1. Algebrou proti splínu ze začátku semestru

Eukleidův algoritmus & Bézoutovy koeficienty

1. Najděte NSD $(37, 10)$ a příslušné Bézoutovy koeficienty. Spočítejte 10^{-1} v tělese $\mathbb{Z}_{37}$.
   [$1 = 3 \cdot 37 - 11 \cdot 10$; v $\mathbb{Z}_{37}$ tedy platí $10^{-1} = -11 \equiv 26 \pmod{37}$]
2. Najděte NSD $(1023, 96)$ a příslušné Bézoutovy koeficienty. [$3 = (-3) \cdot 1023 + 32 \cdot 96$]
3. Spočtěte NSD$(2^{92} - 1, 2^{31} - 1)$ a příslušné Bézoutovy koeficienty.
   [$1 = (-2) \cdot (2^{92} - 1) + \left[(2^{62} + 2^{31} + 1) \cdot (2^{31} - 1)\right]$]
4. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$. [38]

Dělitelnost & počítání modulo

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

5. Vyřešte v celých číslech následující rovnice:
   (a) $x \equiv 2 \pmod{8}$ [$x = 2 + 8k; k \in \mathbb{Z}$]
   (b) $3x \equiv 2 \pmod{5}$ [$x = 4 + 5k; k \in \mathbb{Z}$]
   (c) $6x \equiv 2 \pmod{8}$ [$x = 3 + 4k; k \in \mathbb{Z}$; pozor na změnu modulu, když „dělíme dvojkou“]
   (d) $x^2 + 5x \equiv 0 \pmod{19}$ [$\{0, 14\} + 19k, k \in \mathbb{Z}$]
   (e) $x^2 \equiv 36 \pmod{45}$ [$\{6, 9\} + 15k, k \in \mathbb{Z}$]
6. Ukažte, že $n^2 \equiv 1 \pmod{8}$ pro každé liché $n \in \mathbb{N}$.
7. Buď p prvočíslo. Najděte všechna celočíselná řešení rovnice $x^2 \equiv 1 \pmod{p}$ a ukažte, že jsou opravdu všechna. [$x = \pm 1 + kp, k \in \mathbb{Z}$; převeďte na $p \mid (x + 1)(x - 1)$ a využijte charakterizace prvočísel]

A pro odvážné několik zábavných příkladů navíc

8. Najděte NSD $(89, 55)$ a příslušné Bézoutovy koeficienty. Jak se na výpočtu a výsledku projeví, že jedná o dva po sobě jdoucí členy Fibonacciho posloupnosti? [$1 = (-21) \cdot 89 + 34 \cdot 55$, všechna $q_i = 1$ a Bézoutovy koeficienty jsou až na znaménko rovněž po sobě jdoucí členy Fibonacciho posloupnosti]

9.⋆ Spočtěte NSD$(2k + 1, 3k + 1)$ a příslušné Bézoutovy koeficienty v závislosti na $k \in \mathbb{N}$.
[$1 = (-2) \cdot (3k + 1) + 3 \cdot (2k + 1)$]

10.⋆ 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? [$29^{-1} = 35$; 33^{-1} v $\mathbb{Z}_{39}$ neexistuje; souvisí to zásadně!]

11.⋆ Vyřešte v celých číslech $x^2 + 10x + 6 \equiv 0 \pmod{17}$. [$\{1, 6\} + 17k; k \in \mathbb{Z}$]

12.⋆ Pomocí modulární aritmetiky odvoďte kritéria dělitelnosti pro čísla 9 a 11.

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

14. Rozmyslete si, že Eukleidův algoritmus lze provádět i s polynomy a že výsledkem bude NSD dvou polynomů. Spočtěte NSD$(x^3 + x^2 + x + 1, x^2 + 2x + 2)$ a příslušné Bézoutovy koeficienty. Zkuste úlohu vyřešit jak nad tělesem racionálních čísel, tak nad $\mathbb{Z}_5$. [nad $\mathbb{Q}$: $1 = \frac{1-x}{5} \cdot (x^3 + x^2 + x + 1) + \frac{1}{5}(2 - 2x + x^2)(x^2 + 2x + 2)$, nad $\mathbb{Z}_5$: $3 + x = 1 \cdot (x^3 + x^2 + x + 1) + (1 + 4x) \cdot (x^2 + 2x + 2)$]