jako výše)

$$\begin{pmatrix}0\\1\\1\\1\\1\\0\\0\end{pmatrix} + \left\{\begin{pmatrix}0&1&1&0\\0&1&0&1\\0&1&1&0\\0&1&0&1\\0&1&1&0\\0&0&1&1\\0&1&0&1\end{pmatrix}\right\} = \left\{\begin{pmatrix}0&1&1&0\\1&0&1&0\\1&0&0&1\\1&0&1&0\\1&0&0&1\\0&0&1&1\\0&1&0&1\end{pmatrix}\right\}.$$

Nyní v množině chybových slov hledáme to s nejmenší chybou, tedy sloupec s nejmenším počtem jedniček. V prvním sloupci máme 4 jedničky, ve druhém 2, ve třetím 3 a ve čtvrtém opět 4. Vidíme, že musíme vzít druhý slupec. Poslaná zpráva odpovídala součtu druhého sloupce s obdrženou zprávou, tedy

$$(1\,0\,0\,0\,0\,0\,1)^{\mathrm{T}} + (0\,0\,1\,0\,1\,1\,1)^{\mathrm{T}} = (1\,0\,1\,0\,1\,1\,0)^{\mathrm{T}}$$

což odpovídá zprávě 10101|10 a původní slovo bylo 10. △

Příklad 7.5. Určete generující matici a matici kontroly parity $(7,4)$-kódu generovaného polynomem x^3+x+1. Dekódujte přijatá slova 100|1001 a 101|0110 za předpokladu, že při přenosu došlo k nejmenšímu možnému množství chyb.

Řešení. Zjistíme si matici P. Zbytek po dělení x^3 polynomem x^3+x+1 je $x+1$. Zbytek x^4 je x^2+x, zbytek x^5 je x^3+x^2, který si převedeme na x^2+x+1, a nakonec zbytek x^6 je x^4+x^3, který ji převedeme na $x^2+x+x+1=x^2+1$. Psaním koeficientů zbytků zdola nahoru do sloupců (tedy koeficient u x^2 na poslední řádek, u x na prostřední a u 1 na horní) získáme matici

$$P = \begin{pmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix},$$

z ní matici kontroly parity

$$H = \begin{pmatrix}1&0&0&0&1&1&1\\0&1&0&1&1&1&0\\0&0&1&1&0&1&1\end{pmatrix}$$

a generující matici

$$G = \begin{pmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

Obdrželi jsme zprávu 100|1001. Informační bity jsou 1001, zakódujeme si tedy vektor $(1\,0\,0\,1)^{\mathrm{T}}$ maticí G.

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Chybu přenosu obdržíme odečtením výsledku od obdržené zprávy.

$$\mathbf{e} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Přičtením třetího sloupce matice G snížíme počet jedniček a dostaneme novou chybu

$$\mathbf{e}' = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Vidíme, že přičtením libovolného sloupce matice G by se počet jedniček zvýšil. Chyba $\mathbf{e}'$ je tedy minimální, původní zprávu dostaneme přičtením této minimální chyby k přijaté zprávě:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

a odeslaná zpráva byla 100|1011, tedy původní slovo bylo 1011.

Obdrželi jsme druhou zprávu 101|0110. Zakódujeme si slovo 0110 kódem g.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Chybu získáme odečtením od kódového slova od přijaté zprávy.

$$\mathbf{e} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Vidíme, že přičtením libovolného sloupce matice G k chybě $\mathbf{e}$ by se počet jedniček zvýšil. Můžeme proto rovnou říci, že je chyba minimální a původní zpráva byla

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

a poslané slovo bylo 0110. To je dáno tím, že dojde-li k (jednoduché) chybě na kódových bitech, je výsledná chyba již minimální.

Chceme-li řešit úlohu pomocí lineární algebry, spočítáme si nejprve množinu kódových slov, kde konvence se závorkami je stejná, jako v příkladu 7.4.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \left\{ \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix} \right\} =$$

$$= \left\{ \begin{pmatrix} 0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1 \\ 0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1 \\ 0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix} \right\} \quad (7.3)$$

Spočítáme si syndrom první přijaté zprávy 100|1001.

$$\mathbf{s}_1 = \begin{pmatrix} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Ten si doplníme nulami na konci a zjistíme afinní podprostor chybových slov syndromu $\mathbf{s}_1$ přičtením k lineárnímu podprostoru kódových slov.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \left\{ \begin{pmatrix} 0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1 \\ 0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1 \\ 0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix} \right\} =$$

$$= \left\{ \begin{pmatrix} 1&0&0&1&1&0&0&1&0&1&1&0&0&1&1&0 \\ 1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0 \\ 1&0&0&1&0&1&1&0&1&0&0&1&0&1&1&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix} \right\}$$

Mezi danými chybovými slovy si najdeme to s nejmenším počtem jedniček, což je v našem případě třetí sloupec, tedy minimální chyba je $(0\,0\,0\,0\,0\,1\,0)^{\mathrm{T}}$ a původní zprávu 100|1011 jsme získali přičtením minimální chyby ke zprávě přijaté.

Nyní si spočítáme syndrom druhé přijaté zprávy 101|0110.

$$\mathbf{s}_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Doplníme jej nulami a přičteme k němu lineární podprostor kódových slov z (7.3), abychom získali afinní podprostor chybových slov daného syndromu.

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \left\{ \begin{matrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix} \right\} =$$

$$= \left\{ \begin{matrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix} \right\}$$

Vidíme, že nejmenší počet jedniček má první chybové slovo, takže odečtením tohoto chybového slova od obdržené zprávy dostaneme

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

a poslaná zpráva byla 001|0110, původní informace 0110. △

7.3 Příklady k procvičení

Příklad 7.6. Určete generující matici a matici kontroly parity $(7, 4)$-kódu generovaného polynomem $x^3 + x^2 + 1$. Dekódujte přijatá slova 110|1100 a 101|0111 za předpokladu, že při přenosu došlo k nejmenšímu množství chyb. (Výsledky: 010|1100 a 101|0011.)

Kapitola 8

Kombinatorika

8.1 Opakování z přednášky

kombinatorické pravidlo součtu počty vzájemně vylučujících se možností se sčítají

kombinatorické pravidlo součinu počty nezávislých a současně se vyskytujících možností se mezi sebou násobí

permutace počet bijekcí n-prvkové množiny do sebe je $n!$

kombinace počet výběrů k prvků z n prvků (k-prvkových podmnožin n-prvkové množiny) je

$$\binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k!}$$

variace počet pořadí k prvků z n prvků (uspořádaných k-tic z n-prvkové množiny) můžeme získat jako počet výběrů k prvků z n prvků krát počet (dobrých) uspořádání k prvků, tedy jako

$$\binom{n}{k} \cdot k! = n \cdot (n-1) \cdot \dots \cdot (n-k+1)$$

permutace s opakováním prvků různých druhů máme-li p_1 prvků prvního druhu, p_2 prvků druhého druhu, $\dots$, p_k prvků k-tého druhu, pak počet permutací $p_1 + p_2 + \\ + \dots + p_k$ prvků s opakováním prvků daných druhů je

$$\frac{(p_1 + p_2 + \dots + p_k)!}{p_1! \cdot p_2! \cdot \dots \cdot p_k!}$$

variace s opakováním počet pořadí k prvků z n prvků s opakováním je n^k

kombinace s opakováním počet kombinací k prvků z n prvků s opakováním odpovídá ekvivalentně

- počtu rozdělení k stejných prvků do n krabiček,
- počtu rozmístění $n-1$ oddělovačů mezi lineárně seřazených k stejných prvků
- počtu permutací $k+n-1$ prvků a oddělovačů s opakováním k prvků a $n-1$ oddělovačů

přičemž počet posledních je

$$\frac{(k+n-1)!}{k!(n-1)!} = \binom{k+n-1}{k} = \binom{k+n-1}{n-1}$$

Připomeneme si *princip inkluze a exkluze*. Označme $\#A$ počet prvků konečné množiny A. Mějme systém konečných množin $\{A_i\}_{i=1}^n$. Pak platí

$$\#\bigcup_i A_i = \sum_i \#A_i - \sum_{i\neq j} \#(A_i \cap A_j) + \sum_{i\neq j\neq k} \#(A_i \cap A_j \cap A_k) - \cdots + \\ + (-1)^{n-2} \sum_i \#\bigcap_{j\neq i} A_j + (-1)^{n-1} \#\bigcap_i A_i.$$

8.2 Příklady řešené na cvičení

Příklad 8.1. Určete počet řešení rovnice

$$x + y + z = 2\,024$$

v $\mathbb{N}_0$, respektive v $\mathbb{N}$.

Řešení. Nejprve úlohu řešíme nad $\mathbb{N}_0$. Máme $2\,025$ možností pro x ($x = 0, 1, \ldots, 2\,024$). Pro každou z těchto možností máme $2024 - x + 1$ možností pro y ($y = 0, 1, \ldots, 2024 - x$). Každá z těchto dvojic x a y jednoznačně určuje $z = 2024 - x - y$. Stačí tedy sečíst přes všechny možnosti pro x možnosti pro y v závislosti na x.

$$\sum_{x=0}^{2\,024} (2\,025 - x) = 2\,025 \cdot 2\,025 - \sum_{x=0}^{2\,024} x = 2\,025 \cdot 2\,025 - \frac{2\,025 \cdot 2\,024}{2} = \\ = 2\,025 \cdot (2\,025 - 1\,012) = 2\,025 \cdot 1\,013 = 2\,051\,325.$$

Můžeme si rovněž zapsat číslo $2\,024$ jako součet dvou tisíc dvaceti čtyř jedniček.

$$2\,024 = \underbrace{1 + 1 + \cdots + 1}_{2\,024}$$

Následně se ptáme, kolik z nich přináleží x, kolik y a kolik z. Hledáme tedy, kolika způsoby je možné rozdělit $2\,024$ stejných prvků na tři hromádky. Jedná se tedy o kombinace s opakováním, počet možností je tedy

$$\binom{2\,024 + 2}{2} = \binom{2\,026}{2} = \frac{2\,026 \cdot 2\,025}{2} = 2\,051\,325.$$

Řešíme-li rovnici v $\mathbb{N}$, musí být x, y i z minimálně 1. Můžeme si tedy zavést nové proměnné $x_0 := x - 1$, $y_0 := y - 1$ a $z_0 := z - 1$, které již budou z $\mathbb{N}_0$. Po vyjádření si proměnné x_0, y_0 a z_0 dosadíme do původní rovnice a dostaneme

$$x_0 + 1 + y_0 + 1 + z_0 + 1 = 2\,024$$

neboli

$$x_0 + y_0 + z_0 = 2\,021,$$

přičemž počet řešení nové rovnice je stejný jako počet řešení původní rovnice – ke každé proměnné bychom přičetli 1. Například druhým způsobem řešení pak dospějeme k počtu řešení $\binom{2\,021+2}{2} = \binom{2\,023}{2} = 2\,045\,253$. △

Příklad 8.2. Kolika způsoby můžeme zapsat číslo 22 500 000 jako

a) součin dvou přirozených čísel;

b) součin tří přirozených čísel?

Řešení. Hledáme vlastně počet řešení rovnice $x \cdot y = 22\,500\,000$, resp. $x \cdot y \cdot z = 22\,500\,000$ v $\mathbb{N}$. Nejprve si určíme prvočíselný rozklad 22 500 000. Celkem snadno máme

$$22\,500\,000 = 225 \cdot 100\,000 = 15^2 \cdot 10^5 = 3^2 \cdot 5^2 \cdot 2^5 \cdot 5^5 = 2^5 \cdot 3^2 \cdot 5^7.$$

Řešíme nejprve a). Vzhledem k tomu, že $y = \frac{22\,500\,000}{x}$ je jednoznačně určené x, zajímá nás počet x takových, že x dělí 22 500 000, tedy počet dělitelů tohoto čísla. Napíšeme si $x = 2^a \cdot 3^b \cdot 5^c$. Pak mohou být $a \in \{0, 1, \ldots, 5\}$, $b \in \{0, 1, 2\}$ a $c \in \{0, 1, \ldots, 7\}$. Máme tedy 6 možností pro a, 3 možnosti pro b a 8 možností pro c. Volby jsou na sobě nezávislé, celkem máme tedy $6 \cdot 3 \cdot 8 = 144$ možností pro x a celkem 48 řešení.

Jinak se na úlohu můžeme dívat tak, že zvlášť dělíme 5 dvojek, 2 trojky a 7 pětek na dvě hromádky (jedna pro x a jedna pro y). Rozdělení dvojek, trojek a pětek jsou na sobě nezávislá. Máme tedy tři nezávislé kombinace s opakováním, tedy počet řešení je

$$\binom{5+1}{1} \cdot \binom{2+1}{1} \cdot \binom{7+1}{1} = 6 \cdot 3 \cdot 8 = 144.$$

Nyní řešíme b), již pouze druhou možností (je jednodušší). Dělíme 5 dvojek, 2 trojky a 7 pětek zvlášť na tři hromádky (pro x, y a z), jedná se tedy opět o tři nezávislé kombinace s opakováním, počet řešení b) je

$$\binom{5+2}{2} \cdot \binom{2+2}{2} \cdot \binom{7+2}{2} = \binom{7}{2} \cdot \binom{4}{2} \cdot \binom{9}{2} = 21 \cdot 6 \cdot 36 = 4\,536.$$ △

Poznámka. Pokud bychom řešili úlohu *až na pořadí činitelů*, zkomplikovala by se. V a) by stačilo vydělit počet řešení dvěma (počet permutací dvouprvkové množiny). 22 500 000 není druhá mocnina, takže počet dělitelů je sudý, a dělitele jde spárovat tak, že součin dá vždy kýžené číslo. Až na pořadí tedy lze číslo 22 500 000 zapsat jako součin dvou 72 různými způsoby. Pro druhou mocninu by byl počet dělitelů lichý – pak bychom odečetli 1 (pro příslušnou odmocninu), vydělili dvěma (párování dělitelů) a zase bychom 1 přičetli.

Část b) by již byla složitější. Museli bychom uvažovat šestiprvkovou grupu permutací tříprvkové množiny. Ač 4 536 je dělitelné šesti, nestačí pouze výsledek vydělit. Museli bychom použít *Burnsideovo lemma.* Pro každou permutaci bychom určili počet fixních bodů, tedy počet trojic x, y, z, které se zobrazí samy na sebe. Následně bychom počty sečetli a na závěr vydělili 6.

Příklad 8.3. Kamarádi Artem, Barbora, Cyril, Danuše a Ervín jdou spolu do kina. V kině si sednou do řady vedle sebe. Kolika způsoby si mohou posedat, pokud chtějí, aby

a) Barbora seděla vedle Cyrila;

b) Danuše neseděla vedle Artema;

c) nastaly možnosti a) i b) současně?

Řešení. Označíme si osoby A, B, C, D a E. V a) můžeme uvažovat B a C za jednu osobu a pak výsledek vynásobit dvěma – B a C se mohou vždy prohodit. Zbývají 4 „osoby“ (tři osoby a jedna dvojice), které můžeme libovolně permutovat. Máme tedy $2 \cdot 4! = 2 \cdot 24 = 48$ možností.

V b) můžeme zjistit počet všech rozesazení a odečíst počet možností, kdy A a D sedí vedle sebe. Máme $5! - 2 \cdot 4! = 120 - 48 = 72$ možností.

Úlohu c) řešíme podobně jako b) s tím, že zároveň B a C považujeme za jednu osobu. Permutujeme 4 „osoby“ s tím, že odečítáme $2 \cdot 3!$ možností, kdy A a D sedí vedle sebe. Celkem máme $2 \cdot (4! - 2 \cdot 3!) = 2 \cdot (24 - 12) = 2 \cdot 12 = 24$ možností. △

Příklad 8.4. a) Kolika způsoby se může rozesadit 5 osob v pětimístném autě, když jen dva lidé mají řidičský průkaz?

b) V autobuse je vedle místa pro řidiče ještě 25 míst k sezení. Kolika způsoby se může rozesadit 20 cestujících a 2 řidiči?

Řešení. a) Nejprve posadíme jednoho řidiče. Následně máme $4! = 24$ možností, jak se rozesadí zbytek osazenstva. Pro každou možnost můžeme prohodit řidiče, máme tedy celkem 48 možností.

Jinak lze úlohu řešit tak, že máme 2 možnosti, kdo si sedne na místo řidiče, pak 4 možnosti, kdo na místo spolujezdce a na zadním sedadle máme postupně 3, 2 a 1 možnost. Výsledek vynásobíme, máme tedy $2 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 48$ možností.

b) Máme 2 možnosti, kdo si sedne na místo řidiče. Druhý řidič má 25 možností k sezení, první cestující 24, druhý 23, atd., přičemž poslední, dvacátý, cestující má 5 volných sedadel. Máme tedy celkem $2 \cdot 25 \cdot 24 \cdot \dots \cdot 6 \cdot 5$ možností.

Druhý způsob řešení je nejprve vybrat 21 sedadel pro cestující (pro 20 cestujících a druhého řidiče), to je možné $\binom{25}{21}$ způsoby, následně pro každý výběr sedadel máme 21! rozesazení, a pro každé rozesazení navíc dvě možnosti (prohazujeme řidiče). Celkový počet možností je tedy

$$2 \cdot \binom{25}{21} \cdot 21! = 2 \cdot \frac{25!}{21! \cdot 4!} \cdot 21! = \frac{25!}{4 \cdot 3}. \qquad \triangle$$

Příklad 8.5. Výsledné pořadí týmů první ligy se ztratilo, našlo se pouze relativní pořadí všech sedmi týmů z Čech a relativní pořadí všech šesti týmů z Moravy. Kolika způsoby lze z těchto částečných údajů sestavit pořadí první ligy? Kolika způsoby by to bylo možné, pokud by se první ligy účastnily ještě tři týmy ze Slezska, jejichž relativní pořadí také známe?

Řešení. Pořadí týmů z Čech je známé, stejně jako pořadí týmů z Moravy. Při určování celkových pořadí nás tedy pouze zajímá, jestli je tým na daném místě z Čech, nebo z Moravy. Určujeme proto počet možností, jak mezi sebe týmy seřadit. Pokud si například představíme týmy z Čech jako prvky a týmy z Moravy jako oddělovače, začíná úloha připomínat kombinace s opakováním. Máme tedy $\binom{7+6}{6} = \binom{13}{6} = 1\,716$ možností.

Jinak lze úlohu chápat tak, že určujeme počet permutací třináctiprvkové množiny, přičemž za stejné považujeme ty permutace, kde prohazujeme mezi sebou týmy z Čech a mezi sebou týmy z Moravy. Pak vyjde $\frac{13!}{7! \cdot 6!}$ možností, což je totéž, co $\binom{13}{6} = \binom{13}{7}$.

Přidáme-li týmy ze Slezska, již první způsob (který je vlastně ekvivalentní s druhým) nevede na kombinační číslo. Počet řešení je podobně

$$\frac{(7+6+3)!}{7! \cdot 6! \cdot 3!} = \frac{16!}{7! \cdot 6! \cdot 3!} = 960\,960. \qquad \triangle$$

8.3 Příklady k procvičení

Příklad 8.6. Kolika způsoby můžeme rozdělit (ne nutně spravedlivě) výběr z bankomatu $7 \times 1\,000\,\text{Kč}$ plus $6 \times 500\,\text{Kč}$ (přičemž nehledíme jen na celkovou částku, ale i na počty bankovek)

a) mezi tři lidi,

b) mezi čtyřčlenou rodinu tak, aby alespoň něco zůstalo matce, která peníze vybrala.

