1 Naši noví kamarádi: Eukleidés, Bézout a Euler

Řešení
Verze ze dne 21. února 2024

Cíle cvičení: Důkladně si procvičíme Eukleidův algoritmus nad celými čísly, zejména si uvědomíme, že s jeho pomocí umíme počítat inverzní prvky v konečným tělesech a také některé kongruence. Na závěr se naučíme vzoreček pro výpočet Eulerovy funkce.

Úlohy, které bychom určitě měli umět řešit:

Nejprve připomeňme rozšířený Eukleidův algoritmus hledání největšího společného dělitele přirozených čísel a_0 a a_1: Položíme $(u_0, v_0) \coloneqq (1, 0)$, $(u_1, v_1) \coloneqq (0, 1)$ a $i = 1$ a pak dokud $a_i > 0$ počítáme $a_{i+1} \coloneqq (a_{i-1}) \bmod a_i$, $q_i \coloneqq (a_{i-1})\operatorname{div} a_i$ a dále hodnoty $(u_{i+1}, v_{i+1}) \coloneqq (u_{i-1},\ v_{i-1}) - q_i(u_i, v_i)$ a $i = i + 1$. Výstupem je potom $a_{i-1} = \mathrm{NSD}(a_0, a_1)$ a Bézoutovy koeficienty u_{i-1}, v_{i-1} splňující $\mathrm{NSD}(a_0, a_1) = u_{i-1}a_0 + v_{i-1}a_1$.

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 $1 = 3 \cdot 37 - 11 \cdot 10$. V tělese $\mathbb{Z}_{37}$, kde počítáme modulo 37 tedy platí

$$10^{-1} \equiv -11 \equiv 26 \pmod{37},$$

tedy $10^{-1} = 37$.

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 $18 = (-18) \cdot 1023 + 192 \cdot 96$.

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 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 $n \mid (a-b)$. Z přednášky dobře víme, že 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) Vynásobíme-li obě strany kongruence $3x \equiv 2 \pmod{5}$ hodnotou $2 \equiv 3^{-1} \pmod{5}$, dostaneme ekvivalentní kongruenci

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

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.

Úloha 1.7. Určete hodnotu Eulerovy funkce

(a) $\varphi(600)$,

(b) $\varphi(7425)$ (mohlo by se hodit vědět, že $7425 = 27 \cdot 25 \cdot 11$).

Řešení. Stačí si vzpomenout na vzoreček pro výpočet hodnoty Eulerovy funkce na základě znalosti prvočíselného rozkladu $\varphi(\prod_i p_i^{r_i}) = \prod_i (p_i - 1) p_i^{r_i - 1}$.

(a) $\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 2^2 \cdot (3-1) \cdot (5-1)5 = 160$.

(b) $\varphi(7425) = \varphi(3^3 \cdot 5^2 \cdot 11) = 2 \cdot 3^2 \cdot 4 \cdot 5 \cdot 10 = 3600$.

A teď něco pro zábavu a rozšíření obzorů:

Úloha 1.8. Najděte $\mathrm{NSD}(89, 55)$ a příslušné Bézoutovy koeficienty. Jak se na výpočtu a výsledku projeví, že se 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 1.9. 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 1.10. 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 1.11. 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 1.12. 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 $\mathbb{Z}_{19}$:

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

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 1.13. Najděte všechna čísla n taková, že $\varphi(n) = 18$.

Řešení. Protože číslo $18 = 2 \cdot 3^2$ musí být tvaru $\prod_i (p_i - 1) p_i^{r_i - 1}$ pro prvočíselný rozklad $n = \prod_i p_i^{r_i}$, obsahuje prvočíselný rozklad n nejvýše dvě různá prvočísla a snadnou diskusí zjistíme, že jsou možné pouze hodnoty 19, $27 = 3^3$, $38 = 2 \cdot 19$, $54 = 2 \cdot 3^3$.

Úloha 1.14. Najděte všechna čísla $n > 1$ taková, že $\varphi(n) \mid n$

Řešení. Podobně jako v 1.13 uvážíme, že pro $n = \prod_i p_i^{r_i}$ z podmínky $\varphi(n) \mid n$ plyne, že pro každé i existuje j, pro něž $(p_i - 1) \mid p_j$. Proto jediná prvočísla v prvočíselném rozkladu n mohou být 2 a 3 a tedy $n = 2^k \cdot 3^l$ pro $k \in \mathbb{N}$, $l \in \mathbb{N} \cup \{0\}$.

Úloha 1.15. Označme $\sigma(n)$ součet všech dělitelů přirozeného čísla n. Najděte vzorec pro výpočet $\sigma(n)$, pokud znáte prvočíselný rozklad čísla n. Inspirujte se důkazem vzorce pro Eulerovu funkci

Řešení: Řešení třeba tady.

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.)

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.)