1 Naši noví kamarádi: Eukleidés a Bézout

Řešení
Verze ze dne 17. února 2025

Cíle cvičení: Důkladně si procvičíme Eukleidův algoritmus nad celými čísly, zejména si uvědomíme, že s jeho pomocí umíme počítat inverzní prvky v konečných tělesech a také některé kongruence.

Algorithm 1 Rozšířený Eukleidův algoritmus

Require: $a, b \in \mathbb{Z}$, $a \geq b > 0$
Ensure: $d = \mathrm{NSD}(a, b)$, koeficienty u, v takové, že $d = ua + vb$ (tj. Bézoutovy)

```
a_0 ← a, a_1 ← b
u_0 ← 1, v_0 ← 0
u_1 ← 0, v_1 ← 1
i ← 1
while a_i ≠ 0 do
    q ← a_{i−1} div a_i                ▷ Celočíselný podíl, též ⌊a_{i−1}/a_i⌋
    (a_{i+1}, u_{i+1}, v_{i+1}) ← (a_{i−1}, u_{i−1}, v_{i−1}) − q · (a_i, u_i, v_i)
    i ← i + 1
return (a_{i−1}, u_{i−1}, v_{i−1})
```

Úlohy, které bychom určitě měli umět řešit:

Úloha 1.1. Najděte $\mathrm{NSD}(37, 10)$ a příslušné Bézoutovy koeficienty. Spočítejte 10^{-1} v tělese $\mathbb{Z}_{37}$.

Řešení. Nejprve použijeme Eukleidův algoritmus na vstup 37 a 10, v prvním sloupci tabulky uvádíme zbytky a v druhém a třetím sloupci mezivýsledky pro výpočet Bézoutových koeficientů:

a_i	u_i	v_i
37	1	0
10	0	1
7	1	-3
3	-1	4
1	3	-11
0		

Zjistili jsme, že $1 = 3 \cdot 37 - 11 \cdot 10$. Odtud vidíme, že -11 je řešením kongruence

$$10x \equiv 1 \pmod{37},$$

V tělese $\mathbb{Z}_{37}$, kde počítáme modulo 37, tedy platí $10^{-1} = -11 = 26$.

Úloha 1.2. Najděte $\mathrm{NSD}(1023, 96)$ a příslušné Bézoutovy koeficienty.

Řešení. Stejným postupem jako v 1.1 spočítáme, že $\mathrm{NSD}(1023, 96) = 3 = (-3) \cdot 1023 + 32 \cdot 96$.

Úloha 1.3. Najděte nějaké celočíselné řešení rovnice $1023x + 96y = 18$.

Řešení. Stačí nám přenásobit Bézoutovu rovnost z $3 = (-3) \cdot 1023 + 32 \cdot 96$ hodnotou $6 = \frac{18}{3}$, abychom dostali řešení $19 = (-18) \cdot 1023 + 192 \cdot 96$.

Úloha 1.4. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$.

Řešení. Stejně jako v 1.1 použijeme Eukleidův algoritmus

a_i	u_i	v_i
41	1	0
27	0	1
14	1	-1
13	-1	2
1	2	-3
0		

Protože $1 = 2 \cdot 41 - 3 \cdot 27$, dostáváme, že $27^{-1} = -3 = 38$ v tělese $\mathbb{Z}_{41}$.

Připomeňme si, že je-li $n \in \mathbb{N}$, pak pro celá čísla a, b definujeme $a \equiv b \pmod{n}$ právě tehdy, když $n \mid (a-b)$. Pro $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$ platí $a \square c \equiv b \square d \pmod{m}$, kde $\square$ je některá z operací $+, -, \cdot$ a dokonce $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{mc}$, což je ekvivalentní $ac \equiv bc \pmod{m}$ za předpokladu, že c a m jsou nesoudělná.

Úloha 1.5. Vyřešte v celých číslech následující kongruence:

(a) $x \equiv 2 \pmod{8}$,

(b) $3x \equiv 2 \pmod{5}$,

(c) $27x \equiv 16 \pmod{41}$,

(d) $6x \equiv 2 \pmod{8}$ (pozor na změnu modulu, když „dělíme dvojkou“),

Řešení. (a) Notace znamená, že hledáme všechna taková x, že $(x) \bmod 8 = 2$, proto můžeme přímo napsat obecné řešení $x = 2 + 8k$ pro libovolné $k \in \mathbb{Z}$.