(Výsledky: a) $\binom{9}{2} \cdot \binom{8}{2}$, b) $\binom{10}{3} \cdot \binom{9}{3} - \binom{9}{2} \cdot \binom{8}{2}$.)

Příklad 8.7. Kamarádi Apolena, Bořivoj, Celestýna, Damián a Eliška jdou spolu do kina. V kině si sednou do řady vedle sebe. Kolika způsoby si mohou posedat, pokud chtějí, aby

a) ani Apolena ani Bořivoj neseděli na kraji,

b) Celestýna nebo Damián seděli přesně uprostřed,

c) nastaly obě možnosti a) i b) současně.

(Výsledky: a) $3 \cdot 2 \cdot 3!$, b) $2 \cdot 4!$, c) $2 \cdot 2! \cdot 2!$.)

Příklad 8.8. Na kolik oblastí může nejvýš rozdělit rovinu n přímek? Na kolik oblastí může nejvýš rozdělit prostor n rovin? (Výsledky: první otázka viz video ze cvičení 9, $p_n = p_{n-1}+n$, což se dá vyřešit jako $p_n = \binom{n+1}{2} + 1$; druhá otázka $r_n = r_{n-1} + p_{n-1}$, což se dá vyřešit jako $r_n = \binom{n+1}{3} + n + 1$, prvních pár členů je 1, 2, 4, 8, 15, ...)

Kapitola 9

Kombinatorika, pravděpodobnost

9.1 Opakování z přednášky

Připomeneme si definici a výpočet kombinačního čísla.

$$\binom{n}{k} \stackrel{\text{def}}{=} \frac{n!}{k!\,(n-k)!} = \frac{n\cdot(n-1)\cdot\dots\cdot(n-k+1)\cdot\cancel{(n-k)!}}{k!\,\cancel{(n-k)!}}$$

$$= \frac{n\cdot(n-1)\cdot\dots\cdot(n-k+1)}{k!}$$

Zavedeme si *klesající faktoriál z n podle k* vztahem

$$[n]_k := n\cdot(n-1)\cdot\dots\cdot(n-k+1) \tag{9.1}$$

pro $k \in \mathbb{N}$. Pro $k = 0$ speciálne klademe $[n]_0 = 1$ jako prázdný součin. Je vidět, že pak pro klasický faktoriál máme vztah $n! = [n]_n$. Vidíme, že ve vztahu (9.1) nepotřebujeme, aby n bylo přirozené číslo. Lze tedy vzorcem (9.1) definovat klesající faktoriál podle k z libovolného *reálného* (nebo i komplexního) čísla. (Podobně bychom si mohli zavést rostoucí faktoriál z n podle k jako

$$[n]^k := n\cdot(n+1)\cdot\dots\cdot(n+k-1),$$

což ale zde nebudeme potřebovat.) S touto symbolikou můžeme psát kombinační číslo jako

$$\binom{n}{k} = \frac{[n]_k}{k!}.$$

Při užití tohoto zápisu opět nepotřebujeme, aby n bylo přirozené číslo, můžeme proto definovat pro libovolné *reálné* (komplexní) číslo r (zobecněné) kombinační číslo

$$\binom{r}{k} := \frac{[r]_k}{k!}, \tag{9.2}$$

čteno r nad k. Dále je možno faktoriál zobecnit pomocí *Gamma funkce*. Ta je definována vztahem

$$\Gamma(z) := \int_0^\infty \mathrm{e}^{-t}\, t^{z-1}\,\mathrm{d}t$$

pro každé $z \in \mathbb{C} \setminus \{0, -1, -2, \dots\}$. Platí, že

$$\Gamma(n+1) = n!$$

pro $n \in \mathbb{N}_0$. Pak je možné definovat zobecněné kombinační číslo

$$\binom{z}{w} := \frac{\Gamma(z+1)}{\Gamma(w+1)\,\Gamma(z-w+1)}$$

pro libovolná z, $w \in \mathbb{C}$, pro něž je výraz napravo definován.

Nechť $n \in \mathbb{N}_0$. Definujeme si *dvojitý faktoriál*[1] z n rekurentním vztahem

$$n!! = \begin{cases} 1 & n \in 0, 1, \\ n \cdot (n-2) & n \geq 2. \end{cases}$$

Máme vyjádření

$$n!! = \begin{cases} 1 \cdot 3 \cdot 5 \cdot \dots \cdot n & n \text{ liché}, \\ 2 \cdot 4 \cdot 6 \cdot \dots \cdot n & n \text{ sudé}. \end{cases}$$

Odtud máme

$$n! = n!! \cdot (n-1)!! \tag{9.3}$$

jelikož n a $n-1$ jsou jedno sudé a jedno liché, následně si v součinu seskupíme zvlášť sudé a liché činitele. Můžeme počítat

$$(2\,k)!! = 2 \cdot 4 \cdot 6 \cdot \dots \cdot (2\,k) = 2^k\, k!,$$

tedy pro n sudé máme vyjádření $n!! = 2^{\frac{n}{2}} \left(\frac{n}{2}\right)!$. Dále můžeme díky (9.3) počítat

$$(2\,k+1)!! = \frac{(2\,k+1)!}{(2\,k)!!} = \frac{(2\,k+1)!}{2^k\, k!}. \tag{9.4}$$

Celkem máme tedy vyjádření dvojitého faktoriálu

$$n!! = \begin{cases} 2^{\frac{n}{2}} \left(\frac{n}{2}\right)! & n \text{ sudé}, \\ \frac{n!}{2^{\frac{n-1}{2}} \left(\frac{n-1}{2}\right)!} & n \text{ liché}. \end{cases}$$

[1] Také označovaný jako *semifaktoriál* z n.

9.2 Příklady řešené na cvičení

Příklad 9.1. V šatně si 4 návštěvníci odložili své kabáty a klobouky. Nešťastnou náhodou klobouky spadly na zem. Šatnářka chce klobouky opět pověsit, ale protože si nepamatuje, který patří komu, pověsí je k jednotlivým kabátům zcela náhodně. Kolika způsoby může klobouky pověsit tak, aby alespoň jeden návštěvník dostal svůj klobouk? Jaká je pravděpodobnost, že alespoň jeden návštěvník dostane svůj klobouk?

Řešení. Můžeme si kabáty i klobouky označit čísly 1 až 4. Pak vlastně hledáme všechny permutace čtyřprvkové množiny s alespoň jedním pevným bodem, a to pomocí principu inkluze a exkluze. Máme $\binom{4}{1}$ možností na výběr jednoho pevného bodu, pro každý z nich 3! permutací zbylých prvků. Některé permutace jsme započetli dvakrát, musíme proto odečíst $\binom{4}{2} \cdot 2!$ permutací s alespoň dvěma pevnými body. Permutace s alespoň 3 pevnými body – tedy identitu – jsme přičetli čtyřikrát a pak odečetli šestkrát, musíme ji tedy zpět přičíst třikrát. Celkem máme tedy

$$\binom{4}{1} \cdot 3! - \binom{4}{2} \cdot 2! + 3 \cdot 1! = 4 \cdot 6 - 6 \cdot 2 + 3 = 24 - 12 + 3 = 15$$

možností. Pravděpodobnost, že alespoň jeden návštěvník pak dostane svůj klobouk je

$$\frac{15}{4!} = \frac{15}{24} = \frac{5}{8} = 62,5\,\%. \qquad \triangle$$

Příklad 9.2. Na kolik oblastí může maximálně rozdělit rovinu n kružnic?

Řešení. Zřejmě 0 kružnic rozdělí rovinu na 1 oblast. 1 kružnice rovinu rozdělí na 2 oblasti – vnitřek a vnějšek. Pro dvě kružnice máme 4 oblasti – pokud kružnice nakreslíme tak, aby se protínaly ve dvou bodech, máme vnějšek, pak dvě oblasti ve vnitřku pouze jedné kružnice a oblast průniku obou vnitřků. U tří kružnic podobně dostaneme 3 oblasti vnitřků pouze jedné kružnice, 3 průniky vnitřků právě dvou kružnic, 1 průnik vnitřků všech tří kružnic a jeden vnějšek, tedy celkem 8 oblastí. Pro 4 kružnice je počítání malinko složitější – máme 4 vnitřky pouze jedné z kružnic, 4 průniky vnitřků právě dvou, 4 vnitřky průniků právě tří, jeden průnik vnitřků všech čtyř a vnějšek, celkem tedy dělí 4 kružnice rovinu až na 14 oblastí.

Určeme nyní obecný případ. Označme a_n maximální počet oblastí, na který dělí rovinu n kružnic. Zřejmě maxima dosáhneme tehdy, když se dvě různé kružnice protínají právě ve dvou různých bodech a neexistují společné průniky tří kružnic. Přidáním n-té kružnice k $(n-1)$ předchozím se nová kružnice rozdělí $2 \cdot (n-1)$ průsečíky na $2 \cdot (n-1)$ oblouků, přičemž každý z nich dělí jednu – ale ne každou – z a_{n-1} oblastí na 2 – dělí jich právě $2 \cdot (n-1)$. Máme tedy rekurentní vztah

$$a_n = a_{n-1} + 2 \cdot (n-1)$$

pro $n \geq 2$, kam můžeme dále dosazovat

$$a_n = a_{n-1} + 2 \cdot (n-1) =$$

$$\begin{aligned}
&= a_{n-2} + 2 \cdot \Big((n-1) + (n-2)\Big) = \\
&= a_{n-3} + 2 \cdot \Big((n-1) + (n-2) + (n-3)\Big) = \cdots = \\
&= a_1 + 2 \cdot \Big((n-1) + (n-2) + \cdots + 2 + 1\Big) = 2 + 2 \cdot \frac{n\,(n-1)}{2} = n^2 - n + 2,
\end{aligned}$$

čímž dostaneme explicitní vyjádření a_n pro $n \geq 2$. Vidíme, že pro $n = 1$ vzorec také funguje, neboť $1^2 - 1 + 2 = a_1$, tedy celkem dělí rovinu n kružnic na maximálně

$$a_n = \begin{cases} 1 & n = 0 \\ n^2 - n + 2 & n \geq 1 \end{cases}$$

oblastí. △

Poznámka. Aby bylo řešení úplně korektní, je potřeba dokázat, že n kružnic lze skutečně umístit v rovině tak, že se každé dvě protínají právě ve dvou bodech a přitom neexistují průsečíky tří a víc kružnic. Fakt, že dvě kružnice se protínají maximálně ve dvou bodech, je jednoduché dokázat. To, že je to možné pro n kružnic lze dokázat například indukcí. Důkaz nastíníme. Pro jednoduchost předpokládejme, že všechny kružnice mají stejný poloměr. Máme umístěných $n-1$ kružnic, chceme umístit n-tou. Její střed nesmí ležet moc *daleko*, čímž máme vyznačenou množinu možných středů n-té kružnice. Navíc jej musíme umístit tak, aby nevznikaly průsečíky tří, což ale znamená, že střed kružnice nesmí ležet na jedné z kružnic se středy v průsečících a stejnými poloměry. Tato zakázaná množina má ale *nulovou míru*, takže nová kružnice v obecné poloze bude mít s každou z předchozích 2 průsečíky.

Jinak si (poněkud nesprávně) lze představit situaci tak, že najdeme *Jordanovu křivku,*[2] která má právě 2 průsečíky s každou z předchozích $n-1$ kružnic, a následně deformujeme tuto křivku na kružnici tak, aby kýžená vlastnost zůstala zachována. Tento pohled je ovšem zavádějící a nevede k důkazu, protože již dvěma Jordanovými křivkami lze rovinu rozdělit na libovolně mnoho oblastí (ale minimálně na 2) – stačí si například představit hvězdu s k (oblými) cípy a skrz tyto cípy vést kružnici, což dělí rovinu na $2\,k + 2$ oblastí, čímž již dosáhneme potenciálního nekonečna.

Příklad 9.3. Spočítejte $\binom{-\frac{1}{2}}{n}$ pro $n \in \mathbb{N}_0$.

Řešení. Nejprve si spočítáme prvních pár hodnot.

$$\begin{aligned}
\binom{-\frac{1}{2}}{0} &= 1, & \binom{-\frac{1}{2}}{2} &= \frac{\left(-\frac{1}{2}\right) \cdot \left(-\frac{3}{2}\right)}{2} = \frac{3}{8} \\
\binom{-\frac{1}{2}}{1} &= -\frac{1}{2}, & \binom{-\frac{1}{2}}{3} &\frac{\left(-\frac{1}{2}\right) \cdot \left(-\frac{3}{2}\right) \cdot \left(-\frac{5}{2}\right)}{6} = -\frac{15}{48} = -\frac{5}{16}
\end{aligned}$$

[2] Tedy hladkou uzavřenou křivku bez průsečíků samy se sebou.

Nyní uvažujme případ obecného $n \in \mathbb{N}$. Díky vyjádření zobecněného kombinačního čísla (9.2) máme

$$\binom{-\frac{1}{2}}{n} = \frac{\left[-\frac{1}{2}\right]_n}{n} = \frac{-\frac{1}{2} \cdot \left(-\frac{1}{2} - 1\right) \cdot \dots \cdot \left(-\frac{1}{2} - n + 1\right)}{n!}$$

což si symbolikou $\prod$ můžeme vyjádřit jako

$$\begin{aligned} &= \frac{\prod_{i=0}^{n-1} \left(-\frac{1}{2} - i\right)}{n!} = \frac{\prod_{i=0}^{n-1} \left(-\frac{2\,i+1}{2}\right)}{n!} \\ &= (-1)^n \frac{\prod_{i=0}^{n-1} (2\,i+1)}{n!} = (-1)^n \frac{1 \cdot 3 \cdot \dots \cdot (2\,n-1)}{n!} = (-1)^n \frac{(2\,n-1)!!}{n!} \end{aligned}$$

což nyní můžeme přepsat díky (9.4) a $2\,n - 1 = 2\,(n-1) + 1$ jako

$$= (-1)^n \frac{(2\,n-1)!}{2^n \cdot n! \cdot 2^{n-1} \cdot (n-1)!}$$

což si díky vztahu $n + (n-1) = 2\,n - 1$ můžeme nakonec napsat jako

$$= \frac{(-1)^n}{2^{2\,n-1}} \cdot \frac{(2\,n-1)!}{n!\,(n-1)!}.$$

Z posledního vyjádření dostaneme pro $n \geq 1$ vztah

$$\binom{-\frac{1}{2}}{n} = \frac{(-1)^n}{2^{2\,n-1}} \cdot \binom{2\,n-1}{n}. \qquad \triangle$$

Příklad 9.4. Z váčku s 20 korunami, 15 dvoukorunami a 10 pětikorunami vytáhneme

a) 20 mincí,

b) 30 mincí.

Kolika způsoby to může dopadnout?

Řešení. Řešíme nejprve a). Předpokládejme, že vytáhneme i korunových mincí, j dvoukorun a k pětikorun. Platí

$$i + j + k = 20,$$

přičemž

$$\begin{aligned} i &\in \{0, 1, \dots, 20\}, \\ j &\in \{0, 1, \dots, 15\}, \\ k &\in \{0, 1, \dots, 10\}. \end{aligned} \tag{9.5}$$

Vzhledem k tomu, že vytahujeme 20 mincí, máme *nadbytek* korun, můžeme tedy zapomenout na omezení pro i. Pak sčítáme pro všechny možnosti $k = 0,\dots,10$ počty dvojic (i,j), $j \leq 15$, řešící rovnici

$$i + j = 20 - k.$$

Je-li $k = 0$, máme 16 možností pro j (0, 1, …, 15), každá z nich určuje jednoznačně i. Stejně tak máme 16 možností pro $k = 1$, 2, 3, 4, 5. Tedy pro $k \leq 5$ máme $6 \cdot 16 = 96$ možností. Pro $k = 6$ máme již jen 15 možností ($j = 0$, …, 14). Pro $k = 7$ máme 14 možností, počet se dále snižuje o 1, až pro $k = 10$ máme 11 možností pro i a j. Celkem máme tedy

$$6 \cdot 16 + 15 + 14 + 13 + 12 + 11 = 161$$

možností. Podobně můžeme řešit b). Určujeme vlastně počet řešení rovnice

$$i + j + k = 30$$

se stejnými omezeními (9.5). Musíme tedy již dbát i na omezení pro i. Můžeme procházet všechny možnosti pro k a počítat počty řešení rovnice $i + j = 30 - k$. Je-li $k = 0$, máme 6 možností (díky omezení pro i musí být j minimálně 10 a maximálně 15). Pro $k = 1$ může být již j mezi 9 a 15, tedy 7 možností. Analogicky máme 8 možností pro $k = 2$, 9 pro $k = 3$, atd., až pro $k = 10$ máme 16 možností. Celkem máme tedy

$$6 + 7 + \cdots + 16 = \frac{17 \cdot 16}{2} - \frac{6 \cdot 5}{2} = 121$$

možností.

Úlohu lze také řešit pomocí vytvořujících funkcí. Označme a_n počet možností, kterými lze z váčku s 20 korunami vytáhnout n korun. Zřejmě $a_n = 1$ pro $n \leq 20$ a 0 jinak. Podobně označme b_n počet možností, kterými lze z váčku s 15 dvoukorunami vytáhnout n dvoukorun, a c_n počet možností, kterými lze z váčku s 10 pětikorunami vytáhnout n pětikorun. Zřejmě je $b_n = 1$ $n \leq 15$ a 0 jinak, podobně $c_n = 1$ pro $n \leq 10$ a 0 jinak. Počet možností, kterými lze z váčku s 20 korunami, 15 dvoukorunami a 10 pětikorunami je roven n-tému členu konvoluce těchto posloupností, tedy číslu $(a * b * c)_n$. Vytvořující funkce posloupností a_n, b_n a c_n jsou polynomy

$$\begin{aligned}
\mathrm{V}(a)(x) &= 1 + x + x^2 + \cdots + x^{20},\\
\mathrm{V}(b)(x) &= 1 + x + x^2 + \cdots + x^{15},\\
\mathrm{V}(c)(x) &= 1 + x + x^2 + \cdots + x^{10},
\end{aligned}$$

které si můžeme přepsat pomocí částečných součtů geometrických řad jako

$$\begin{aligned}
\mathrm{V}(a)(x) &= \frac{1 - x^{21}}{1 - x},\\
\mathrm{V}(b)(x) &= \frac{1 - x^{16}}{1 - x},
\end{aligned}$$

$$\mathrm{V}(c)(x) = \frac{1-x^{11}}{1-x}.$$

Vytvořující funkce konvoluce posloupností $a * b * c$ je rovna součinu vytvořujících posloupností

$$\begin{aligned}\mathrm{V}(a*b*c)(x) &= \mathrm{V}(a)(x)\cdot\mathrm{V}(b)(x)\cdot\mathrm{V}(c)(x) = \frac{x^{21}-1}{x-1}\cdot\frac{x^{16}-1}{x-1}\cdot\frac{x^{11}-1}{x-1}\\ &= \frac{1-x^{11}-x^{16}-x^{21}+x^{27}+x^{32}+x^{37}-x^{48}}{(1-x)^3}\end{aligned}$$

kde pomocí trojí autokonvoluce posloupnosti samých jedniček (10.3) získáme vyjádření

$$= (1-x^{11}-x^{16}-x^{21}+x^{27}+x^{32}+x^{37}-x^{48})\cdot\sum_{k=0}^{\infty}\binom{k+2}{2}x^k$$

kde řada napravo bude ve skutečnosti od 46. mocniny dále nulová. Dvacátou mocninu získáme pomocí součinů $1\cdot x^{20}$ s koeficientem $\binom{22}{2}$, $x^{11}\cdot x^9$ s koeficientem $-\binom{11}{2}$ a $x^{16}\cdot x^4$ s koeficientem $-\binom{6}{2}$. U x^{20} máme tedy koeficient

$$\binom{22}{2} - \binom{11}{2} - \binom{6}{2} = 161.$$

Podobně třicátou mocninu získáme pomocí součinů $1\cdot x^{30}$, $x^{11}\cdot x^{19}$, $x^{16}\cdot x^{14}$, $x^{21}\cdot x^9$ a $x^{27}\cdot x^3$ s výsledným koeficientem rovným součtu koeficientů

$$\binom{32}{2} - \binom{21}{2} - \binom{16}{2} - \binom{11}{2} + \binom{5}{2} = 121.$$

Vidíme, že 20 mincí můžeme vytáhnout 161 způsoby a 30 mincí můžeme vytáhnout 121 způsoby. △

Příklad 9.5. Jaká je pravděpodobnost, že na 10 kostkách padne součet 25?

