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 $\operatorname{nsd}(a, b)$, $\gcd(a, b)$ 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

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

△

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

[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] Podle `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 $(F_n, F_{2\,n}) = F_n$. $\triangle$