(b) Přenásobíme-li kongruenci $3x \equiv 2 \pmod{5}$ hodnotou $2 \equiv 3^{-1} \pmod{5}$, dostaneme

$$x \equiv 2 \cdot 3x \equiv 2 \cdot 2 \equiv 4 \pmod{5}$$

Nyní úvahou z (a) dostáváme obecné řešení tvaru $x = 4 + 5k$ pro $k \in \mathbb{Z}$.

(c) Postupujeme jako výše a využijeme kongruenci $27^{-1} \equiv 38 \equiv -3 \pmod{41}$ spočtenou v úloze 1.4. Obdobnou úvahou jako v (b) dostaneme

$$x \equiv 38 \cdot 27x \equiv 16 \equiv (-3) \cdot 16 \equiv -7 \equiv 34 \pmod{41},$$

a proto $x = 34 + 41k$ pro $k \in \mathbb{Z}$.

(d) Nejprve kongruenci ekvivalentně upravíme na $3x \equiv 1 \pmod{4}$, odkud předchozím postupem snadno obdržíme obecné řešení $x = 3 + 4k$ pro $k \in \mathbb{Z}$.

Úloha 1.6. Ukažte, že $n^2 \equiv 1 \pmod{8}$ pro každé liché $n \in \mathbb{N}$.

Řešení. Je-li $n = 2k + 1$ pro $k \in \mathbb{N}$, pak

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 \equiv 1 \pmod{8},$$

protože součin $k(k+1)$ je sudý.

A teď něco pro zábavu a rozšíření obzorů:

Úloha 1.7. Najděte $\mathrm{NSD}(89, 55)$ a příslušné Bézoutovy koeficienty. Jak se na výpočtu a výsledku projeví, že jedná o dva po sobě jdoucí členy Fibonacciho posloupnosti?

Řešení. Eukleidův algoritmus nám dá $1 = (-21) \cdot 89 + 34 \cdot 55$, všimneme si, že v jeho průběhu jsou všechny hodnoty $q_i = 1$, poslední dvě nenulové hodnoty a_i jsou 2 a 1, proto jsou Bézoutovy koeficienty až na znaménko rovněž po sobě jdoucí členy Fibonacciho posloupnosti.

Úloha 1.8. Spočtěte $\mathrm{NSD}(2^{92} - 1, 2^{31} - 1)$ a příslušné Bézoutovy koeficienty.

Řešení. Dělení se zbytkem je u našich čísel snadné, použijeme tedy standardně Eukleidův algoritmus

a_i	u_i	v_i
$2^{92} - 1$	1	0
$2^{31} - 1$	0	1
$2^{30} - 1$	1	$-2^{61} - 2^{30}$
1	-2	$2^{62} + 2^{31} + 1$
0		

a dostáváme $1 = (-2) \cdot (2^{92} - 1) + (2^{62} + 2^{31} + 1) \cdot (2^{31} - 1)$.

Úloha 1.9. Spočtěte $\mathrm{NSD}(2k + 1, 3k + 1)$ a příslušné Bézoutovy koeficienty v závislosti na $k \in \mathbb{N}$.

Řešení. Postupujeme opět standardně Eukleidovým algoritmem:

a_i	u_i	v_i
$3k + 1$	1	0
$2k + 1$	0	1
k	1	-1
1	-2	3
0		

a tedy $1 = (-2) \cdot (3k + 1) + 3 \cdot (2k + 1)$.

Úloha 1.10. Spočtěte největšího společného dělitele polynomů $p = x^4 - x^3 - 4x^2 - x + 1$ a $q = x^4 - 4x^3 + 5x^2 - 4x + 1$ s reálnými koeficienty. (Pro tuto úlohu sice ještě nemáme dostatečné „teoretické zázemí“, ale možná by šlo použít podobné postupy jako pro celá čísla?)

Řešení. Provedeme analogii Eukleidova algoritmu s pomocí dělení se zbytkem. Polynom $p \bmod q$ je roven $r = 3x^3 - 9x^2 + 3x$. Při dalším dělení si můžeme uvědomit, že zbytek po dělení polynomem $3x^3 - 9x^2 + 3x$ bude stejný, jako zbytek po dělení polynomem $x^3 - 3x^2 + x$, čímž si můžeme trochu usnadnit práci (pokud by se po nás chtěly i Bézoutovy koeficienty, tak bychom to ale museli zohlednit) a získat tak další polynom $s = q \bmod r = x^2 - 3x + 1$, který je zjevně dělitelem r, a je tedy hledaným NSD.