Řešení. Mějme posloupnost a, kde a_n značí počet možností, že při hodu jednou (klasickou) kostkou padne číslo n. Zřejmě $a_n = 1$ pro n mezi 1 a 6 a 0 jinak. Protože jsou hody deseti kostkami na sobě nezávislé, odpovídá počet možností, že součet při hodu bude n, n-tému členu desetinásobné konvoluce posloupnosti a se sebou. Členy této posloupnosti získáme pomocí vytvořujících funkcí. Máme

$$\mathrm{V}(a)(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 = x\cdot\frac{1-x^6}{1-x}.$$

Pak

$$\mathrm{V}(a^{*10})(x) = (\mathrm{V}(a)(x))^{10} = x^{10}\left(\frac{1-x^6}{1-x}\right)^{10}$$

Výraz na pravé straně si můžeme upravit. Pomocí binomické věty máme

$$(1-x)^{10} = \sum_{i=0}^{10} (-1)^i \binom{10}{i} x^{6\,i}.$$

Pak s využitím (10.3) máme

$$\mathrm{V}(a^{*10})(x) = x^{10} \cdot \sum_{i=0}^{10} (-1)^i \binom{10}{i} x^{6\,i} \cdot \sum_{j=0}^{\infty} \binom{j+9}{9} x^j.$$

Hledáme koeficient u x^{25}. Hledáme vlastně všechna řešení rovnice

$$10 + 6\,i + j = 25,$$

neboli $6\,i + j = 15$. Máme pouze 3 možnosti – $i = 0$ a $j = 15$ s koeficientem $(-1)^{10}\binom{10}{0} \cdot \cdot \binom{15+9}{9}$, $i = 1$ a $j = 9$ s koeficientem $(-1)^1\binom{10}{1} \cdot \binom{9+9}{9}$ a $i = 2$ a $j = 3$ s koeficientem $(-1)^2\binom{10}{2} \cdot \binom{3+9}{9}$. Celkem je tedy koeficient u x^{25} roven součtu, tedy číslu

$$\binom{24}{9} - 10\binom{18}{9} + \binom{10}{2}\binom{12}{9} = 831\,204.$$

Součet 25 při hodu 10 kostkami tedy může padnout 831 204 způsoby. Celkem může při hodu 10 kostkami padnout 6^{10} možností. Pravděpodobnost, že součet bude 25 je tedy

$$\frac{831\,204}{6^{10}} = \frac{831\,204}{60\,466\,176} = \frac{23\,089}{1\,679\,616} \approx 1,375\,\%. \qquad \triangle$$

9.3 Příklady k procvičení

Příklad 9.6. Určete, čemu se rovná $\binom{-1}{n}$. (Výsledek: $(-1)^n$.)

Příklad 9.7. Ve volejbalové extralize je 13 týmů. Po první polovině je odehráno 12 zápasů, z každého z nichž je možné získat 0, 1, 2 nebo 3 body, přičemž Brno předvedlo žalostný výsledek a získalo 10 bodů z 36 možných. Jaká je pravděpodobnost stejného bodového zisku, pokud by se každý zápas místo odehrání losoval se stejnou pravděpodobností $\frac{1}{4}$ pro každou z variant 0, 1, 2 a 3 body?

$$\text{(Výsledek: } \frac{\binom{12}{0}\binom{21}{11} - \binom{12}{1}\binom{17}{11} + \binom{12}{2}\binom{13}{11}}{4^{12}} = \frac{209\,352}{4^{12}} \approx 1,25\,\%.)$$

Příklad 9.8. Nevyvážená kostka má pravděpodobnost, že padne šestka, dvakrát vyšší než pro ostatní čísla. Jaká je pravděpodobnost, že při hodech čtyřmi takovými kostkami padne součet 13? (Výsledek: jedná se o koeficient u x^{13} ve výrazu

$$\left(\frac{1}{7}\,x + \cdots + \frac{1}{7}\,x^5 + \frac{2}{7}\,x^6\right) = \frac{x^4}{7^4} \cdot \left(\frac{1-x^6}{1-x} + x^5\right)^4$$

který můžeme pomocí binomické věty upravit na

$$\frac{x^4}{7^4}\left(\sum_{\substack{0\le k\le 4\\ 0\le l\le k}}\binom{4}{k}\binom{k}{l}(-2)^{k-l}\,x^{6\,k-l}\right)\left(\sum_{k=0}^{\infty}\binom{k+3}{3}x^k\right)$$

odkud dojdeme k výsledku

$$\frac{\binom{4}{0}\binom{0}{0}(-2)^0\binom{12}{3}+\binom{4}{1}\binom{1}{0}(-2)^1\binom{6}{3}+\binom{4}{1}\binom{1}{1}(-2)^0\binom{7}{3}}{7^4}=\frac{200}{7^4}\approx 8,33\,\%,$$

pro obyčejnou kostku vyjde podobně $\frac{140}{6^4}\approx 10,80\,\%$.)

Kapitola 10

Posloupnosti, vytvořující funkce

10.1 Opakování z přednášky

Mějme posloupnost přirozených (celých, reálných, komplexních, ...) čísel $a = \{a_n\}_{n=0}^{\infty}$. Její vytvořující funkcí rozumíme (formální) mocninnou řadu

$$\mathrm{V}\, a := \sum_{n=0}^{\infty} a_n\, x^n.$$

Konverguje-li tato řada absolutně na nějakém okolí 0, pak zadává na okolí 0 (hladkou) funkci.[1] Dostáváme tak korespondenci mezi (vhodnými) posloupnostmi čísel a analytickými funkcemi definovanými na nějakém okolí nuly. Danou funkci značíme $\mathrm{V}\, a$, nebo $\mathrm{V}(a)(x)$.

Pro příklad je vytvořující funkce posloupnosti samých jedniček geometrická řada

$$V(\{1\}_{n=0}^{\infty}) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Zde je přehled vlastností vytvořujících funkcí posloupností.

- Přiřazení vytvořující funkce je *lineární operátor*, tj.

  $$\mathrm{V}(\alpha\, a + \beta\, b) = \alpha\ \mathrm{V}\, a + \beta\ \mathrm{V}\, b$$

  pro α, $\beta \in \mathbb{R}$ a a, b posloupnosti.

- Vytvořující funkce má v nule všechny deriace, tj. Taylorův rozvoj vytvořující funkce je

  $$\mathrm{V}(a)(x) = \sum_{k=0}^{\infty} \frac{\mathrm{V}(a)^{(k)}(0)}{k!}\, x^k,$$

  odkud

  $$\mathrm{V}^{(k)}(0) = k!\, a_k.$$

- Vytvořující funkce lze derivovat jako řadu člen po členu i jako funkci, zde je nutný nenulový poloměr konvergence řady! Pak

$$\frac{\mathrm{d}\,\mathrm{V}(a)(x)}{\mathrm{d}x} = \sum_{k=1}^{\infty} a_k\, k\, x^{k-1} = \sum_{k=0}^{\infty} (k+1)\, a_{k+1}\, x^k,$$

  tj. jedná se o vytvořující funkci posloupnosti $\{(k+1)\, a_{k+1}\}_{k=0}^{\infty}$.

- Podobně lze vytvořující funkci integrovat jako funkci i jako mocninnou řadu člen po členu. Stejně jako v případě derivace je nutný nenulový poloměr konvergence. Pak

$$\int_0^x \mathrm{V}(a)(t)\,\mathrm{d}t = \sum_{k=0}^{\infty} a_k\, \frac{x^{k+1}}{k+1},$$

  takže jde o vytvořující funkci posloupnosti A definované vztahy $A_0 = 0$ a $A_k = \frac{a_{k-1}}{k}$ pro $k \geq 1$.

- Konvolučním součinem dvou posloupností $a = \{a_k\}_{k=0}^{\infty}$ a $b = \{b_k\}_{k=0}^{\infty}$ rozumíme posloupnost $a * b$, kde

$$(a * b)_k = \sum_{i+j=k} a_i\, b_j = \sum_{i=0}^{k} a_i\, b_{k-i}.$$

  Jedná se o koeficient k-tého člene rozvoje součinu $\mathrm{V}(a) \cdot \mathrm{V}(b)$, jelikož se jedná o koeficient k-tého člene v Cauchyovském součinu mocninných řad. Odtud vidíme, že konvlouční součin je asociativní, komutativní a distributivní vzhledem ke sčítání.

- Konstanty $\alpha \in \mathbb{R}$ si můžeme ztotožnit s posloupnostmi $(\alpha, 0, 0, \dots)$. Pak skalární násobek $\alpha\, a$ posloupnosti a odpovídá součinu $\alpha * a$.

- Lineární funkce x je vytvořující funkcí posloupnosti $(0, 1, 0, 0, \dots) =: x$, kterou proto označíme stejně. Pak x^n je vytvořující funkcí posloupnosti $\underbrace{x * x * \cdots * x}_{n} = x^{*n}$.

- Polynomy jsou vytvořující funkce konečných posloupností. Vzhledem k předchozímu lze polynom $p_0 + p_1\, x + \cdots + p_n\, x^n$ chápat jako vytvořující funkci posloupnosti

$$p_0 + p_1 * x + \cdots + p_n * x^{*n},$$

  kde konstanty a x chápeme jako posloupnosti dle předchozích bodů.

- Mějme posloupnost $a = \{a_k\}_{k=0}^{\infty}$ a $n \in \mathbb{N}$. Definujme posloupnost b předpisem $b_k = 0$ pro $k < n$ a $b_k = a_{k-n}$ pro $k \geq n$. Jedná se o posloupnost $(\underbrace{0, \dots, 0}_{n}, a_0, a_1 \dots)$. Pomocí konvoluce ji lze vyjádřit jako $b = a * x^{*n}$, tudíž $\mathrm{V}\, b = x^n\ \mathrm{V}\, a$.

- Mějme posloupnost $a = \{a_k\}_{k=0}^{\infty}$ a $n \in \mathbb{N}$. Definujme posloupnost b předpisem $b_k = a_{k+n}$. Pak
$$\mathrm{V}(b)(x) = \frac{\mathrm{V}(a)(x) - a_0 - a_1\,x - \ldots - a_{n-1}\,x^{n-1}}{x^n}. \tag{10.1}$$
(Tento vztah by také bylo možné zapsat pomocí konvolucí, museli bychom ale povolit indexování členů posloupností i zápornými čísly.)

Na závěr si připoměňme některé užitečné vzorečky. Nechť $a = \{a_k\}_{k=0}^{\infty}$. Posloupnost částečných součtů definujeme předpisem $s_k = \sum_{i=0}^{k} a_i$. Pak platí
$$\mathrm{V}(s)(x) = \frac{\mathrm{V}(a)(x)}{1-x} \tag{10.2}$$
Dvěma způsoby si odvodíme následující vzorec.
$$\frac{1}{(1-\alpha\,x)^{n+1}} = \sum_{k=0}^{\infty} \binom{k+n}{n} \alpha^k\,x^k \tag{10.3}$$
Začneme se součtem geometrické řady $\sum_{k=0}^{\infty} y^k = \frac{1}{1-y}$. Substitucí $y = \alpha\,x$ získáme vztah
$$\frac{1}{1-\alpha\,x} = \sum_{k=0}^{\infty} \alpha^k\,x^k, \tag{10.4}$$
kde suma napravo konverguje absolutně na intervalu $\left(-\frac{1}{|\alpha|}, \frac{1}{|\alpha|}\right)$. Můžeme proto (10.4) n-krát derivovat, čímž dostaneme
$$(-1)\,(-2)\cdots(-n)\frac{(-\alpha)^n}{(1-\alpha\,x)^{n+1}} = \sum_{k=n}^{\infty} \alpha^k\,k\,(k-1)\cdots(k-n+1)\,x^{k-n}$$
což si můžeme dále upravit na
$$n!\,\frac{\alpha^n}{(1-\alpha x)^{n+1}} = \sum_{k=0}^{\infty} \alpha^{k+n}\,(k+n)\,(k+n-1)\cdots(k+1)\,x^k$$
kde pravou stranu upravíme na
$$n!\,\frac{\alpha^n}{(1-\alpha x)^{n+1}} = \sum_{k=0}^{\infty} \alpha^{k+n}\,\frac{(k+n)!}{k!}\,x^k$$
odkud podělením rovnice $n!$ a α^n dostaneme
$$\frac{1}{(1-\alpha x)^n} = \sum_{k=0}^{\infty} \alpha^k \frac{(k+n)!}{k!\,n!}\,x^k.$$
Platí ovšem $\frac{(k+n)!}{k!\,n!} = \binom{k+n}{k} = \binom{k+n}{n}$, čímž dostaneme finální vzoreček. Jinou možností je nejprve vzít $(n+1)$-násobnou autokonvoluci posloupnosti samých jedniček, kde k-tý člen bude počet řešení rovnice $i_1 + \cdots + i_{n+1} = k$, tedy kombinační číslo $\binom{k+n+1-1}{n+1-1} = \binom{k+n}{n}$ (dělíme k jedniček do $n+1$ přihrádek). Následně stačí vzít substituci $y = \alpha\,x$.

10.2 Příklady řešené na cvičení

Příklad 10.1. Rozložte na parciální zlomky funkci

$$\frac{5\,x-4}{x^2-x-2}.$$

Řešení. Máme rozklad

$$x^2-x-2=(x+1)\,(x-2).$$

Proto můžeme psát

$$\frac{5\,x-4}{x^2-x-2}=\frac{A}{x-2}+\frac{B}{x-1}. \tag{10.5}$$

Zbývá najít konstanty A a B. Rovnici (10.5) si vynásobíme x^2-x-2 a na pravé straně si výraz upravíme na lineární tvaru $a\,x+b$.

$$\begin{aligned}5\,x-4&=A\,(x+1)+B\,(x-2)\\5\,x-4&=(A+B)\,x+A-2\,B\end{aligned}$$

Nyní si díky lineární nezávislosti 1 a x vyjádřime rovnici jako lineární soustavu

$$\begin{pmatrix}1&1\\1&-2\end{pmatrix}\cdot\begin{pmatrix}A\\B\end{pmatrix}=\begin{pmatrix}5\\-4\end{pmatrix}.$$

Tu řešíme například pomocí Gaussovy eliminace.

$$\left(\begin{array}{cc|c}1&1&5\\1&-2&-4\end{array}\right)\sim\left(\begin{array}{cc|c}1&1&5\\0&-3&-9\end{array}\right)\sim\left(\begin{array}{cc|c}1&1&5\\0&1&3\end{array}\right)\sim\left(\begin{array}{cc|c}1&0&2\\0&1&3\end{array}\right)$$

Vidíme, že $A=2$ a $B=3$. Máme tedy rozklad na parciální zlomky

$$\frac{5\,x-4}{x^2-x-2}=\frac{2}{x-2}+\frac{3}{x+1}.$$ △

Příklad 10.2. Rozviňte do mocninné řady následující funkce.

a) $\frac{1}{(1-x)^2}$ b) $\frac{5\,x-4}{x^2*-x-2}$ c) $\frac{x}{x+5}$ d) $\frac{x^2+x+2}{2\,x^3-x^2-4\,x+3}$

Řešení. a) Máme funkci $\frac{1}{(1-x)^2}$. Můžeme si pomoci součtem geometrické řady

$$\sum_{k=0}^{\infty}x^k=\frac{1}{1-x} \tag{10.6}$$

která konverguje *absolutně* na $(-1,1)$. Lze proto derivovat (10.6) člen po členu.

$$\sum_{k=1}^{\infty}k\,x^{k-1}=-1\cdot(-1)\cdot(1-x)^{-2}$$

Výrazy si upravíme a dostaneme výsledný rozvoj do geometrické řady.

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

Jiná možnost řešení je vzpomenout si na vzorec (10.3) pro $\alpha = 1$. Z něj máme rozklad rovnou.

