Teorie čísel: Cvičení 12 – výsledky a vybraná řešení

9. května 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@gmail.com

Výsledky a řešení:

-2. Pokud x splňuje rovnici, tak jistě $x \neq 0 \pmod{13}$, tj. $(x \pmod{13}) \in \mathbb{Z}_{13}^*$. Jak víme z předchozích cvičení, primitivní prvek modulo 13 je například 2. Prvek 2 tak má řád 12 a všechny prvky $\mathbb{Z}_{13}^*$ lze zapsat ve tvaru 2^a, $0 \leq a \leq 11$. Řešíme tedy kongruenci $(2^a)^3 = 2^{3a} \equiv 1 \pmod{13}$, což je splněno právě tehdy když $12 \mid 3a$ neboli $4 \mid a$. Dostáváme tak řešení $x \equiv 2^0, 2^4, 2^8 \pmod{13}$ čili $x \equiv 1, 3, 9 \pmod{13}$.

Poznámka: Pokud by se na pravé straně zadané kongruence nevyskytovala 1, ale jiný prvek $\mathbb{Z}_{13}^*$, mohli bychom si ho vyjádřit pomocí primitivního prvku ve tvaru 2^k pro vhodné k a situace by se řešila obdobně.

-1. Hledáme tedy prvky $x \in \mathbb{Z}_{15}^*$ takové, že $x^2 = 1$ a $x \neq 1$. Máme tak $x^2 \equiv 1 \pmod{15}$, což lze přepsat na součin

$$(x-1)(x+1) \equiv 0 \pmod{15}.$$

To je splněno právě tehdy, když $x \equiv \pm 1 \pmod{3}$ a $x \equiv \pm 1 \pmod{5}$ (3 a 5 jsou prvočísla, a tedy už musí některou z uvedených závorek dělit). To můžeme rozdělit na 4 případy, které vyřešíme pomocí čínské zbytkové věty:

(a) $x \equiv 1 \pmod{3}$ a $x \equiv 1 \pmod{5}$. To odpovídá prvku $1 \in \mathbb{Z}_{15}^*$, o kterém ale víme, že není involucí.

(b) $x \equiv 1 \pmod{3}$ a $x \equiv -1 \pmod{5}$. To odpovídá prvku $4 \in \mathbb{Z}_{15}^*$ (skutečně $4^2 = 16 \equiv 1 \pmod{15}$).

(c) $x \equiv -1 \pmod{3}$ a $x \equiv 1 \pmod{5}$. To odpovídá prvku $11 \in \mathbb{Z}_{15}^*$.

(d) $x \equiv -1 \pmod{3}$ a $x \equiv -1 \pmod{5}$. To odpovídá prvku $14 = -1 \in \mathbb{Z}_{15}^*$.

Všechny involuce v $\mathbb{Z}_{15}^*$ jsou tedy $4, 11, 14$.

Jak víme z předchozí cvičení, tak v cyklických grupách (tj. $\mathbb{Z}_n(+)$ pro nějaké n) existuje nanejvýš jedna involuce (plyne z řešitelnosti rovnice $2x \equiv 0 \pmod{n}$), grupa $\mathbb{Z}_{15}^*$ tak nemůže být cyklická.

0. a) Na $\mathbb{Z}_{45}$ se díváme jako na sčítací grupu, hledáme tedy všechny prvky $a \in \mathbb{Z}_{45}$, že neplatí ani jedna z rovností $a = 5n$ a $5 = an$ pro žádné n. Z první podmínky vidíme, že pokud $5 \mid a$, tak 5 nemíjí a. Podobně si můžeme rozmyslet, že pokud $NSD(a, 45) = 1$ (tj. a má inverz modulo 45), tak existuje n takové, že $an \equiv 5 \pmod{45}$ – jednoduše stačí zvolit $n = 5a^{-1}$. Tyto prvky tedy taky nemíjí 5.

Zbývá nám případ $5 \nmid a$ a $3 \mid a$. Ukážeme, že všechny tyto prvky skutečně už a míjí. Jistě $a \neq 5n$, neboť $5 \nmid a$. Podobně ale všechny prvky tvaru an jsou dělitelné 3 (což se v $\mathbb{Z}_{45}$ zachová neboť $3 \mid 45$), což 5 nesplňuje. Tedy právě všechny prvky množiny $3\mathbb{Z}_{45} \setminus 5\mathbb{Z}_{45} = \{3, 6, 9, 12, 18, 21, 24, 27, 33, 36, 39, 42\}$ míjí 5.

b) Neboť je 2 nesoudělná s 45, tak je v $\mathbb{Z}_{45}$ invertibilní a generuje celou $\mathbb{Z}_{45} = \langle 2 \rangle$. Nemíjí tedy žádný prvek.

c) Situace je očividně velmi symetrická části a) a analogickými argumenty platí, že prvky a, které míjí 3 jsou právě takové, že $3 \nmid a$ a $5 \mid a$ neboli $NSD(a, 45) = 5$. Takové prvky jsou právě $\{5, 10, 20, 25, 35, 40\}$.

Poznámka: Podmínku, že x míjí y v nějaké grupě lze přeformulovat tak, že $x \notin \langle y \rangle$ a $y \notin \langle x \rangle$.

1. a) $x \equiv 1 \pmod{13}$
   b) $x \equiv \pm 1 \pmod{13}$
   c) $x \equiv 2, 3, 10, 11 \pmod{13}$
   d) Tato kongruence nemá řešení.
   e) $x \equiv 5, 6 \pmod{11}$

2. a) $11, 19, 29,$
   b) $16, 35, 50.$

3. a) Nemíjí žádný prvek.
   b) $(3\mathbb{Z}_{60} \cup 5\mathbb{Z}_{60}) \setminus 2\mathbb{Z}_{60}$
   c)$(3\mathbb{Z}_{60} \cup 5\mathbb{Z}_{60}) \setminus 4\mathbb{Z}_{60}$
   d) $(4\mathbb{Z}_{60} \cup 5\mathbb{Z}_{60}) \setminus 6\mathbb{Z}_{60}$

4. Použijte čínskou zbytkovou větu k převedení kongruencí do kongruencí modulo prvočísla.

7. $n = 2, 3, 4, 6, 8, 12, 24$