Úloha 1.11. Určete zbytky po dělení (bez pomoci Eulerovy věty, pokud víte, co to je): (a) $33^{10} \bmod 10$, (b) $7^{777} \bmod 9$.

Řešení. (a) $33^{10} \equiv 3^{10} = 9^5 \equiv (-1)^5 = -1 \equiv 9 \pmod{10}$

(b) $7^{777} \equiv (-2)^{777} = (-8)^{777/3} \equiv 1^{777/3} = 1 \pmod 9$

Úloha 1.12. Je možné uvažovat inverzní prvek a^{-1} také modulo m, které není prvočíslo? Co třeba 29^{-1} nebo 33^{-1} v okruhu $\mathbb{Z}_{39}$? Jak to souvisí s (ne)soudělností?

Řešení. Protože jsou $\mathrm{NSD}(29, 39) = 1$, obvyklým způsobem spočteme $29^{-1} = 35$. Naopak 33^{-1} v $\mathbb{Z}_{39}$ neexistuje, protože $\mathrm{NSD}(33, 39) = 3 > 1$. Obecně si můžeme uvědomit, že $a \in \mathbb{Z}_b^*$, právě když $\mathrm{NSD}(a, b) = 1$. Zpětnou implikaci dostaneme s využitím Bézoutových koeficientů, a pokud $c = \mathrm{NSD}(a, b) > 1$, pak pro každé celé x máme $c \mid ax$, a proto $ax \not\equiv 1 \pmod b$.

Úloha 1.13. Nalezněte a dokažte podmínku pro nenulová celá čísla a, b, m ekvivalentní tomu, že kongruence $ax \equiv b \pmod{m}$ má nějaké řešení.

Řešení. Dokážeme, že kongruence má řešení právě tehdy, když $\mathrm{NSD}(a, m) \mid b$. Označme $d = \mathrm{NSD}(a, m)$.

Předpokládejme, že kongruence má řešení x; pak tedy platí $m \mid (ax - b)$, neboli $ax - b = km$ pro nějaké $k \in \mathbb{Z}$. Přeuspořádáním dostáváme $b = ax - km$, kde pravá strana je dělitelná d, tedy také $d \mid b$.

Na druhou stranu, pokud $d \mid b$, pomocí Bézoutovy věty nalezneme $x', k' \in \mathbb{Z}$ splňující $x'a + k'm = d$. Jelikož je b/d celé číslo, můžeme položit $x = bx'/d$, $k = bk/d$ a máme $ax + km = b$, neboli $ax \equiv b \pmod{m}$.

Úloha 1.14. Vyřešte v celých číslech následující kongruence:

(a) $x^2 + 5x \equiv 0 \pmod{19}$,

(b) $x^2 \equiv 1 \pmod{p}$ pro p prvočíslo,

⋆ (c) $x^2 + 10x + 6 \equiv 0 \pmod{17}$.

Řešení. (a) Můžeme úlohu nejprve řešit v tělese $\mathbb{Z}_{19}$:

$$x^2 + 5x = x(x + 5) = 0,$$

což znamená, že v $\mathbb{Z}_{19}$ buď $x = 0$ nebo $x = -5 = 14$. Odtud dostáváme, že $x \in \mathbb{Z}$ je řešení právě když $x \equiv 0$ nebo $x \equiv 14 \pmod{19}$ a množinou všech řešení je $\{19k \mid k \in \mathbb{Z}\} \cup \{14 + 19k \mid k \in \mathbb{Z}\}$.

(b) Kongruence je ekvivalentní podmínce $p \mid x^2 - 1 = (x + 1)(x - 1)$, proto s využitím charakterizace prvočísel dostáváme obecné řešení $\pm 1 + kp$ pro všechna $k \in \mathbb{Z}$.

(c) Stačí nahlédnout, že

$$(x - 1)(x - 6) \equiv x^2 - 7x + 6 \equiv x^2 + 10x + 6 \equiv 0 \pmod{17}$$

a pak postupovat obdobně jako v (a), abychom dostali množinu všech řešení tvaru $\{1 + 17k \mid k \in \mathbb{Z}\} \cup \{6 + 17k \mid k \in \mathbb{Z}\}$.