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

Řada konverguje na $(-1, 1)$.

b) Funkce je stejná jako v příkladu 10.1. Máme tedy rozklad na parciální zlomky

$$\frac{5\,x-4}{x^2-x-2} = \frac{2}{x-2} + \frac{3}{x+1}.$$

Každý ze zlomků si rozvineme zvlášť. Máme rovnou

$$\frac{3}{1+x} = 3 \cdot \sum_{k=0}^{\infty} (-1)^k\, x^k$$

na $(-1, 1)$. Dále počítáme

$$\frac{2}{x-2} = -\frac{1}{1-\frac{x}{2}} = -\sum_{k=0}^{\infty} \left(\frac{x}{2}\right)^k = -\sum_{k=0}^{\infty} \frac{1}{2^k}\, x^k.$$

Řada konverguje pro $\frac{x}{2} \in (-1, 1)$, neboli na intervalu $(-2, 2)$. Výsledný rozvoj získáme jako součet řad, který bude konvergovat na průniku, tedy na intervalu $(-1, 1)$.

$$\frac{5\,x-4}{x^2-x-2} = 3 \cdot \sum_{k=0}^{\infty} (-1)^k\, x^k - \sum_{k=0}^{\infty} \frac{1}{2^k}\, x^k = \sum_{k=0}^{\infty} \left(3 \cdot (-1)^k - \frac{1}{2^k}\right) x^k$$

c) Můžeme si funkci $\frac{x}{x+5}$ upravovat a rovnou získáme rozvoj.

$$\frac{x}{x+5} = \frac{x}{5} \cdot \frac{1}{1+\frac{x}{5}} = \frac{x}{5} \cdot \sum_{k=0}^{\infty} \left(-\frac{x}{5}\right) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{5^k}\, x^k$$

Řada konverguje pro $-\frac{x}{5} \in (-1, 1)$, neboli pro $x \in (-5, 5)$.

d) Nejprve si musíme funkci $\frac{x^2+x+2}{2\,x^3-x^2-4\,x+3}$ rozložit na parciální zlomky. Máme rozklad

$$2\,x^3 - x^2 - 4\,x + 3 = (x-1)^2\,(2\,x+3).$$

Pak bude platit

$$\frac{x^2+x+2}{2\,x^3-x^2-4\,x+3} = \frac{A}{x-1} + \frac{B}{(x-1)^2} + \frac{C}{2\,x+3} \tag{10.7}$$

pro nějaké konstanty A, B, $C \in \mathbb{Q}$. Nalezneme je obvyklým způsobem – rovnici (10.7) si vynásobíme $(x-1)^2\,(2\,x+3)$ a dáme si k sobě koeficienty u monomů příslušné mocniny.

$$\begin{aligned} x^2+x+2 &= A\,(x-1)(2\,x+3) + B\,(2\,x+3) + C\,(x-1)^2 \\ x^2+x+2 &= (2\,A+C)\,x^2 + (A+2\,B-2\,C)\,x - 3\,A + 3\,B + C \end{aligned}$$

Dostaneme soustavu lineárních rovnic

$$\begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & -2 \\ -3 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix},$$

kterou řešíme pomocí Gaussovy eliminace s výběrem pivota.

$$\left(\begin{array}{ccc|c} 2 & 0 & 1 & 1 \\ 1 & 2 & -2 & 1 \\ -3 & 3 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|c} 2 & 0 & 1 & 1 \\ 5 & 2 & 0 & 3 \\ -5 & 3 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 2 & 0 & 1 & 1 \\ 5 & 2 & 0 & 3 \\ 0 & 5 & 0 & 4 \end{array}\right) \sim$$
$$\sim \left(\begin{array}{ccc|c} 2 & 0 & 1 & 1 \\ 25 & 0 & 0 & 7 \\ 0 & 5 & 0 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 0 & 0 & 25 & 11 \\ 25 & 0 & 0 & 7 \\ 0 & 5 & 0 & 4 \end{array}\right)$$

Pak $A = \frac{7}{25}$, $B = \frac{4}{5}$ a $C = \frac{11}{25}$. Máme tedy rozklad

$$\frac{x^2+x+2}{2\,x^3-x^2-4\,x+3} = \frac{7}{25}\,\frac{1}{x-1} + \frac{4}{5}\,\frac{1}{(x-1)^2} + \frac{11}{25}\,\frac{1}{2\,x+3}$$

což si upravíme do tvaru vhodného pro použití vzorce (10.3)

$$= -\frac{7}{25}\,\frac{1}{1-x} + \frac{4}{5}\,\frac{1}{(1-x)^2} + \frac{11}{75}\,\frac{1}{1-\left(-\frac{2}{3}\,x\right)}.$$

Za použití (10.3), resp. (10.4) dostaneme

$$\frac{x^2+x+2}{2\,x^3-x^2-4\,x+3} = \sum_{k=0}^{\infty} \left[-\frac{7}{25} + \frac{4}{5}\binom{k+1}{1} + \frac{11}{75}\left(-\frac{2}{3}\right)^k \right] x^k,$$

což si upravíme na finální rozvoj

$$\frac{x^2+x+2}{2\,x^3-x^2-4\,x+3} = \sum_{k=0}^{\infty} \left[\frac{4}{5}\,k + \frac{13}{25} + \frac{11}{25}\,\frac{(-2)^k}{3^{k+1}} \right] x^k. \qquad \triangle$$

Příklad 10.3. Určete vytvořující funkce pro následující posloupnosti.

a) $\left\{2\,(k+1)\right\}_{k=0}^{\infty}$

b) $\left\{2\,k+1\right\}_{k=0}^{\infty}$

c) $\left\{(-1)^k\,(k+1)\right\}_{k=0}^{\infty}$

d) $\left\{(k+1)^3\right\}$

Řešení. a) Vytvořující funkcí bude součet mocninné řady

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

kde jsme si vzpomněli na řešení části a) příkladu 10.2. Řada má součet pro všechna $x\in(-1,1)$, což bude také definiční obor naší vytvořující funkce.

b) Opět hledáme součet mocninné řady

$$\sum_{k=0}^{\infty}(2\,k+1)\,x^k.$$

Můžeme si psát $2\,k+1 = 2\,(k+1)-1$, tedy

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

kde pro pravou stranu použijeme vzorec (10.3), čímž dostaneme výsledek

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

c) Hledáme součet

$$\sum_{k=0}^{\infty}(-1)^k\,(k+1)\,x^k.$$

Jelikož $k+1 = \binom{k+1}{1}$, stačí použít vzorec (10.3) pro $n=1$ a $\alpha=-1$. Máme tak na $(-1,1)$ součet

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

d) Hledáme součet řady

$$\sum_{k=0}^{\infty}(k+1)^3\,x^k.$$

Vzpomeneme si na (10.3), odkud na intervalu $(-1,1)$ máme

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

Chceme si výraz $(k+1)^3$ vyjádřit pomocí kombinačních čísel tvaru $\binom{k+n}{n}$. Máme

$$k+1 = \binom{k+1}{1}. \tag{10.8}$$

Dále

$$\binom{k+2}{2} = \frac{(k+2)\,(k+1)}{2} = \frac{1}{2}\,(k+1+1)\,(k+1) = \frac{1}{2}\,\Big((k+1)^2 + (k+1)\Big),$$

neboli (s vyjádřením $k+1$ z (10.8))

$$(k+1)^2 = 2 \cdot \binom{k+2}{2} - \binom{k+1}{1}. \tag{10.9}$$

Následně

$$\binom{k+3}{3} = \frac{(k+3)\,(k+2)\,(k+1)}{6} = \frac{1}{6}\,(k+1)\,(k+1+1)\,(k+1+2) = \\ = \frac{1}{6}\Big((k+1)^3 + 3\,(k+1)^2 + 2\,(k+1)\Big),$$

takže

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

kam si dosadíme za $(k+1)^2$ z (10.9) a za $k+1$ z (10.8), takže máme

$$(k+1)^3 = 6 \cdot \binom{k+3}{3} - 6 \cdot \binom{k+2}{2} + \binom{k+1}{1}. \tag{10.10}$$

Pak díky (10.10) a (10.3) dostaneme

$$\begin{aligned}\sum_{k=0}^{\infty} (k+1)^3\, x^k &= 6 \cdot \sum_{k=0}^{\infty} \binom{k+3}{3} x^k - 6 \cdot \sum_{k=0}^{\infty} \binom{k+2}{2} x^k + \sum_{k=0}^{\infty} \binom{k+1}{1} x^k \\ &= \frac{6}{(1-x)^4} - \frac{6}{(1-x)^3} + \frac{1}{(1-x)^2} = \frac{6 - 6\,(1-x) + (1-x)^2}{(1-x)^4} \\ &= \frac{x^2 + 4\,x - 1}{(x-1)^4}\end{aligned}$$

vytvořující funkci na intervalu $(-1, 1)$. △

Poznámka (k části d)). (Zobecněné) kombinační číslo $\binom{x+n}{n}$ je díky definici

$$\binom{x+n}{n} = \frac{[x+n]_n}{n} = \frac{(x+n)\cdot(x+n-1)\cdot\dots\cdot(x+1)}{n!}$$

vlastně *polynomem* stupně n v proměnné x, lze tedy říci, že $\binom{x+n}{n} \in \mathbb{Q}[x]$ ($\mathbb{R}[x]$, $\mathbb{C}[x]$), přičemž o jedna se zvětšující stupně zajišťují, že množina

$$\left\{\binom{x+n}{n}\right\}_{n=0}^{\infty}$$

tvoří *bázi* vektorového prostoru polynomů nad daným tělesem. To znamená, že libovolný polynom

$$p(x) \in \mathbb{Q}[x] \quad (\text{nebo } \mathbb{R}[x], \mathbb{C}[x])$$

lze vyjádřit jako (konečnou) lineární kombinaci zobecněných kombinačních čísel podobným způsobem jako v části d). Stejně jako tam je výpočet *rekurentní* – mocninu x^n si vyjádříme pomocí $\binom{x+n}{n}$ a *nižších* mocnin x. Lze tedy říci, že vytvořující funkce posloupnosti $\{p(k)\}_{k=0}^{\infty}$, kde p je nějaký polynom, bude lineární kombinací funkcí $\frac{1}{(1-x)^{n+1}}$, přičemž nejvyšší použité n je právě stupeň polynomu p.

Příklad 10.4. Najděte vzorec pro součet $1 + 2^2 + 3^2 + \cdots + k^2$.

Řešení. Uvažujme posloupnost $a_k = k^2$ pro $k \in \mathbb{N}_0$. Hledáme vzorec pro částečný součet členů této posloupnosti, tedy pro předpis posloupnosti $s_k = \sum_{i=0}^{k} a_k$. Použijeme k tomu vytvořující funkce.

Chceme vyjádřit k^2 jako lineární kombinaci $\binom{k+n}{n}$. Máme

$$2 \cdot \binom{k+2}{2} = 2 \cdot \frac{(k+2)\,(k+1)}{2} = k^2 + 3\,k + 2,$$

neboli $k^2 = 2\binom{k+2}{2} - 3\,k - 2$. Jelikož $k = \binom{k+1}{1} - 1$, dostáváme

$$k^2 = 2\binom{k+2}{2} - 3\binom{k+1}{1} + 1.$$

Pak vytvořující funkce posloupnosti a je (vzpomeneme si na (10.3))

$$\mathrm{V}(a)(x) = \frac{2}{(1-x)^3} - \frac{3}{(1-x)^2} + \frac{1}{1-x}.$$

Díky (10.2) máme

$$\mathrm{V}(s)(x) = \frac{\mathrm{V}(a)(x)}{1-x} = \frac{2}{(1-x)^4} - \frac{3}{(1-x)^3} + \frac{1}{(1-x)^2}.$$

Následně opět použijeme (10.3), abychom získali výsledek:

$$\begin{aligned} s_k &= 2\binom{k+3}{3} - 3\binom{k+2}{2} + 1\binom{k+1}{1} \\ &= \frac{k^3}{3} + \frac{k^2}{2} + \frac{k}{6}. \end{aligned}$$

△

Poznámka. Podobně by se dalo postupovat i obecněji. Máme-li posloupnost $a_k = p(k)$, kde

$$\begin{aligned} p(x) &= p_0 + p_1\,x + \cdots + p_n\,x^n \\ &= P_0\binom{x+0}{0} + P_1\binom{x+1}{1} + \cdots + P_n\binom{x+n}{n} \end{aligned}$$

je polynom, bude pro posloupnost částečných součtů posloupnosti a_k platit

$$s_k = P_0\binom{k+1}{1} + P_1\binom{k+2}{2} + \cdots + P_n\binom{k+n+1}{n+1}.$$

Příklad 10.5. Najděte vzorec pro součet $1 - 2 + 3 - 4 + \cdots + (-1)^{k+1}\,k$.

Řešení. Intuitivně bychom viděli, že součty jsou 1, -1, 2, -2, atd. Pak pro $\ell \geq 1$ platí $s_{2\,\ell-1} = -\ell$ a $s_{2\,\ell} = \ell$.

Najděme explicitní vzorec pro k-tý člen pomocí vytvořujících funkcí. Zaveďme si proto posloupnost $a = \{(-1)^k\,(k+1)\}_{k=0}^{\infty}$ a posloupnost jejích částečných součtů s. Potřebujeme získat vytvořující funkce $\mathrm{V}\,a$ a $\mathrm{V}\,s$. Podle vzorce (10.3) pro $n = 1$ a $\alpha = -1$ máme na $(-1, 1)$

$$\mathrm{V}(a)(x) = \frac{1}{(1+x)^2}.$$

Následně máme podle (10.2)

$$\mathrm{V}(s)(x) = \frac{1}{(1+x)^2\,(1-x)} = \frac{A}{1+x} + \frac{B}{(1+x)^2} + \frac{C}{1-x}.$$

Musíme určit konstanty A, B a C. Platí

$$\begin{aligned} 1 &= A\,(1-x^2) + B\,(1-x) + C\,(1+x)^2 = A\,(1-x^2) + B\,(1-x) + C\,(1+2\,x+x^2) \\ &= (-A+C)\,x^2 + (-B+2\,C)\,x + A + B + C. \end{aligned}$$

Řešíme tedy lineární rovnici

$$\begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Schematicky

$$\left(\begin{array}{ccc|c} -1 & 0 & 1 & 0 \\ 0 & -1 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 1 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 4 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & \frac{1}{4} \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & \frac{1}{4} \\ 0 & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & \frac{1}{4} \end{array}\right)$$

tedy $A = \frac{1}{4}$, $B = \frac{1}{2}$ a $C = \frac{1}{4}$. Pak

$$\begin{aligned}\mathrm{V}(s)(x) &= \frac{1}{4}\cdot\frac{1}{1+x} + \frac{1}{2}\cdot\frac{1}{(1+x)^2} + \frac{1}{4}\cdot\frac{1}{1-x}\\ &\overset{(10.3)}{=} \frac{1}{4}\,\mathrm{V}\Big((-1)^k\Big)(x) + \frac{1}{2}\,\mathrm{V}\Big((-1)^k\,(k+1)\Big)(x) + \frac{1}{4}\,\mathrm{V}(1)(x),\end{aligned}$$

tedy

$$s_k = \frac{2\,(-1)^k\,(k+1) + (-1)^k + 1}{4} = \frac{(-1)^k\,(2\,k+3)+1}{4}. \qquad \triangle$$

Příklad 10.6. Nechť $p \in \mathbb{N}$ je perioda. Definujme posloupnost a_k předpisem

$$a_k := \begin{cases} 1 & p \mid k, \\ 0 & \text{jinak.}\end{cases}$$

Určete vytvořující funkci posloupnosti a a vzorec pro k-tý člen.

Řešení. Pokud $p = 1$, pak $a_k = 1$ pro každé k (což je rovnou předpis pro k-tý člen) a vytvořující funkce je $\frac{1}{1-x}$. Nechť tedy $p > 1$. Pak zřejmě

$$\begin{aligned}\mathrm{V}(a)(x) &= 1 + x^p + x^{2\,p} + \cdots\\ &= \sum_{k=0}^{\infty} x^{p\,k} = \frac{1}{1-x^p}.\end{aligned}$$

Pro zjištění předpisu pro k-tý člen chceme rozložit polynom $1 - x^p$ na lineární činitele tvaru $1 - \alpha x$. Substitucí $x = \frac{1}{t}$ a vynásobením t^p bychom zjistili, že α budou právě kořeny polynomu $x^p - 1$. Vezměme

$$\zeta_p := \mathrm{e}^{\frac{2\,\pi\,\mathrm{i}}{p}} = \cos\frac{2\,\pi}{p} + \mathrm{i}\,\sin\frac{2\pi}{p}.$$

Jedná se o p-tou odmocninu z jedné, neboť

$$\zeta_p^p = \left(\mathrm{e}^{\frac{2\,\pi\,\mathrm{i}}{p}}\right)^p = \mathrm{e}^{p\cdot\frac{2\,\pi\,\mathrm{i}}{p}} = \mathrm{e}^{2\,\pi\,\mathrm{i}} = 1.$$

Ze stejného důvodu bude také i (celočíselná) mocnina ζ_p odmocninou z jedné. Jelikož má $x^p - 1$ v $\mathbb{C}$ p různých kořenů (má p kořenů počítaných i s násobností a je nesoudělný se svojí derivací), jsou jimi právě různé mocniny ζ_p. Máme tak rozklad

$$\begin{aligned}1 - x^p &= \prod_{i=1}^{p}(1-\zeta_p^i)\\ &= (1-\zeta_p\,x)\cdot(1-\zeta_p^2\,x)\cdot\cdots\cdot(1-\zeta_p^{p-1}x)\cdot(1-x).\end{aligned}$$

Bude tedy platit

$$\mathrm{V}(a)(x) = \frac{1}{1-x^p} = \frac{A_1}{1-\zeta_p\,x} + \cdots + \frac{A_p}{1-x}$$

$$= \sum_{i=1}^{p-1} \frac{A_i}{1 - \zeta_p^i\, x}.$$

Vynásobením $1 - x^p$ zjistíme, že

$$1 = \sum_{i=1}^{p} A_i \prod_{j \neq i} (1 - \zeta_p^j\, x).$$

Z Viètových vztahů plyne, že

$$\sum_{i=1}^{p} \zeta_p^i = \sum_{i \neq j} \zeta_p^i\, \zeta_p^j = \cdots = \sum_{i_1 \neq i_2 \neq \cdots \neq i_n} \zeta_p^{i_1} \cdot \dots \cdot \zeta_p^{i_n} = 0$$

a to pro všechny n-tice pro n od jedné po $p - 1$. Odtud vidíme, že můžeme vzít $A_i = \frac{1}{p}$. (Jelikož součet A_i s koeficienty rovnými součinům mocnin ζ_p^j musí být vždy nulový, což je splněno, jsou-li A_i stejné; $\sum_{i=1}^{p} A_i = 1$ určuje hodnotu A_i). Máme tedy

$$\mathrm{V}(a)(x) = \frac{1}{p} \cdot \left[\frac{1}{1 - \zeta_p\, x} + \frac{1}{1 - \zeta_p^2\, x} + \cdots + \frac{1}{1 - \zeta_p^{p-1}\, x} + \frac{1}{1 - x} \right],$$

odkud můžeme získat vzorec pro k-tý člen.

$$a_k = \frac{\zeta_p^k + \zeta_p^{2\,k} + \cdots + \zeta_p^{(p-1)\,k} + 1}{p} \qquad \triangle$$

Poznámka. Číslo ζ_p je obecně komplexní iracionální. (Je však vždy algebraické jako kořen polynomu $x^p - 1$.) Reálné je pouze pro $p = 1$ – $\zeta_1 = 1$ – a pro $p = 2$ – $\zeta_2 = -1$. Máme pro $p = 2$ vytvořující funkci

$$\frac{1}{1 - x^2} = \frac{1}{2} \left[\frac{1}{1 - x} + \frac{1}{1 + x} \right],$$

a odtud vzorec $\frac{(-1)^k + 1}{2}$ pro posloupnost, kde sudé členy jsou 1 a liché 0. Dále například pro $p = 4$ máme $\zeta_4 = \mathrm{i}$, rozklad

$$\frac{1}{1 - x^4} = \frac{1}{4} \left[\frac{1}{1 - x} + \frac{1}{1 + x} + \frac{1}{1 - \mathrm{i}\, x} + \frac{1}{1 + \mathrm{i}\, x} \right]$$

a vzorec

$$\frac{1 + (-1)^k + \mathrm{i}^k + (-\mathrm{i})^k}{4} = \frac{\mathrm{i}^k + \mathrm{i}^{2\,k} + \mathrm{i}^{3\,k} + \mathrm{i}^{4\,k}}{4} = \begin{cases} 1 & 4 \mid k \\ 0 & \text{jinak.} \end{cases}$$

Poznámka. Podobně můžeme získat vzorec pro k-tý člen libovolné periodické posloupnosti. Je-li posloupnost b_k periodická s periodou p, lze ji určit konečně mnoha hodnotami B_0, B_1, …, B_{p-1}. Pak b_k je rovno tomu z B_ℓ, pro něž je $k \equiv \ell \pmod{p}$. To lze také psát tak, že

$$b_k = \sum_{i=0}^{p-1} B_i\, a_{k-i},$$

neboli že je b součtem vhodných násobků vhodně posunutých posloupností a. Pak díky vlastnostem vytvořujících funkcí je

$$\mathrm{V}(b)(x) = \frac{B_0 + B_1\,x + \cdots + B_{p-1}\,x^{p-1}}{1 - x^p}$$

a

$$b_k = \sum_{i=0}^{p-1} \frac{B_i}{p} \cdot \left(\zeta_p^{k-i} + \zeta_p^{2\,(k-i)} + \cdots + \zeta_p^{(p-1)\,(k-i)} + 1\right).$$

Samozřejmě však tyto vzorce nejsou pro praktické počítání příliš vhodné, při implementaci je daleko jednodušší použít podmíněný příkaz.

10.3 Příklady k procvičení

Příklad 10.7. Rozviňte do mocninné řady funkci

a) $\frac{x^2-10}{x^2+x-2}$,

b) $\frac{x}{x^3-5\,x^2+8\,x-4}$.

(Výsledky: a) rozklad na parciální zlomky vyjde $1 + \frac{2}{2+x} + \frac{3}{1-x}$, pak rozvoj vyjde $1 + {} + \sum_{k=0}^{\infty} \left(\left(-\frac{1}{2}\right)^k + 3\right) x^k$, tj. $a_k = [k = 0] + \left(-\frac{1}{2}\right)^k + 3$; b) rozklad na parciální zlomky vyjde $-\frac{1}{1-x} + \frac{1}{2-x} + \frac{2}{(2-x)^2}$, rozvoj pak $\sum_{k=0}^{\infty} \left(-1 + \left(\frac{1}{2}\right)^{k+1} + \left(\frac{1}{2}\right)^{k+1} (k+1)\right) x^k$, tj. $b_k = {} = -1 + \frac{k+2}{2^{k+1}}$.)

Příklad 10.8. Určete vytvořující funkci posloupnosti $\{k^2\}_{k=0}^{\infty}$. (Výsledek: $k^2 = 2\binom{k+2}{2} - {} - 3\binom{k+1}{1} + 2\binom{k+0}{0}$, tudíž $\mathrm{V}(k^2)(x) = \frac{2}{(1-x)^3} - \frac{3}{(1-x)^2} + \frac{2}{1-x} = \frac{2\,x^2-x+1}{(1-x)^3}$.)

Příklad 10.9. Najděte vzorec pro součet $1{\cdot}2^1 + 2{\cdot}2^2 + 3{\cdot}2^3 + \cdots + k{\cdot}2^k$. (Výsledek: vytvořující funkce vyjde $\frac{2\,x}{(1-x)\,(1-2\,x)^2} = \frac{2}{1-x} - \frac{4}{1-2\,x} + \frac{2}{(1-2\,x)^2}$, vzorec pro k-tý člen je $(k-1)\,2^{k+1} + 2$.)

Kapitola 11

Řešení rekurencí

11.1 Opakování z přednášky

Rekurencí řádu n obecně rozumíme rovnici (soustavu rovnic)

$$\mathcal{F}(a_k, a_{k-1}, \ldots, a_{k-n}, k, \mathbf{p}) = 0, \tag{11.1}$$

kde $\mathcal{F}\colon \mathbb{R}^{n+1} \times \mathbb{N}_0 \times P \to \mathbb{R}$ je funkce, jejíž hodnota závisí na $n+1$ členech neznámé posloupnosti a, indexu k a potenciálně vícesložkovém parametru $\mathbf{p} \in P$, kde P je množina parametrů. Soustavu uvažujeme pro všechna $\mathbb{Z}$, $\mathbb{N}$, nebo pro nějakou vhodnou podmnožinu. Rekurence tvaru

$$a_k = F(a_{k-1}, \ldots, a_{k-n}, k, \mathbf{p})$$

se nazývá rozřešená vzhledem k členu nejvyššího indexu. Zpravidla se uvažuje platná pro $k \geq n$, hodnoty a_0, …, a_{n-1} jsou pak počátečními podmínkami. Zde se budeme zabývat lineárními rekurencemi s konstatními koeficinety, tj. rekurencemi tvaru

$$a_k = A_1\, a_{k-1} + A_2\, a_{k-2} + \cdots + A_n\, a_{k-n} + f_k, \tag{11.2}$$

pro $k \geq n$, kde A_1, …, A_n jsou konstanty a f_k je nějaká posloupnost.

K řešení použijeme vytvořující funkce. Máme tři různé metody přechodu od rekurencí k vytvořujícím funkcím. První metoda je nejpřímočařejší. Rovnou si (11.2) vynásobíme x^k a pak sčítáme přes všechna $k \geq n$. Následně přičítáním a odečítáním konečně mnoha členů dostaneme kýžené vytvořující funkce. V praxi

$$\begin{aligned}
\sum_{k=n}^{\infty} a_{k-i}\, x^k &= x^i \sum_{k=n}^{\infty} a_{k-i}\, x^{k-i} = x^i \sum_{k=n-i}^{\infty} a_k\, x^k \\
&= x^i \left(-a_0 - a_1\, x - \cdots - a_{n-i-1}\, x^{n-i-1} + \sum_{k=0}^{\infty} a_k\, x^k \right) \\
&= -a_0\, x^i - a_1\, x^{i+1} - \cdots - a_{n-i-1}\, x^{n-1} + x^i\ \mathrm{V}(a)(x)
\end{aligned}$$

pro $i < n$. To provedeme pro všechna $i < n$. Podobně získáme vytvořující funkci pro posloupnost f_k. Tímto způsobem převedeme rekurenci na funkcionální rovnici, kde neznámou je vytvořující funkce.

Druhé dva způsoby přechodu využívají úpravy rekurence do tvaru, který platí pro všechna $k \geq 0$ (respektive v požadované množině). První metoda je teoreticky obecnější. Rovnice (11.1) můžeme přeindexováním upravit do tvaru

$$\mathcal{F}(a_{k+n}, a_{k+n-1}, \ldots, a_k, k+n, \mathbf{p}) = 0,$$

přičemž nyní platí pro všechna $k \geq 0$. V našich podmínkách rovnice (11.2) dostaneme

$$a_{k+n} = A_1\, a_{k+n-1} + A_2\, a_{k+n-2} + \cdots + A_n\, a_k + f_{k+n},$$

což platí pro $k \geq 0$, vynásobíme x^k a sčítáme přes všechna k. Pro dopočítání do tvaru s vytvořujícími funkcemi využíváme (10.1).

Poslední metoda je pro naše účely rovnice tvaru (11.2) nejužitečnější. Zavedeme si symbolik hranatých závorek. Buď φ výrok. Pak zavedeme

$$[\varphi] := \begin{cases} 1 & \varphi \quad \text{platí}, \\ 0 & \varphi \text{ neplatí}. \end{cases} \tag{11.3}$$

Zejména budeme používat $[k = i]$. Rovnice (11.2) platí pro $k \geq n$. Pro $i < n$ si dosadíme do (11.2) na levou stranu zadané hodnoty a_i, a na pravé straně spočítáme hodnotu výrazu, přičemž klademe $a_{-m} := 0$ pro $m \in \mathbb{N}$. Následně k pravé straně přičteme konstantu C tak, aby rovnost platila. Do všech rovnic rekurence pak přičteme na pravou stranu výraz $C \cdot [k = i]$, který je nenulový (a roven C) pouze pro $k = i$. Tak učiníme pro všechna $0 \leq i < n$. Takto upravená rekurence

$$\begin{aligned} a_k = A_1\, a_{k-1} + A_2\, a_{k-2} + \cdots + A_n\, a_{k-n} + f_k + \\ + C_0\,[k=0] + C_1\,[k=1] + \cdots + C_{n-1}\,[k=n-1] \end{aligned}$$

platí již pro všechna $k \geq 0$, můžeme tudíž sčítat rovnou přes všechna k sčítat. Pak

$$\sum_{k=0}^{\infty} a_{k-i}\, x^k = x^i \sum_{k=0}^{\infty} a_{k-i}\, x^{k-i} = x^i \sum_{k=0}^{\infty} a_k\, x^k = x^i\ \mathrm{V}(a)(x)$$

protože členy se zápornými mocninami x mají nulové koeficienty. Výrazy $C_i\,[k=i]$ jsou nenulové, pouze násobí-li se x^i, dávají tedy $C_i\, x^i$. Pak tedy po pořechodu k vytvořujícím funkcím řešíme rovnici

$$\begin{aligned} \mathrm{V}(a)(x) = A_1\, x\ \mathrm{V}(a)(x) + \cdots + A_n\, x^n\, Vf(a)(x) + \\ + \mathrm{V}(f)(x) + C_0 + C_1\, x + \cdots + C_{n-1}\, x^{n-1}. \end{aligned}$$

Rovnici pro vytvořující funkci vyřešíme vzhledem, tj. zjistíme předpis vytvořující funkce. Následně musíme rozvinout tuto funkci do mocninné řady, přičemž se bude hodit rozklad na parciální zlomky z Kapitoly 10. Nakonec a_k bude koeficient u x^k v rozvoji funkce.

Dále řešíme úlohy, kde jsou posloupnosti sdružené rekurencemi, tj. v rovnicích nevystupuje posloupnost jedna, ale máme hned několik posloupností (počtu posloupností musí odpovídat počet rovnic, jinak budeme mít volné parametry). Princip řešení je stejný – chceme přejít od posloupností k vytvořujícím funkcím. Po přechodu (např. jedním ze způsobů popsaných výše pro lineární rovnice, jiné zde ani řešit nebudeme) dostaneme soustavu funkcionálních rovnic (tj. neznámými jsou funkce proměnné x), kterou vyřešíme. Získáme tak předpisy vytvořujících funkcí hledaných posloupností, z nich opět standardním způsobem odvodíme vzorce pro k-té členy.

Řešíme-li soustavu dvou lineárních (funkcionálních) rovnic, bude se hodit známý vzoreček pro inverzi k matici 2×2.

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \frac{1}{\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \frac{1}{a\,d - b\,c} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \end{aligned} \tag{11.4}$$

11.2 Příklady řešené na cvičení

Příklad 11.1. Pomocí vytvořující funkce vyřešte následující rekurenci:

$$a_k = 2\,a_{k-1} + 3\,k^2 + 2\,k + 5$$

pro $k \geq 1$, $a_0 = 0$.

Řešení. Chceme přejít k vytvořujícím funkcím. Ukážeme všechny možnosti. První možností je rovnou vynásobit x^k a sčítat přes všechna $k \geq 1$. Potřebujeme si vyjádřit polynom $3\,k^2 + 2\,k + 5$ pomocí kombinačních čísel. Máme $1 = \binom{k+0}{0}$, $k = \binom{k+1}{1} - 1$, dále

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

tedy

$$k^2 = 2\binom{k+2}{2} - 3\binom{k+1}{1} + 1,$$

odtud

$$3\,k^2 + 2\,k + 5 = 6\binom{k+2}{2} - 7\binom{k+1}{1} + 6. \tag{11.5}$$

Máme tedy pro $k \geq 1$

$$a_k = 2\,a_{k-1} + 6\binom{k+2}{2} - 7\binom{k+1}{1} + 6.$$

Rovnici vynásobíme x^k a sčítáme přes všechna $k \geq 1$.

$$\sum_{k=1}^{\infty} a_k\,x^k = 2\sum_{k=1}^{\infty} a_{k-1}\,x^k + 6\sum_{k=1}^{\infty}\binom{k+2}{2}x^k - 7\sum_{k=1}^{\infty}\binom{k+1}{1}x^k + 6\sum_{k=1}^{\infty}x^k$$

K sumě vlevo si přičteme a odečteme $a_0\,x^0$, což v našem případě, $a_0 = 0$ nic nedělá. Z první sumy napravo si vytkneme x a přeznačíme tak, aby šla suma od 0. K posledním třem sumám si opět přičteme a odečteme členy s x^0.

$$\begin{aligned}\sum_{k=0}^{\infty} a_k\,x^k = 2\,x\sum_{k=0}^{\infty} a_k\,x^k + 6\sum_{k=0}^{\infty}\binom{k+2}{2}x^k - 7\sum_{k=0}^{\infty}\binom{k+1}{1}x^k + \\ + 6\sum_{k=0}^{\infty}x^k - 6\binom{0+2}{2} + 7\binom{0+1}{1} - 6 \qquad (11.6)\end{aligned}$$

Poslední člen na konci je -5. Sumy s $a_k\,x^k$ dávají vytvořující funkci $\mathrm{V}(a)(x)$, takže si je dáme vlevo a vytkneme. Vpravo použijeme vzorec (10.3).

$$(1-2\,x)\;\mathrm{V}(a)(x) = \frac{6}{(1-x)^3} - \frac{7}{(1-x)^2} + \frac{6}{1-x} - 5 = \frac{5\,x^3 - 9\,x^2 + 10}{(1-x)^3}$$

Poděleném $1-2\,x$ získáme vytvořující funkci.

$$\mathrm{V}(a)(x) = \frac{5\,x^3 - 9\,x^2 + 10}{(1-x)^3\,(1-2\,x)}$$

Jinou možností je přepsat si rekurenci tak, aby platila pro všechna $k \geq 0$.

$$a_{k+1} = 2\,a_k + 3\,(k+1)^2 + 2\,(k+1) + 5, \qquad (11.7)$$

Zaveďme si posloupnost $b_k = a_{k+1}$. Pak lze (11.7) přepsat jako

$$b_k = 2\,a_k + 3\,(k+1)^2 + 2\,(k+1) + 5.$$

Nyní si cheme výraz $3\,(k+1)^2 + 2\,(k+1) + 5$ zapsat pomocí kombinačních čísel. Máme $(k+1) = \binom{k+1}{1}$ a $(k+1)^2 = 2\binom{k+2}{2} - \binom{k+1}{1}$ díky (10.9). Pak platí

$$b_k = 2\,a_k + 6\binom{k+2}{2} - \binom{k+1}{1} + 5$$

což můžeme vynásobit x^k a sčítat přes všechna $k \geq 0$, abychom dostali (díky (10.3))

$$\mathrm{V}(b)(x) = 2\,\mathrm{V}(a)(x) + \frac{6}{(1-x)^3} - \frac{1}{(1-x)^2} + \frac{5}{1-x}.$$

Jelikož $\mathrm{V}(b)(x) = \frac{\mathrm{V}(a)(x) - a_0}{x} = \frac{\mathrm{V}(a)(x)}{x}$ díky $a_0 = 0$, máme rovnici

$$\frac{\mathrm{V}(a)(x)}{x} - 2\,\mathrm{V}(a)(x) = \frac{6}{(1-x)^3} - \frac{1}{(1-x)^2} + \frac{5}{1-x}$$

neboli

$$\frac{1-2\,x}{x}\,\mathrm{V}(a)(x) = \frac{10 - 9\,x + 5\,x^2}{(1-x)^3},$$

což si můžeme přepsat na

$$\mathrm{V}(a)(x) = \frac{5\,x^3 - 9\,x^2 + 10\,x}{(1-x)^3\,(1-2\,x)}.$$

Další možností je využít symboliky hranatých závorek (11.3). Máme zadáno $a_0 = 0$, podle vzorce

$$a_0 = 2\,a_{-1} + 5 = 5$$

neboť klademe $a_{-k} := 0$, musíme tedy odečíst v zadávající rovnici 5, ale jenom pro $k = 0$. Získáme rovnici

$$a_k = 2\,a_{k-1} + 3\,k^2 + 2\,k + 5 - 5\,[k = 0]$$

platnou pro všechna $k \geq 0$, kterou vynásobíme x^k a sčítáme přes všechna nezáporná k. Po úpravě polynomu pomocí (11.5) získáme

$$\sum_{k=0}^{\infty} a_k\,x^k = \sum_{k=0}^{\infty} a_{k-1}\,x^k + 6\sum_{k=0}^{\infty}\binom{k+2}{2}x^k - 7\sum_{k=0}^{\infty}\binom{k+1}{1}x^k + 6\sum_{k=0}^{\infty}x^k - 5$$

Z první sumy vytkneme x, pak máme vytvořující funkci. Ty dáme k sobě na levou stranu a vytkneme je. Pak získáme vlastně (11.6). Napravo použijeme geometrickou řadu, sečteme, podělíme $1 - 2\,x$ a získáme vytvořující funkci.

$$\begin{aligned}\mathrm{V}(a)(x) &= \frac{5\,x^3 - 9\,x^2 + 10\,x}{(1-x)^3\,(1-2\,x)} \\ &= \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{(1-x)^3} + \frac{D}{1-2\,x}\end{aligned}$$

Všemi třemi postupy jsme získali stejnou vytvořující funkci. To je samozřejmě dáno tím, že jsou ekvivalentní.

Nalezneme konstanty A, B, C a D standardním způsobem. Rovnici si vynásobíme $(1-x)^3\,(1-2\,x)$ a získáme

$$\begin{aligned}5\,x^3-9\,x^2+10\,x &= A\,(1-x)^2\,(1-2\,x)+B\,(1-x)\,(1-2\,x)+\\ &\quad +C\,(1-2\,x)+D\,(1-x)^3\\ &= (-2\,A-D)\,x^3+(5\,A+2\,B+3\,D)\,x^2+\\ &\quad +(-4\,A-3\,B-2\,C-3\,D)\,x+A+B+C+D.\end{aligned}$$

Odtud máme soustavu lineárních rovnic, kterou si zapíšeme schematicky a řešíme Gaussovou eliminací s výběrem pivota.

$$\left(\begin{array}{rrrr|r}-2&0&0&-1&5\\5&2&0&3&-9\\-4&-3&-2&-3&10\\1&1&1&1&0\end{array}\right)\sim\left(\begin{array}{rrrr|r}2&0&0&1&-5\\-1&2&0&0&6\\2&-3&-2&0&-5\\-1&1&1&0&5\end{array}\right)\sim$$

$$\sim\left(\begin{array}{rrrr|r}2&0&0&1&-5\\-1&2&0&0&6\\0&-1&0&0&5\\-1&1&1&0&5\end{array}\right)\sim\left(\begin{array}{rrrr|r}2&0&0&1&-5\\-1&0&0&0&16\\0&1&0&0&-5\\-1&0&1&0&10\end{array}\right)\sim\left(\begin{array}{rrrr|r}0&0&0&1&27\\1&0&0&0&-16\\0&1&0&0&-5\\0&0&1&0&-6\end{array}\right)$$

Takže máme $A=-16$, $B=-5$, $C=-6$ a $D=27$. Pak

$$\mathrm{V}(a)(x)=-\frac{16}{1-x}-\frac{5}{(1-x)^2}-\frac{6}{(1-x)^3}+\frac{27}{1-2\,x}.$$

S použitím (10.3) dostaneme vzorec pro k-tý člen.

$$\begin{aligned}a_k &= -16-5\binom{k+1}{1}-6\binom{k+2}{2}+27\cdot 2^k\\ &= 27\cdot 2^k-16-5\,(k+1)-3\,(k+2)\,(k+1)\\ &= 27\cdot 2^k-3\,k^2-14\,k-27\\ &= 27\,(2^k-1)-3\,k^2-14\,k\end{aligned}$$ △

Příklad 11.2. Pomocí vytvořující funkce vyřešte následující rekurenci:

$$a_k=3\,a_{k-1}-2\,a_{k-2}$$

pro $k\geq 2$, $a_0=1$, $a_1=3$.