Úloha 1.15. Vyřešte soustavu kongruencí $x + 2y \equiv 3 \pmod{12}$, $3x + 4y \equiv 9 \pmod{12}$.

Řešení. Můžeme postupovat např. tak, že z první kongruence vyjádříme $x \equiv 3 - 2y$, dosazením do druhé pak máme $2y \equiv 0 \pmod{12}$, neboli $y \equiv 0 \pmod{6}$. Z první kongruence pak dostáváme $x \equiv 3 \pmod{12}$.

⋆ **Úloha 1.16.** Najděte všechna $x, y, z, w \in \mathbb{Z}$ splňující $x^2 + y^2 + z^2 = 15w^2$ (*Návod:* řešte nejprve kongruenci modulo 8.)

Řešení. Předpokládejme, že existuje nenulové řešení; pak existuje i takové řešení, kde jsou všechna čtyři čísla nesoudělná. Snadno nahlédneme, že libovolná druhá mocnina může být pouze 0, 1 nebo 4 modulo 8. Vyzkoušením mnoha možností zjistíme, že levá strana rovnosti může být kongruentní pouze 0, 1, 2, 3, 4, 5, 6 modulo 8, zatímco pravá pouze 0, 4, 7. Musí tedy nastat případ, kdy jsou obě strany buď 0 nebo 4, což ale nastane pouze v případě, že jsou všechna čísla sudá, což je spor s nesoudělností.

⋆ **Úloha 1.17.** Pomocí modulární aritmetiky odvoďte kritéria dělitelnosti pro čísla 9 a 11.

⋆ **Úloha 1.18.** Ukažte, že století (pokud se nezmění kalendář) nikdy nebudou začínat středou, pátkem ani nedělí. (1. ledna 2001 bylo pondělí.)

Úlohy ze soutěží (pro zahnání akutní nudy):

Úloha 1.19. Jaká je hodnota přirozeného čísla n, pokud nejmenší společný násobek 60 a n je o 777 větší než největší společný dělitel 60 a n?

Řešení. Chceme vyřešit rovnici $\text{nsn}(60, n) = 777 + \text{NSD}(60, n)$, kde nsn je nejmenší společný násobek a NSD je největší společný dělitel. Největší společný dělitel 60 a n dělí 60, takže je to jedno z čísel 1, 2, 3, 5, 6, 10, 12, 20, 30 nebo 60. Obě strany rovnice jsou dělitelné 60 a jediná možná hodnota $\text{NSD}(60, n)$, která tohle splňuje, je 3. Ale pak $\text{NSD}(60, n) = 780$ a $60 \cdot n = 3 \cdot 780$, takže $n = 39$.

Úloha 1.20. Najděte nejmenší přirozené číslo n, pro které je $11 \cdot 19 \cdot n$ rovno součinu tří po sobě jdoucích celých čísel.

Řešení. Protože 11 a 19 jsou prvočísla, musí být jedno z těchto tří po sobě jdoucích čísel dělitelné 11 a jedno (ne nutně jiné) 19. Protože je součin kladný, musí i tato tři čísla být kladná. Hledáme tedy co nejmenší kladné násobky 11 a 19, které se liší nanejvýš o 2. Nejmenší takové jsou $3 \cdot 19 = 57$ a $5 \cdot 11 = 55$. Pak už mezi ně stačí jen doplnit 56 a tato tři po sobě jdoucí čísla vynásobit: $55 \cdot 56 \cdot 57 = 11 \cdot 19 \cdot 840$. Hledaným číslem n je tedy 840.

Úloha 1.21. Přirozené číslo má 25! různých kladných dělitelů. Kolik nejvíce z nich může být pátou mocninou prvočísla?

Řešení. Číslo $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, kde p_i jsou různá prvočísla, má právě $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ kladných dělitelů. Z toho vidíme, že nejvyšší počet pátých mocnin prvočísel, které mohou dělit zadané číslo, je roven nejvyššímu možnému počtu činitelů větších nebo rovných šesti v nějakém rozkladu čísla 25!. Rozložíme proto číslo 25! na prvočinitele

$$25! = 2^{22} \cdot 3^{10} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$$

a poskládáme z těchto prvočísel co nejvíce činitelů větších nebo rovných šesti. Prvočísla větší než 5 necháme samotná, všechny pětky a trojky spojíme s dvojkami a konečně přepíšeme 2^6 na 8^2. Dohromady tak dostaneme číslo 27.