Řešení. Budeme počítat prvně s abstraktními hodnotami a_0, a_1, následně dosadíme. Také již použijeme pouze postup se symbolikou hranatých závorek (11.3). Rovnici

$$a_k=3\,a_{k-1}-2\,a_{k-2}$$

si upravíme tak, aby platila pro všechna k. Pro $k = 0$ máme

$$a_0 = \underbrace{3\,a_{-1} - 2\,a_{-2}}_{0} + a_0\,[k = 0],$$

pro $k = 1$ pak

$$a_1 = \underbrace{3\,a_0 - 2\,a_{-1}}_{3\,a_0} - 3\,a_0\,[k = 0] + a_1\,[k = 1].$$

Celkem tedy máme rekurenci

$$a_k = 3\,a_{k-1} - 2\,a_{k-2} + a_0\,[k = 0] + (a_1 - 3\,a_0)\,[k = 1]$$

platnou pro všechna $k \geq 0$ (dokonce pro $k \in \mathbb{Z}$, neboť pro záporná k bychom dostali $0 = 0$), kterou vynásobíme x^k a sčítáme od 0 do ∞.

$$\sum_{k=0}^{\infty} a_k\,x^k = 3\,\sum_{k=0}^{\infty} a_{k-1}\,x^k - 2\,\sum_{k=0}^{\infty} a_{k-2}\,x^k + a_0 + (a_1 - 3\,a_0)\,x$$

Z poslední sumy si vytkneme x^2, z prostřední sumy x, následně (s přeindexováním) dostaneme

$$\sum_{k=0}^{\infty} a_k\,x^k = 3\,x\,\sum_{k=0}^{\infty} a_k\,x^k - 2\,x^2\,\sum_{k=0}^{\infty} a_k\,x^k + a_0 + (a_1 - 3\,a_0)\,x,$$

kde sumy již jsou vytvořujícími funkcemi pro a, tedy

$$\mathrm{V}(a)(x) = 3\,x\;\mathrm{V}(a)(x) - 2\,x^2\;\mathrm{V}(a)(x) + a_0 + (a_1 - 3\,a_0)\,x$$

Dáme si na levou stranu výrazy s $\mathrm{V}\,a$, kterou vytkneme, a na pravou výrazy bez ní. Máme

$$\begin{aligned}\mathrm{V}(a)(x)\,(1 - 3\,x + 2\,x^2) &= (a_1 - 3\,a_0)\,x + a_0.\\ \mathrm{V}(a)(x) &= \frac{(a_1 - 3\,a_0)\,x + a_0}{1 - 3\,x + 2\,x^2}.\end{aligned}$$

Máme rozklad $2\,x^2 - 3\,x + 1 = (2\,x - 1)\,(x - 1) = (1 - 2\,x)\,(1 - x)$, budeme tedy mít rozklad

$$\mathrm{V}(a)(x) = \frac{A}{1 - 2\,x} + \frac{B}{1 - x}.$$

Zbývá najít standardním způsobem konstanty A a B. Platí

$$\begin{aligned}(a_1 - 3\,a_0)\,x + a_0 &= A\,(1 - x) + B\,(1 - 2\,x)\\ &= (-A - 2\,B)\,x + (A + B).\end{aligned}$$

Dostaneme soustavu lineárních rovnic, kterou řešíme schematicky.

$$\left(\begin{array}{cc|r} -1 & -2 & a_1 - 3\,a_0 \\ 1 & 1 & a_0 \end{array}\right) \sim \left(\begin{array}{cc|r} 0 & -1 & a_1 - 2\,a_0 \\ 1 & 1 & a_0 \end{array}\right) \sim \left(\begin{array}{cc|r} 0 & 1 & -a_1 + 2\,a_0 \\ 1 & 0 & a_1 - a_0 \end{array}\right)$$

Pak $A = a_1 - a_0$ a $B = 2\,a_0 - a_1$ a platí

$$\mathrm{V}(a)(x) = \frac{a_1 - a_0}{1 - 2\,x} + \frac{2\,a_0 - a_1}{1 - x},$$

odkud již pomocí (10.3) získáme vzorec pro k-tý člen

$$\begin{aligned} a_k &= (a_1 - a_0)\,2^k + 2\,a_0 - a_1 \\ &= (2^k - 1)\,a_1 + (2 - 2^k)\,a_0. \end{aligned}$$

Povšimněme si, že pro $k = 0$ dostaneme a_0 a pro $k = 1$ dostaneme a_1. Také si všimněte, že a_k je jako číslo[1] *lineární kombinací* čísel a_0 a a_1. To je dáno tím, že rovnice zadávající naši rekurenci je homogenní. V zadání máme $a_0 = 1$ a $a_1 = 3$, takže

$$a_k = 2 \cdot 2^k - 1 = 2^{k+1} - 1. \qquad \triangle$$

Příklad 11.3. Pomocí vytvořující funkce vyřešte následující rekurenci:

$$a_k = 6\,a_{k-1} - 5\,a_{k-2} + 16\,k$$

pro $k \geq 2$, $a_0 = -4$, $a_1 = -9$.

Řešení. Rovnou budeme dosazovat za a_0 a a_1. Rekurenci si přepíšeme pomocí symboliky hranatých závorek (11.3) tak, aby platila pro všechna k. Pro $k = 0$ máme

$$-4 = a_0 = \underbrace{6\,a_{-1} - 5\,a_{-2}}_{0} + 16 \cdot 0 - 4\,[k = 0],$$

pro $k = 1$ pak

$$-9 = a_1 = \underbrace{\overbrace{6\,a_0 - 5\,a_{-1}}^{-24} + 16 \cdot 1}_{-8} - [k = 1].$$

Celkem tak získáme rekurenci

$$a_k = 6\,a_{k-1} - 5\,a_{k-2} + 16\,k - 4\,[k = 0] - [k = 1]$$

platnou pro všechna $k \geq 0$, kterou vynásobíme x^k a sčítáme přes všechna platná k, kde jsme si $16\,k$ vyjádřili jako $16\binom{k+1}{1} - 16$.

$$\sum_{k=0}^{\infty} a_k\,x^k = 6\sum_{k=0}^{\infty} a_{k-1}x^k - 5\sum_{k=0}^{\infty} a_{k-2}\,x^k + 16\sum_{k=0}^{\infty}(k+1)\,x^k - 16\sum_{k=0}^{\infty} x^k - 4 - x$$

[1] Jako posloupnost je a lineární kombinací posloupností $\{2^k\}_{k=0}^{\infty}$ a $\{1\}_{k=0}^{\infty}$.

Ze sum s a_k si vytkneme a po případném přeznačení získáme vytvořující funkce. U ostatních využijeme (10.3) a dostaneme

$$\mathrm{V}(a)(x) = 6\,x\ \mathrm{V}(a)(x) - 5\,x^2\ \mathrm{V}(a)(x) + \frac{16}{(1-x)^2} - \frac{16}{1-x} - 4 - x.$$

Nyní si seskupíme nalevo výrazy s $\mathrm{V}\,a$ a napravo bez ní.

$$\mathrm{V}(a)(x)\,(1 - 6\,x - 5\,x^2) = \frac{16}{(1-x)^2} - \frac{16}{1-x} - 4 - x = \frac{-x^3 - 2\,x^2 + 23\,x - 4}{(1-x)^2}$$

Máme rozklad $1 - 6\,x + 5\,x^2 = (1 - 5\,x)(1 - x)$ (součin koeficientů u x musí být koeficient u x^2, součet koeficient u x). Podělením tedy získáme finální tvar vytvořující funkce.

$$\begin{aligned}\mathrm{V}(a)(x) &= -\frac{x^3 + 2\,x^2 - 23\,x + 4}{(1-x)^3(1-5\,x)} \\ &= \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{(1-x)^3} + \frac{D}{1-5\,x}\end{aligned}$$

Standardním způsobem zjistíme koeficienty A, B, C a D.

$$\begin{aligned}-x^3 - 2\,x^2 + 23\,x - 4 &= A\,(1-x)^2\,(1-5\,x) + B\,(1-x)\,(1-5\,x) \\ &\quad + C\,(1-5\,x) + D\,(1-x)^3 \\ &= (-5\,A - D)\,x^3 + (11\,A + 5\,B + 3\,D)\,x^2 \\ &\quad + (-7\,A - 6\,B - 5\,C - 3\,D)\,x + (A + B + C + D)\end{aligned}$$

Získáme soustavu lineárních rovnic, kterou řešíme schematicky Gaussovou eliminací s výběrem pivota.

$$\left(\begin{array}{rrrr|r} -5 & 0 & 0 & -1 & -1 \\ 11 & 5 & 0 & 3 & -2 \\ -7 & -6 & -5 & -3 & 23 \\ 1 & 1 & 1 & 1 & -4 \end{array}\right) \sim \left(\begin{array}{rrrr|r} 5 & 0 & 0 & 1 & 1 \\ -4 & 5 & 0 & 0 & -5 \\ 8 & -6 & -5 & 0 & 26 \\ -4 & 1 & 1 & 0 & -5 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{rrrr|r} 5 & 0 & 0 & 1 & 1 \\ -4 & 5 & 0 & 0 & -5 \\ -12 & -1 & 0 & 0 & 1 \\ -4 & 1 & 1 & 0 & -5 \end{array}\right) \sim \left(\begin{array}{rrrr|r} 5 & 0 & 0 & 1 & 1 \\ -64 & 0 & 0 & 0 & 0 \\ -12 & -1 & 0 & 0 & 1 \\ -16 & 0 & 1 & 0 & -4 \end{array}\right) \sim \left(\begin{array}{rrrr|r} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -4 \end{array}\right)$$

Máme $A = 0$, $B = -1$, $C = -4$ a $D = 1$. Platí tedy

$$\mathrm{V}(a)(x) = \frac{1}{1-5\,x} - \frac{1}{(1-x)^2} - \frac{4}{(1-x)^3}.$$

S použitím vzorce (10.3) získáme vzorec pro k-tý člen.

$$a_k = 5^k - \binom{k+1}{1} - 4\binom{k+2}{2}$$

$$\begin{aligned} &= 5^k - (k+1) - 2\,(k+2)\,(k+1) \\ &= 5^k - 2\,k^2 - 7\,k - 5 \end{aligned} \qquad \triangle$$

Příklad 11.4. Najděte explicitní vyjádření pro k-té členy posloupností $a = \{a_k\}_{k=0}^{\infty}$ a $b = \{b_k\}_{k=0}^{\infty}$, které jsou definované vztahy

$$\begin{aligned} a_k - b_{k-1} &= 2, \\ b_k - a_{k-1} &= 0 \end{aligned}$$

pro $k \geq 1$, $a_0 = 1$ a $b_0 = 0$.

Poznámka. Z druhé rekurence si můžeme vyjádřit $b_{k-1} = a_{k-2}$, následně dosadit do první a získat rovnici

$$a_k - a_{k-2} = 2$$

pro $k \geq 2$, kde počáteční podmínky jsou $a_0 = 1$, $a_1 = 2 + b_0 = 2$. Tím si úlohu můžeme převést na řešení jedné rekurence, což by vedlo k výsledku. Pro názornost však budeme úlohu řešit pomocí propojených rekurencí.

Řešení. Nejprve řešíme pro a_0, b_0 abstraktní, následně dosadíme. Postupujeme klasicky, obě rovnice si upravíme pomocí symboliky hranatých závorek (11.3) tak, aby platily pro všechna $k \geq 0$. Máme

$$\begin{aligned} a_0 - \underbrace{b_{-1}}_{0} &= 2 - 2\,[k=0] + a_0\,[k=0] = 2 + (a_0 - 2)\,[k=0], \\ b_0 - \underbrace{a_{-1}}_{0} &= 0 + b_0\,[k=0]. \end{aligned}$$

Získáme tedy soustavu

$$\begin{aligned} a_k - b_{k-1} &= 2 + (a_0 - 2)\,[k=0] \\ b_k - a_{k-1} &= b_0\,[k=0], \end{aligned}$$

kterou si vynásobíme x^k a sčítáme přes všechna $k \geq 0$. Máme

$$\begin{aligned} \sum_{k=0}^{\infty} a_k\,x^k - \sum_{k=0}^{\infty} b_{k-1}\,x^k &= 2\sum_{k=0}^{\infty} x^k + a_0 - 2, \\ \sum_{k=0}^{\infty} b_k\,x^k - \sum_{k=0}^{\infty} a_{k-1}\,x^k &= b_0. \end{aligned}$$

Soustavu si můžeme upravit, z druhých sum nalevo vytkneme x, napravo se v první rovnici odečtou -2 a nultý člen sumy, takže můžeme vytknout x. Vznikne soustava

$$\sum_{k=0}^{\infty} a_k\,x^k - x\sum_{k=0}^{\infty} b_k\,x^k = a_0 + 2\,x\sum_{k=0}^{\infty} x^k,$$

$$\sum_{k=0}^{\infty} b_k\, x^k - x \sum_{k=0}^{\infty} a_k\, x^k = b_0.$$

Nalevo máme vytvořující funkce. V první rovnici napravo vznikne zlomek $\frac{2\,x}{1-x}$. Získáme tak soustavu

$$\begin{aligned} \mathrm{V}(a)(x) - x\ \mathrm{V}(b)(x) &= a_0 + \frac{2\,x}{1-x}, \\ \mathrm{V}(b)(x) - x\ \mathrm{V}(a)(x) &= b_0. \end{aligned}$$

Vznikne soustava dvou lineárních (funkcionálních) rovnic, tj. neznámými jsou funkce. Ke druhému řádku přičteme x-násobek prvního. Vznikne soustava

$$\begin{aligned} \mathrm{V}(a)(x) - x\ \mathrm{V}(b)(x) &= a_0 + \frac{2\,x}{1-x}, \\ (1-x^2)\ \mathrm{V}(b)(x) &= b_0 + a_0\,x + \frac{2\,x^2}{1-x}, \end{aligned}$$

kterou si můžeme přepsat do tvaru

$$\begin{aligned} \mathrm{V}(a)(x) &= a_0 + \frac{2\,x}{1-x} + x\ \mathrm{V}(b)(x) \\ \mathrm{V}(b)(x) &= \frac{b_0 + a_0\,x}{1-x^2} + \frac{2\,x^2}{(1-x)^2\,(1+x)}. \end{aligned}$$

Nyní chceme standardní metodou zjistit b_k. Máme

$$\begin{aligned} \mathrm{V}(b)(x) &= \frac{b_0 + a_0\,x}{1-x^2} + \frac{2\,x^2}{(1-x)^2\,(1+x)} \\ &= \frac{(b_0 + a_0\,x)\,(1-x) + 2\,x^2}{(1-x)^2\,(1+x)} \\ &= \frac{b_0 + (a_0 - b_0)\,x + (2-a_0)\,x^2}{(1-x)^2\,(1+x)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1+x}. \end{aligned}$$

Chceme zjistit A, B a C. Platí

$$\begin{aligned} b_0 + (a_0 - b_0)\,x + (2-a_0)\,x^2 &= A\,(1-x^2) + B\,(1+x) + C\,(1-x)^2 \\ &= (-A+C)\,x^2 + (B-2\,C)\,x + A + B + C. \end{aligned}$$

Získáme soustavu lineárních rovnic o třech neznámých, kterou řešíme schematicky Gaussovou eliminací. První rovnici si vynásobíme -1 a pak od třetí odečítáme rovnou první i druhou. Následně vynulujeme poslední sloupec.

$$\left(\begin{array}{ccc|c} 1 & 0 & -1 & a_0 - 2 \\ 0 & 1 & -2 & a_0 - b_0 \\ 1 & 1 & 1 & b_0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -1 & a_0 - 2 \\ 0 & 1 & -2 & a_0 - b_0 \\ 0 & 0 & 4 & 2\,b_0 - 2\,a_0 + 2 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & \frac{a_0+b_0-3}{2} \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & \frac{b_0-a_0+1}{2} \end{array}\right)$$

Máme pak $A = \frac{a_0+b_0-3}{2}$, $B = 1$ a $C = \frac{b_0-a_0+1}{2}$. Máme vytvořující funkci pro b

$$\mathrm{V}(b)(x) = \frac{a_0+b_0-3}{2} \cdot \frac{1}{1-x} + \frac{1}{(1-x)^2} + \frac{b_0-a_0+1}{2} \cdot \frac{1}{1+x},$$

ze které pomocí (10.3) zjistíme

$$\begin{aligned} b_k &= \frac{a_0+b_0-3}{2} + k + 1 + (-1)^k \frac{b_0-a_0+1}{2} \\ &= k + \frac{(-1)^k - 1 + \left(1+(-1)^k\right) b_0 + \left(1-(-1)^k\right) a_0}{2} \end{aligned} \tag{11.8}$$

pro $k \geq 0$. Protože

$$\mathrm{V}(a)(x) = a_0 + \frac{2\,x}{1-x} + x\ \mathrm{V}(b)(x),$$

zjistíme díky vlastnostem vytvořujících funkcí a (10.3), že $a_0 = a_0$ a

$$a_k = 2 + b_{k-1}$$

pro $k \geq 1$ (což není vůbec překvapující, ze zadávající rovnice získáme totéž vyjádření). Dosazením z (11.8) zjistíme, že

$$\begin{aligned} a_k &= 2 + k - 1 + \frac{(-1)^{k-1} - 1 + \left(1+(-1)^{k-1}\right) b_0 + \left(1-(-1)^{k-1}\right) a_0}{2} \\ &= k + \frac{1-(-1)^k + \left(1-(-1)^k\right) b_0 + \left(1+(-1)^k\right) a_0}{2} \end{aligned} \tag{11.9}$$

pro $k \geq 1$ Dosazením $k = 0$ do (11.9) získáme hodnotu

$$0 + \frac{1-1+(1-1)\,b_0 + (1+1)\,a_0}{2} = a_0$$

tedy můžeme říci, že vztah (11.9) platí pro všechna $k \geq 0$. Máme tedy explicitní předpisy pro k-té členy posloupností a i b. Pro naše konkrétní hodnoty $a_0 = 1$, $b_0 = 0$ pak vychází vztahy

$$\begin{aligned} a_k &= k + \frac{1-(-1)^k+1+(-1)^k}{2} = k+1, \\ b_k &= k + \frac{(-1)^k - 1 + 1 - (-1)^k}{2} = k. \end{aligned}$$

△

Jiné řešení. Stejným postupem získáme soustavu pro vytvořující funkce

$$\begin{aligned} \mathrm{V}(a)(x) - x\ \mathrm{V}(b)(x) &= \frac{2\,x}{1-x} + a_0 \\ \mathrm{V}(b)(x) - x\ \mathrm{V}(a)(x) &= b_0 \end{aligned}$$

což je vlastně lineární funkcionální rovnice

$$\begin{pmatrix} 1 & -x \\ -x & 1 \end{pmatrix} \cdot \begin{pmatrix} \mathrm{V}(a)(x) \\ \mathrm{V}(b)(x) \end{pmatrix} = \begin{pmatrix} \frac{2\,x}{1-x} + a_0 \\ b_0 \end{pmatrix}.$$

Determinant matice je $1 - x^2$, podle (11.4) tak máme

$$\begin{pmatrix} \mathrm{V}(a)(x) \\ \mathrm{V}(b)(x) \end{pmatrix} = \frac{1}{1-x^2} \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{2\,x}{1-x^2} + a_0 \\ b_0 \end{pmatrix} = \cdots = \begin{pmatrix} \frac{a_0 + (b_0 - a_0 + 2)\,x - b_0\,x^2}{(1-x)^2\,(1+x)} \\ \frac{b_0 + (a_0 - b_0)\,x + (2 - a_0)\,x^2}{(1-x)^2\,(1+x)}. \end{pmatrix}$$

Dále bychom postupovali standardně, až bychom dospěli k výsledku. △

Příklad 11.5. Najděte explicitní vyjádření pro k-té členy posloupností $a = \{a_k\}_{k=0}^{\infty}$ a $b = \{b_k\}_{k=0}^{\infty}$, které jsou definované vztahy

$$\begin{aligned} a_k &= b_{k-1} - b_{k-2}, \\ b_k &= a_{k-1} + b_{k-2} + a_{k-2} \end{aligned}$$

pro $k \geq 2$, $a_0 = 4$, $a_1 = 4$, $b_0 = 4$ a $b_1 = 0$.

Poznámka. Podobně jako v příkladu 11.4 bychom mohli z první rovnice vyjádřit $a_{k-1} = b_{k-2} - b_{k-3}$ a $a_{k-2} = b_{k-3} - b_{k-4}$. Pak dosazením do druhé rovnice bychom získali

$$\begin{aligned} b_k &= (b_{k-2} - b_{k-3}) + b_{k-2} + (b_{k-3} - b_{k-4}) \\ &= 2\,b_{k-2} - b_{k-4} \end{aligned}$$

pro $k \geq 4$, kde bychom museli spočítat i počáteční podmínky. Nicméně zde je již skoro jednodušší počítat rovnou.

Řešení. Nejprve si upravíme rekurence tak, aby platily pro všechna $k \geq 0$. Dosazením $a_0 = 4$ dostaneme

$$4 = \underbrace{b_{-1} + b_{-2}}_{0} + 4\,[k = 0],$$

z $a_1 = 4$ máme již platnou rovnost

$$4 = \underbrace{b_0 + b_{-1}}_{4}.$$

Dosazením $b_0 = 4$ do druhé rekurence dostaneme

$$4 = \underbrace{a_{-1} + b_{-2} + a_{-2}}_{0} + 4\,[k = 0],$$

pro $b_1 = 0$ máme

$$0 = \underbrace{a_1 + b_{-1} + a_{-1}}_{4} - 4\,[k = 1].$$

Přepíšeme tedy rekurenci na tvar platný pro všechna $k \geq 0$.

$$\begin{aligned} a_k &= b_{k-1} - b_{k-2} + 4\,[k=0] \\ b_k &= a_{k-1} + b_{k-2} + a_{k-2} + 4\,[k=0] - 4\,[k=1] \end{aligned}$$

Vynásobením x^k a sčítáním přes všechna k přejdeme k vytvořujícím funkcím.

$$\begin{aligned} \mathrm{V}(a)(x) &= x\ \mathrm{V}(b)(x) - x^2\ \mathrm{V}(b)(x) + 4 \\ \mathrm{V}(b)(x) &= x\ \mathrm{V}(a)(x) + x^2\ \mathrm{V}(b)(x) + x^2\ \mathrm{V}(a)(x) + 4 - 4\,x \end{aligned}$$

Soustavu si můžeme přepsat na tvar

$$\begin{aligned} \mathrm{V}(a)(x) - x\,(1-x)\ \mathrm{V}(b)(x) &= 4 \\ -x\,(1+x)\ \mathrm{V}(a)(x) + (1-x^2)\ \mathrm{V}(b)(x) &= 4 - 4\,x. \end{aligned}$$

V maticovém tvaru dostáváme

$$\begin{pmatrix} 1 & -x\,(1-x) \\ -x\,(1+x) & 1 \end{pmatrix} \cdot \begin{pmatrix} \mathrm{V}(a)(x) \\ \mathrm{V}(b)(x) \end{pmatrix} = \begin{pmatrix} 4 \\ 4-4\,x \end{pmatrix}.$$

Determinant matice je $1 - x^2 - x^2\,(1-x^2) = 1 - 2\,x^2 + x^4 = (1-x^2)^2$. Dále počítáme (s použitím (11.4))

$$\begin{aligned} \begin{pmatrix} \mathrm{V}(a)(x) \\ \mathrm{V}(b)(x) \end{pmatrix} &= \frac{4}{(1-x^2)^2} \cdot \begin{pmatrix} 1-x^2 & x\,(1-x) \\ x\,(1+x) & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1-x \end{pmatrix} \\ &= \frac{4}{(1-x^2)^2} \cdot \begin{pmatrix} (1-x)\,(1+2\,x-x^2) \\ 1+x^2 \end{pmatrix}. \end{aligned}$$

Máme tedy po zkrácení $\mathrm{V}\,a$ $1-x$

$$\mathrm{V}(a)(x) = \frac{4+8\,x-x^2}{(1+x)^2\,(1-x)}$$

a

$$\mathrm{V}(b)(x) = \frac{4+4\,x^2}{(1-x^2)^2}.$$

Rozložíme $\mathrm{V}\,a$ na parciální zlomky.

$$\mathrm{V}(a)(x) = \frac{4+8\,x-x^2}{(1+x)^2\,(1-x)} = \frac{A}{1+x} + \frac{B}{(1+x)^2} + \frac{C}{1-x}$$

Pak

$$4 + 8\,x - 4\,x^2 = A\,(1-x^2) + B\,(1-x) + C\,(1+x)^2,$$

dosazením $x = 1$ získáme $4 + 8 - 4 = 8 = 4\,C$, tedy $C = 2$; dosazením $x = -1$ dostaneme $4 - 8 - 4 = -8 = 2\,B$, tedy $B = -2$. Z rovnice pro absolutní člen získáme $4 = A + B + C$, tedy $A = 6$. Máme rozklad

$$\mathrm{V}(a)(x) = \frac{6}{1+x} - \frac{4}{(1+x)^2} + \frac{2}{1-x},$$

s použitím vzorce (10.3) dostaneme vyjádření a_k.

$$\begin{aligned} a_k &= 6 \cdot (-1)^k - 4\,(k+1) \cdot (-1)^k + 2 \\ &= -4\,k \cdot (-1)^k + 2\,(1 + (-1)^k) \end{aligned}$$

V b rozložíme na parciální zlomky.

$$\mathrm{V}(b)(x) = \frac{4 + 4\,x^2}{(1-x^2)^2} = \frac{A}{1+x} + \frac{B}{(1+x)^2} + \frac{C}{1-x} + \frac{D}{(1-x)^2},$$

odtud

$$4 + 4\,x^2 = A\,(1+x)\,(1-x)^2 + B\,(1-x)^2 + C\,(1+x)^2\,(1-x) + D\,(1+x)^2.$$

Dosazením $x = 1$ získáme $4 + 4 = 8 = 4\,D$, tedy $D = 2$; dosazením $x = -1$ pak $4 + 4 = = 8 = 4\,B$, tedy $B = 2$. Z rovnice pro absolutní člen získáme $A + B + C + D = 4$, tedy $A + C = 0$, z rovnice pro koeficient u x^3 pak $A - C = 0$. Dohromady $A = C = 0$. Máme tedy

$$\mathrm{V}(b)(x) = \frac{2}{(1+x)^2} + \frac{2}{(1-x)^2}.$$

Opět s použitím (10.3) dostaneme explicitní vzorec pro b_k.

$$b_k = 2\,(k+1)\,(-1)^k + 2\,(k+1) = 2\,(k+1)\,(1 + (-1)^k) \qquad \triangle$$

Příklad 11.6. Najděte explicitní vyjádření pro k-té členy posloupností $a = \{a_k\}_{k=0}^{\infty}$ a $b = \{b_k\}_{k=0}^{\infty}$, které jsou definované vztahy

$$\begin{aligned} a_k &= 3\,b_{k-1} - a_{k-1} && \text{pro } k \geq 1, \\ b_k &= 2\,a_{k-2} - 4\,b_{k-1} && \text{pro } k \geq 2, \end{aligned}$$

$a_0 = 3$, $b_0 = 2$ a $b_1 = -12$.

Řešení. Nejprve si upravíme rovnice tak, aby platily pro všechna $k \geq 0$. Máme

$$\begin{aligned} 3 = a_0 &= \underbrace{3\,b_{-1} - a_{-1}}_{0} + 3\,[k = 0], \\ 2 = b_0 &= \underbrace{2\,a_{-2} - 4\,b_{-1}}_{0} + 2\,[k = 0] \end{aligned}$$

a

$$-12 = b_1 = \underbrace{3\,a_{-1} - 4\,b_0}_{-8} - 4\,[k=1].$$

Celkem tedy dostáváme rovnice platné pro všechna $k \geq 0$.

$$\begin{aligned} a_k &= 3\,b_{k-1} - a_{k-1} + 3\,[k=0] \\ b_k &= 2\,a_{k-2} - 4\,b_{k-1} + 2\,[k=0] - 4\,[k=1] \end{aligned}$$

Vynásobením x^k a sečtením přes všechna k si přejdeme k vytvořujícím funkcím. U členů s indexem $k-1$ vytkneme x a přeznačíme, u členů s indexem $k-2$ pak vytkneme x^2 a přeznačíme.

$$\begin{aligned} \mathrm{V}(a)(x) &= 3\,x\ \mathrm{V}(b)(x) - x\ \mathrm{V}(a)(x) + 3 \\ \mathrm{V}(b)(x) &= 2\,x^2\ \mathrm{V}(a)(x) - 4\,x\ \mathrm{V}(b)(x) + 2 - 4\,x \end{aligned}$$

Členy s $\mathrm{V}\,a$, $\mathrm{V}\,b$ si dáme nalevo, čímž vznikne lineární soustava.

$$\begin{aligned} (1+x)\ \mathrm{V}(a)(x) - 3\,x\ \mathrm{V}(b)(x) &= 3 \\ -2\,x^2\,\mathrm{V}(a)(x) + (1+4\,x)\ \mathrm{V}(b)(x) &= 2 - 4\,x \end{aligned}$$

Soustavu si přepíšeme jako jednu rovnici s maticemi a vektory.

$$\begin{pmatrix} 1+x & -3\,x \\ -2\,x^2 & 1+4\,x \end{pmatrix} \cdot \begin{pmatrix} \mathrm{V}(a)(x) \\ \mathrm{V}(b)(x) \end{pmatrix} = \begin{pmatrix} 3 \\ 2-4\,x \end{pmatrix}$$

Determinant matice je $(1+x)\,(1+4\,x) - (-2\,x^2)\,(-3\,x) = 1 + 5\,x + 4\,x^2 - 6\,x^3 =: p(x)$. Pak p-násobek výsledku je díky (11.4)

$$\begin{aligned} p(x) \cdot \begin{pmatrix} \mathrm{V}(a)(x) \\ \mathrm{V}(b)(x) \end{pmatrix} &= \begin{pmatrix} 1+4\,x & 3\,x \\ 2\,x^2 & 1+x \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 2-4\,x \end{pmatrix} = \\ &= \begin{pmatrix} 3 + 12\,x + 6\,x - 12\,x^2 \\ 6\,x^2 + 2 - 2\,x - 4\,x^2 \end{pmatrix} = \begin{pmatrix} 3 + 18\,x - 12\,x^2 \\ 2 - 2\,x + 2\,x^2 \end{pmatrix} \end{aligned}$$

Máme rozklad $p(x) = (1+2\,x-2\,x^2)\,(1+3\,x)$. Dále máme si dosadíme $x = \frac{1}{t}$ do polynomu $1 + 2\,x - 2\,x^2$ a vynásobíme t^2, následně hledáme kořeny polynomu $t^2 + 2\,t - 2$ pomocí diskriminantu

$$t_{1,2} = \frac{-2 \pm \sqrt{4 - 4 \cdot (-2)}}{2} = -1 \pm \sqrt{3}.$$

To nám dává rozklad $1+2\,x-2\,x^2 = (1-t_1\,x)\,(1-t_2\,x) = \left(1 + \left(1+\sqrt{3}\right)\,x\right)\,\left(1 + \left(1-\sqrt{3}\right)\,x\right)$. Máme tedy vyjádření

$$\mathrm{V}(a)(x) = \frac{3 + 18\,x - 12\,x^2}{\left(1+3\,x\right)\,\left(1 + \left(1+\sqrt{3}\right)\,x\right)\,\left(1 + \left(1-\sqrt{3}\right)\,x\right)},$$

$$\mathrm{V}(b)(x) = \frac{2 - 2\,x + 2\,x^2}{\left(1 + 3\,x\right)\,\left(1 + \left(1 + \sqrt{3}\right)\,x\right)\,\left(1 + \left(1 - \sqrt{3}\right)\,x\right)}.$$

Vidíme, že v obou případech je jmenovatel stejný, navíc má polynom p při různé kořeny. Chceme rozložit $\mathrm{V}\,a$ na parciální zlomky. Máme

$$\mathrm{V}(a)(x) = \frac{A}{1 + \left(1 + \sqrt{3}\right)\,x} + \frac{B}{1 + \left(1 - \sqrt{3}\right)\,x} + \frac{C}{1 + 3\,x}. \tag{11.10}$$

Vynásobením polynomem p získáme rovnici

$$\begin{aligned} 3 + 18\,x - 12\,x^2 = {} & A\,\left(1 + \left(1 - \sqrt{3}\right)\,x\right)\,\left(1 + 3\,x\right) + \\ & + B\,\left(1 + \left(1 + \sqrt{3}\right)\,x\right)\,\left(1 + 3\,x\right) + \\ & + C\,\left(1 + 2\,x - 2\,x^2\right). \end{aligned}$$

Schematicky $L = P$. Dosazením $x = -\frac{1}{3}$ máme

$$\begin{aligned} L_{-\frac{1}{3}} &= 3 + 18\,\left(-\frac{1}{3}\right) - 12\,\left(\frac{1}{9}\right) = \frac{27 - 54 - 12}{9} = -\frac{39}{9}, \\ P_{-\frac{1}{3}} &= \left[1 + 2\,\left(-\frac{1}{3}\right) - 2\,\left(\frac{1}{9}\right)\right]\,C = \frac{9 + 6 - 2}{9}\,C = \frac{C}{9}, \end{aligned}$$

odtud $C = -39$. Chceme dosadit $x = -\frac{1}{1+\sqrt{3}}$. Máme

$$-\frac{1}{1 + \sqrt{3}} = -\frac{1}{1 + \sqrt{3}} \cdot \frac{1 - \sqrt{3}}{1 - \sqrt{3}} = -\frac{1 - \sqrt{3}}{1 - 3} = \frac{1 - \sqrt{3}}{2} = x,$$

dále $\left(1 + \sqrt{3}\right)^2 = 4 + 2\,\sqrt{3}$ a

$$\frac{1}{4 + 2\,\sqrt{3}} = \frac{1}{4 + 2\,\sqrt{3}} \cdot \frac{4 - 2\,\sqrt{3}}{4 - 2\,\sqrt{3}} = \frac{4 - 2\,\sqrt{3}}{16 - 12} = \frac{2 - \sqrt{3}}{2} = x^2.$$

Pak dosazením dostaneme

$$\begin{aligned} L_{\frac{1-\sqrt{3}}{2}} &= 3 + 18\,\frac{1 - \sqrt{3}}{2} - 12\,\frac{2 - \sqrt{3}}{2} = 3 + 9\,\left(1 - \sqrt{3}\right) - 6\,\left(2 - \sqrt{3}\right) = -3\,\sqrt{3}, \\ P_{\frac{1-\sqrt{3}}{2}} &= \left(1 + \frac{\left(1 - \sqrt{3}\right)^2}{2}\right)\,\left(1 + 3\,\frac{1 - \sqrt{3}}{2}\right)\,A \\ &= \frac{2 + 4 - 2\,\sqrt{3}}{2} \cdot \frac{2 + 3 - 3\,\sqrt{3}}{2}\,A = \frac{\left(6 - 2\,\sqrt{3}\right)\,\left(5 - 3\,\sqrt{3}\right)}{4}\,A \end{aligned}$$

$$= \frac{30 - 10\sqrt{3} - 18\sqrt{3} + 18}{4} A = \left(12 - 7\sqrt{3}\right) A.$$

Odtud

$$A = \frac{-3\sqrt{3}}{12 - 7\sqrt{3}} = \frac{-3\sqrt{3}\left(12 + 7\sqrt{3}\right)}{144 - 49 \cdot 3} = \frac{-3\left(21 + 12\sqrt{3}\right)}{-3} = 21 + 12\sqrt{3}.$$

Chceme dosadit $x = -\frac{1}{1-\sqrt{3}}$. Podobně jako dříve máme

$$-\frac{1}{1-\sqrt{3}} \cdot \frac{1+\sqrt{3}}{1+\sqrt{3}} = -\frac{1+\sqrt{3}}{1-3} = \frac{1+\sqrt{3}}{2} = x$$

a

$$x^2 = \frac{4 + 2\sqrt{3}}{4} = \frac{2+\sqrt{3}}{2}.$$

Dosazením do (11.10) dostaneme

$$\begin{aligned}
L_{\frac{1+\sqrt{3}}{2}} &= 3 + 18\,\frac{1+\sqrt{3}}{2} - 12\,\frac{2+\sqrt{3}}{2} = 3 + 9\left(1+\sqrt{3}\right) - 6\left(2+\sqrt{3}\right) = 3\sqrt{3}, \\
P_{\frac{1+\sqrt{3}}{2}} &= \left(1 + \frac{\left(1+\sqrt{3}\right)^2}{2}\right)\left(1 + 3\,\frac{1+\sqrt{3}}{2}\right) B \\
&= \frac{2+4+2\sqrt{3}}{2} \cdot \frac{2+3+3\sqrt{3}}{2} B = \frac{\left(6+2\sqrt{3}\right)\left(5+3\sqrt{3}\right)}{4} B \\
&= \frac{30 + 10\sqrt{3} + 18\sqrt{3} + 18}{4} B = \left(12 + 7\sqrt{3}\right) B,
\end{aligned}$$

odtud

$$B = \frac{3\sqrt{3}}{12 + 7\sqrt{3}} = \frac{3\sqrt{3}\left(12 - 7\sqrt{3}\right)}{144 - 49 \cdot 3} = \sqrt{3}\left(7\sqrt{3} - 12\right) = 21 - 12\sqrt{3}.$$

Máme tedy

$$\mathrm{V}(a)(x) = \frac{21 + 12\sqrt{3}}{1 + \left(1+\sqrt{3}\right) x} + \frac{21 - 12\sqrt{3}}{1 + \left(1-\sqrt{3}\right) x} - \frac{39}{1 + 3x},$$

odkud s pomocí (10.3) dostaneme vzorec pro k-tý člen posloupnosti a.

$$a_k = (-1)^k \cdot \left[\left(21 + 12\sqrt{3}\right) \cdot \left(1+\sqrt{3}\right)^k + \left(21 - 12\sqrt{3}\right) \cdot \left(1-\sqrt{3}\right)^k - 39 \cdot 3^k\right]$$

Chceme najít rozklad $\mathrm{V}\,b$ na parciální zlomky. Máme

$$\mathrm{V}(b)(x) = \frac{2 - 2x + 2x^2}{\left(1+3x\right)\left(1 + \left(1+\sqrt{3}\right) x\right)\left(1 + \left(1-\sqrt{3}\right) x\right)}$$

$$= \frac{A}{1+\left(1+\sqrt{3}\right)x} + \frac{B}{1+\left(1-\sqrt{3}\right)x} + \frac{C}{1+3x}.$$

Vynásobením polynomem p dostaneme rovnici

$$\begin{aligned} 2-2x+2x^2 = A\left(1+\left(1-\sqrt{3}\right)x\right)\left(1+3x\right) + \\ + B\left(1+\left(1+\sqrt{3}\right)x\right)\left(1+3x\right) + \\ + C\left(1+2x-2x^2\right), \end{aligned}$$

schematicky $L = P$. Dosazováním chceme zjistit A, B, C. Vidíme, že pravá strana rovnice je stejná jako pravá strana rovnice pro $\mathrm{V}\,a$. Bude tedy

$$\begin{aligned} P_{-\frac{1}{3}} &= \frac{C}{9}, \\ P_{\frac{1-\sqrt{3}}{2}} &= \left(12-7\sqrt{3}\right)A, \\ P_{\frac{1+\sqrt{3}}{2}} &= \left(12+7\sqrt{3}\right)B. \end{aligned}$$

Stačí spočítat hodnoty levé strany rovnice.

$$\begin{aligned} L_{-\frac{1}{3}} &= 2+\frac{2}{3}+\frac{2}{9} = \frac{18+6+2}{2} = \frac{26}{9} \\ L_{\frac{1-\sqrt{3}}{2}} &= 2-2\,\frac{1-\sqrt{3}}{2}+2\,\frac{2-\sqrt{3}}{2} = 2-\left(1-\sqrt{3}\right)+2-\sqrt{3} = 3 \\ L_{\frac{1+\sqrt{3}}{2}} &= 2-2\,\frac{1+\sqrt{3}}{2}+2\,\frac{2+\sqrt{3}}{2} = 2-\left(1+\sqrt{3}\right)+2+\sqrt{3} = 3 \end{aligned}$$

Máme tak rovnou

$$\begin{aligned} A &= \frac{3}{12-7\sqrt{3}} = \frac{3\left(12+7\sqrt{3}\right)}{-3} = -12-7\sqrt{3}, \\ B &= \frac{3}{12+7\sqrt{3}} = \frac{3\left(12-7\sqrt{3}\right)}{-3} = -12+7\sqrt{3}, \\ C &= 26. \end{aligned}$$

Pak

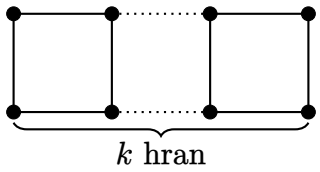
$$\mathrm{V}(b)(x) = -\frac{12+7\sqrt{3}}{1+\left(1+\sqrt{3}\right)x} - \frac{12-7\sqrt{3}}{1+\left(1-\sqrt{3}\right)x} + \frac{26}{1+3x},$$

odkud opět s použitím (10.3) dostaneme vzorec pro k-tý člen posloupnosti b.

$$b_k = (-1)^k \cdot \left[26\cdot 3^k - \left(12+7\sqrt{3}\right)\cdot\left(1+\sqrt{3}\right)^k - \left(12-7\sqrt{3}\right)\cdot\left(1-\sqrt{3}\right)^k\right]$$

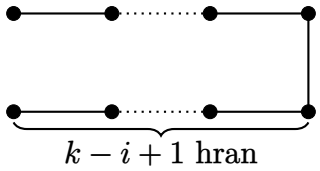
Zajímavostí je, že ze zadávajících rovnic rekurencí plyne, že a_k, $b_k \in \mathbb{Z}$ i přes to, že se ve vzorcích pro k-tý člen obou posloupností vyskytují iracionální čísla. △

Příklad 11.7. Uvažme graf G_k zadaný obrázkem.



Označme a_k počet jeho koster. Odvoďte rekurentní formuli pro a_k. Určete vytvořující funkci posloupnosti a a vzorec pro k-tý člen.

Řešení. Podíváme se na poslední „čtverec“. Pokud se některá ze tří „vnějších“ hran v dané kostře nenachází, jedná se o kostru G_{k-1}. Pokud zde máme všechny tři hrany, najdeme nejdelší graf tvaru



pro každý z nichž máme dvě možnosti, jak jej připojit ke kostře grafu G_i. Nakonec máme jednu kostru pro případ, že daná „vidlice“ je sama kostrou grafu G_k. Pak

$$a_k = 3\,a_{k-1} + 2\,a_{k-2} + 2\,a_{k-3} + \cdots + 2\,a_0 + 1$$

je rekurentní zadání posloupnosti a_k. Označíme-li $s_k = \sum_{n=0}^{k} a_k$ posloupnost částečných součtů, máme

$$a_k = a_{k-1} + 2\,s_{k-1} + 1. \tag{11.11}$$

Index se snižuje maximálně o 1, proto si musíme upravit (11.11) tak, aby platila pro všechna k. Dosazením $k = 0$ máme

$$1 = a_0 = \underbrace{a_{-1} + 2\,s_{-1}}_{0} + 1,$$

tedy nemusíme nic přidávat. Vynásobením x^k a sčítáním přejdeme k vytvořujícím funkcím

$$\mathrm{V}(a)(x) = x\ \mathrm{V}(a)(x) + 2\,x\ \mathrm{V}(s)(x) + \frac{1}{1-x},$$

odkud s využitím (10.2) získáme

$$\mathrm{V}(a)(x) = x\ \mathrm{V}(a)(x) + \frac{2\,x}{1-x}\ \mathrm{V}(a)(x) + \frac{1}{1-x},$$

z čehož po vynásobení $1-x$ máme

$$(1-x)\ \mathrm{V}(a)(x) = (x-x^2)\ \mathrm{V}(a)(x) + 2\,x\ \mathrm{V}(a)(x) + 1$$

a po úpravě

$$\mathrm{V}(a)(x) = \frac{1}{1 - 4\,x + x^2}. \tag{11.12}$$

Odtud bychom také mohli získat zjednodušenou rekurenci, z

$$\mathrm{V}(a)(x) = 4\,x\ \mathrm{V}(a)(x) - x^2\ \mathrm{V}(a)(x) + 1$$

bychom dostali

$$a_k = 4\,a_{k-1} - a_{k-2} + [k = 0]. \tag{11.13}$$

Existuje ale i způsob, jak získat (11.13) přímo z (11.11) bez vytvořujících funkcí. Jelikož $a_{k-1} = s_{k-1} - s_{k-2}$ máme pro rozdíl dvou po sobě jdoucích členů z (11.13)

$$\begin{aligned} a_k - a_{k-1} &= a_{k-1} + 2\,s_{k-1} + 1 - (a_{k-2} + 2\,s_{k-2} + 1) \\ &= a_{k-1} + 2\,(s_{k-1} - s_{k-2}) - a_{k-2} = 3\,a_{k-1} - a_{k-2} \end{aligned}$$

neboli

$$a_k = 4\,a_{k-1} - a_{k-2}$$

pro $k \geq 2$ (jelikož používáme index snižujeme nejvýše o 2). Počáteční podmínky jsou $a_0 = 1$ (G_0 je svojí jedinou kostrou) a $a_1 = 4$ (jednu hranu čtverce vynecháme). Pro zjištění vytvořující funkce bychom upravili rekurenci tak, aby platila pro $k \geq 0$. Dosazením $k = 0$ získáme

$$1 = a_0 = \underbrace{4\,a_{-1} - a_{-2}}_{0} + [k = 0],$$

po dosazení $k = 1$ získáme již platnou rovnost

$$4 = a_1 = \underbrace{4\,a_0 - a_{-1}}_{4}.$$

Tím získáme (11.13). Vytvořující funkci bychom mohli získat také klasicky z (11.13). My ji však již máme vypočtenou v (11.12), chceme ji pro získání vzorce pro k-tý člen rozložit na parciální zlomky. Protože polynom $x^2 - 4\,x + 1$ je symetrický vzhledem ke zobrazení $x \mapsto \frac{1}{x}$, budou koeficienty u x právě kořeny onoho polynomu. Máme

$$x_{1,2} = \frac{4 \pm \sqrt{16 - 4}}{2} = \frac{4 \pm 2\sqrt{3}}{2} = 2 \pm \sqrt{3},$$

takže $1 - 4\,x + x^2 = \left(1 - \left(2 + \sqrt{3}\right)\,x\right)\,\left(1 - \left(2 - \sqrt{3}\right)\,x\right)$. Je vidět, že oba kořeny jsou si navzájem inverzní. Máme pak

$$\mathrm{V}(a)(x) = \frac{1}{1 - 4\,x + x^2} = \frac{A}{1 - \left(2 + \sqrt{3}\right)\,x} + \frac{B}{1 - \left(2 - \sqrt{3}\right)\,x},$$

neboli po vynásobení $1 - 4\,x + x^2$

$$1 = B\,\left(1 - \left(2 + \sqrt{3}\right)\,x\right) + A\,\left(1 - \left(2 - \sqrt{3}\right)\,x\right).$$

Dosazením $x = 2 + \sqrt{3}$ získáme

$$1 = B\,\left(1 - \left(2 + \sqrt{3}\right)^2\right) = B\,\left(1 - 4 - 4\sqrt{3} - 3\right) = B\,\left(-6 - 4\sqrt{3}\right)$$

neboli

$$B = \frac{1}{-6 - 4\sqrt{3}} = \frac{-6 + 4\sqrt{3}}{-12} = \frac{3 - 2\sqrt{3}}{6}.$$

Podobně dosazením $x = 2 - \sqrt{3}$ získáme

$$1 = A\,\left(1 - \left(2 - \sqrt{3}\right)^2\right) = B\,\left(1 - 4 + 4\sqrt{3} - 3\right) = B\,\left(-6 + 4\sqrt{3}\right)$$

odtudi

$$A = \frac{1}{-6 + 4\sqrt{3}} = \frac{-6 - 4\sqrt{3}}{-12} = \frac{3 + 2\sqrt{3}}{6}.$$

Pak

$$\mathrm{V}(a)(x) = \frac{3 + 2\sqrt{3}}{6} \cdot \frac{1}{1 - \left(2 + \sqrt{3}\right)\,x} + \frac{3 - 2\sqrt{3}}{6} \cdot \frac{1}{1 - \left(2 - \sqrt{3}\right)\,x},$$

odkud vidíme s použitím (10.3) vzorec pro k-tý člen.

$$a_k = \frac{3 + 2\sqrt{3}}{6} \cdot \left(2 + \sqrt{3}\right)^k + \frac{3 - 2\sqrt{3}}{6} \cdot \left(2 - \sqrt{3}\right)^k$$

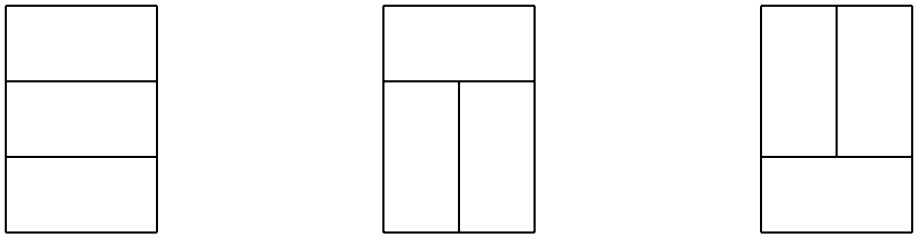
Opět (podobně jako v příkladech 10.6 a 11.6) ve vzorci vystupují iracionální čísla, přesto je výsledek celočíselný. △

Příklad 11.8. Označme a_k počet pokrytí (nerozlišenými) kostkami domina obdélníku o rozměrech $2\,k \times 3$. Určete vytvořující funkci a vzorec pro k-tý člen posloupnosti a.

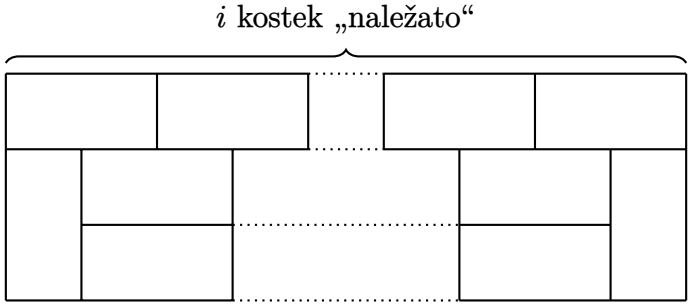
Řešení. Jdeme zprava dokud nenarazíme na svislou čáru. To nastane buď po jednom kroku, kde máme na výběr tří možnosti, viz obrázek 11.1, nebo po více krocích, kde musí nastat buď situace na obrázku 11.2, nebo situace vertikálně „překlopená“. Pro každou z těchto možností pak máme a_{k-i} pokrytí zbylého obdélníku nalevo.

Pro počet pokrytí tedy platí

$$a_k = 3\,a_{k-1} + 2\,a_{k-2} + \cdots + 2\,a_1 + 2$$



Obrázek 11.1: Tři pokrytí obdélníku 2×3.



Obrázek 11.2: Možné pokrytí obdélníku $(2\,i) \times 3$.

kde poslední dvojka je pro případ, kdy jsme pokryli již celý obdélník jako na obrázku 11.2. Vzhledem k tomu, že pro $k = 0$ máme prázdný obdélník a jediné (prázdné) pokrytí, lze vztah interpretovat jako

$$\begin{aligned} a_k &= 3\,a_{k-1} + 2\,a_{k-2} + \cdots + 2\,a_0 \\ &= a_{k-1} + 2\,a_{k-1} + 2\,a_{k-2} + \cdots + 2\,a_0. \end{aligned}$$

Označíme-li $s_k := \sum_{i=0}^{k} a_i$ posloupnost částečných součtů, máme vztah

$$a_k = a_{k-1} + 2\,s_{k-1}.$$

Všimněte si, že se nápadně podobá vztahu v příkladu 11.7. Již odtud bychom mohli přejít k vytvořujícím funkcím pomocí (10.2), raději si však rekurenci upravíme, což zjednoduší výpočet vytvořující funkce. Pomocí vyjádření $a_{k-1} = s_{k-1} - s_{k-2}$ máme po odečtení vztahu pro a_k a pro a_{k-1}

$$\begin{aligned} a_k - a_{k-1} &= a_{k-1} + 2\,s_{k-1} - a_{k-2} - 2\,s_{k-2} \\ &= a_{k-1} - a_{k-2} + 2\,\underbrace{(s_{k-1} - s_{k-2})}_{a_{k-1}} \\ &= 3\,a_{k-1} - a_{k-2}. \end{aligned}$$

Přičtením a_{k-1} dostaneme konečně vztah

$$a_k = 4\,a_{k-1} - a_{k-2}, \tag{11.14}$$

který platí pro $k \geq 2$ (index snižujeme maximálně o 2). Dále máme 1 prázdné pokrytí obdélníku 0×3, tj. $a_0 = 1$, a 3 pokrytí obdélníku 2×3 (viz obrázek 11.1), tj. $a_1 = 3$. Všimněme si, že rekurentní vztah je stejný jako v příkladu 11.7, ovšem s jinými počátečními podmínkami. Obdélníky záporné šířky moc nedávají smysl, pro pořádek klademe ale členy a se zápornými indexy rovny 0. Dosazením $k = 0$ do rekurentního vzorce dostaneme

$$1 = a_0 = \underbrace{4\,a_{-1} - a_{-2}}_{0} + 1,$$

dosazením $k = 1$ pak

$$3 = a_1 = \underbrace{4\,a_0 - a_{-1}}_{4} - 1.$$

Odtud dostaneme vztah

$$a_k = 4\,a_{k-1} - a_{k-2} + [k = 0] - [k = 1],$$

platný pro všechna $k \geq 0$, takže můžeme vynásobením x^k a sečtením přes všechna k přejít k vytvořujícím funkcím, přičemž ze sum napravo vytkneme x, respektive x^2 a přeindexujeme, čímž dostaneme

$$\mathrm{V}(a)(x) = 4\,x\ \mathrm{V}(a)(x) - x^2\ \mathrm{V}(a)(x) + 1 - x.$$

Členy s $\mathrm{V}\,a$ si dáme nalevo a vytkneme, následně podělíme polynomem, který u $\mathrm{V}\,a$ vznikne.

$$\begin{aligned}\mathrm{V}(a)(x) &= \frac{1-x}{1-4\,x+x^2} = \frac{1-x}{\left(1-\left(2+\sqrt{3}\right)\,x\right)\left(1-\left(2-\sqrt{3}\right)\,x\right)} \\ &= \frac{A}{1-\left(2+\sqrt{3}\right)\,x} + \frac{B}{1-\left(2-\sqrt{3}\right)\,x} \qquad (11.15)\end{aligned}$$

Při rozkladu si vzpomeneme na příklad 11.7, jmenovatel je stejný. Platí tak

$$\left(2+\sqrt{3}\right)\,\left(2-\sqrt{3}\right) = 1, \qquad (11.16)$$

$$\begin{aligned}1-\left(2\pm\sqrt{3}\right)^2 &= 1-\left(7\pm 4\sqrt{3}\right) \\ &= -6\mp 4\sqrt{3}. \qquad (11.17)\end{aligned}$$

Vynásobením (11.15) polynomem $1 - 4\,x + x^2$ dostaneme

$$1 - x = A\left(1-\left(2-\sqrt{3}\right)\,x\right) + B\left(1-\left(2+\sqrt{3}\right)\,x\right)$$

odkud po dosazení $x = 2 + \sqrt{3}$ díky (11.16) a (11.17) dostaneme

$$1 - 2 - \sqrt{3} = B\,\left(-6-4\sqrt{3}\right)$$

neboli

$$\begin{aligned} B &= \frac{-1-\sqrt{3}}{-6-4\sqrt{3}} = \frac{1+\sqrt{3}}{6+4\sqrt{3}} = \frac{\left(1+\sqrt{3}\right)\left(6-4\sqrt{3}\right)}{-12} \\ &= \frac{-6+2\sqrt{3}}{-12} = \frac{3-\sqrt{3}}{6}. \end{aligned}$$

Podobně dosazením $x = 2-\sqrt{3}$ opět díky (11.16) a (11.17) dostaneme

$$1-2+\sqrt{3} = A\left(-6+4\sqrt{3}\right)$$

a odtud

$$A = \frac{\sqrt{3}-1}{4\sqrt{3}-6} = \frac{\left(\sqrt{3}-1\right)\left(4\sqrt{3}+6\right)}{12} = \frac{6+2\sqrt{3}}{1}2 = \frac{3+\sqrt{3}}{6}.$$

Pak máme rozklad vytvořující funkce

$$\begin{aligned} \mathrm{V}(a)(x) &= \frac{1-x}{1-4\,x+x^2} \\ &= \frac{3+\sqrt{3}}{6}\cdot\frac{1}{1-\left(2+\sqrt{3}\right)x} + \frac{3-\sqrt{3}}{6}\cdot\frac{1}{1-\left(2-\sqrt{3}\right)x} \end{aligned}$$

a odtud vzorec pro k-tý člen posloupnosti a.

$$a_k = \frac{3+\sqrt{3}}{6}\cdot\left(2+\sqrt{3}\right)^k + \frac{3-\sqrt{3}}{6}\cdot\left(2-\sqrt{3}\right)^k \qquad \triangle$$

11.3 Příklady k procvičení

Příklad 11.9. Pomocí vytvořující funkce vyřešte následující rekurenci:

$$a_k = 4\,a_{k-1} - 3\,a_{k-2} - 2$$

pro $k \geq 2$, $a_0 = 1$, $a_1 = 6$. (Výsledek: vytvořující funkce $\mathrm{V}(a)(x) = \frac{-4\,x^2+x+1}{(1-3\,x)\,(1-x)^2} = \frac{2}{1-3\,x} - \frac{2}{1-x} + \frac{1}{(1-x)^2}$, vzorec pro k-tý člen je $a_k = 2\cdot 3^k + k - 1$.)

Příklad 11.10. Najděte expicitní vyjádření pro k-tý člen posloupností $a = \{a_k\}_{k=0}^{\infty}$ a $b = \{b_k\}_{k=0}^{\infty}$, které jsou definované vztahy

$$\begin{aligned} a_k &= 3\,a_{k-1} + b_{k-1} \\ b_k &= a_{k-1} + 3\,b_{k-1} \end{aligned}$$

pro $k \geq 1$, $a_0 = 0$, $b_0 = 2$. (Výsledek: $a_k = 4^k - 2^k$, $b_k = 4^k + 2^k$.)

Příklad 11.11. Najděte expicitní vyjádření pro k-tý člen posloupností $a = \{a_k\}_{k=0}^{\infty}$ a $b = \{b_k\}_{k=0}^{\infty}$, které jsou definované vztahy

$$\begin{aligned} a_k &= 3\,a_{k-1} + 4\,b_{k-1} - 4\,a_{k-2} \\ b_k &= 2\,a_{k-1} - 4\,b_{k-1} - 4\,b_{k-2} \end{aligned}$$

pro $k \geq 2$, $a_0 = 1$, $a_1 = -2$, $b_0 = -\frac{17}{4}$, $b_1 = 4$, přičemž je doporučeno počítat celou dobu s neurčitými koeficienty a určit je teprve na konci. (Výsledek: rozklad jmenovatele vytvořujících funkcí je $(1+x)\,(1-2\,x)^2\,(1+4\,x)$, načež vyjde $a_k = (k-1)\,2^k + 2\,(-1)^k$ a $b_k = \frac{1}{4}\,(k-1)\,2^k - 4\,(-1)^k$.)