Teorie čísel: Cvičení 13 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, email:simonkahlavinkova@gmail.com

Nápovědy:

-1. Použijte standardní postup, který bude předvedený na cvičení: Nalezněte primitivní prvek modulo 13, označte $x = 2^a$ a hledejte vhodné exponenty a.

0. Použijte standardní postup, který bude předvedený na cvičení: Pro zadané číslo b pracujte nezávisle s oběma podmínkami $a \notin \langle b \rangle$ (její význam by měl být jasný) a $b \notin \langle a \rangle$ (nad kterou je potřeba se zamyslet; říká něco o dělitelích čísla 45 obsažených v rozkladu čísla b).

1. Postupujte jako v příkladu -2.; i pravou stranu vyjádřete pomocí primitivního prvku.

2. Postupujte jako v příkladu 0.

3. Použijte Čínskou zbytkovou větu: K ověření platnosti potřebné kongruence stačí (a je nutné) ověřit onu kongruenci modulo příslušná prvočísla. (Obecně mocniny prvočísel, ale to tady není relevantní.)

4. Vycházejte přímo z definic.

5. Jako příklad 0.

6. Použijte ČZV, vyjděte přímo z definic.

7. Určitě by stačilo ověřit, že žádné z čísel $1, \ldots, 6$ není svědek (což není příliš pracné). Pokud si pamatujete přesnější informaci než jen „Pro složené číslo vždy existuje svědek.“, můžete ji využít a ušetřit si tím práci.

8. Formulace je záměrně nesymetrická, ale ve skutečnosti hrají b a f stejnou roli (tvrzení má totiž platit pro každé b a každé f). Přirozenější je dokázat si nejprve obměnnou implikaci v podobě: $(x, y) \in \langle (x', y') \rangle \Rightarrow x \in \langle x' \rangle$; z ní pak už plynou obě podmínky pro míjení.

9. Jedna z možností je využití toho, že $\mathbb{Z}_p^*$ je těleso.

10. Postupujte jako v příkladech 0. a 3.

11. Použijte ČZV.

12. Uvažujte o $\mathrm{NSD}(a, n)$ a $\mathrm{NSD}(b, n)$.

13. Pro $p = 2$ dojdete ke sporu už modulo 4. Pro liché p využijte toho, že existuje primitivní prvek.

14. Uvažte primitivní prvek modulo větší z prvočísel.

Výsledky:

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

2. (a) Nemíjí žádný prvek.
   (b) $(3\mathbb{Z}_{60} \cup 5\mathbb{Z}_{60}) \setminus 2\mathbb{Z}_{60}$, neboli prvky, které nejsou dělitelné 2, ale jsou dělitelné 3 nebo 5.
   (c) $(3\mathbb{Z}_{60} \cup 5\mathbb{Z}_{60}) \setminus 4\mathbb{Z}_{60}$, neboli prvky, které nejsou dělitelné 4, ale jsou dělitelné 3 nebo 5.
   (d) $(4\mathbb{Z}_{60} \cup 5\mathbb{Z}_{60}) \setminus 6\mathbb{Z}_{60}$, neboli prvky, které nejsou dělitelné 6, ale jsou dělitelné 4 nebo 5.

4. Jediní lháři jsou ± 1.

5. V obou případech jsou ± 1 jediní lháři.

6. Jediní lháři jsou ± 1.

7. Stačí ověřit, že žádné z čísel $\pm 1, \pm 2, \pm 3$ není svědek. Díky větě 5.8 dokonce stačí ověřit, že alespoň tři z těchto čísel nejsou svědci. Pokud použijeme nedokázanou větu ze skript A. Drápala, uvedenou na konci sekce 5.7, víme, že pro složené číslo N může být lhářů nejvýše $N/4$, takže pro $N = 7$ stačí ověřit, že ± 1 nejsou svědci, což je jasné.

11. $n = 2, 3, 4, 6, 8, 12, 24$, neboli čísla větší než jedna, v jejichž rozkladu se 3 vyskytne v nulté či první mocnině a dvojka v nulté, první, druhé či třetí.

Vybraná vzorová řešení:

-2. Pokud x splňuje rovnici, tak jistě $x \neq 0 \pmod{13}$, takže hledáme řešení v $\mathbb{Z}_{13}^*$. Jak víme z předchozích cvičení (nebo snadno ověříme), primitivní prvek modulo 13 je například 2. Všechny prvky $\mathbb{Z}_{13}^*$ lze zapsat ve tvaru 2^k, $0 \leq k \leq 11$. Zavedeme-li substituci $x = 2^k$, řešíme kongruenci $2^{3k} \equiv 1 \pmod{13}$, 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, viz další příklady.

-1. 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 $\mathrm{NSD}(a, 45) = 1$ (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) Protože je 2 nesoudělná s 45, víme, že je v $\mathbb{Z}_{45}$ invertibilní. Proto $\langle 2 \rangle = \mathbb{Z}_{45}$. Žádný prvek proto nemůže splnit $a \notin \langle 2 \rangle$, takže 2 nemíjí vůbec žádný prvek.

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

0 **a)** $N = 51 = 3 \cdot 17$, $N - 1 = 2 \cdot 25$. Lháři tedy budou právě $0 < a < 51$ splňující $a^{25} \equiv \pm 1 \pmod{51}$.Mohli bychom začít náhodně zkoušet čísla, trefili bychom se buď do lháře nebo svědka a postupně bychom našli příklad od obojího. Zkusme ale ukázat sofistikovanější postup, jak lháře najít. Rozebereme postupně dva možné případy:

- $a^{25} \equiv 1 \pmod{51}$

  Vidíme, že je to z čínské zbytkové věty ekvivalentní dvojici podmínek $a^{25} \equiv 1 \pmod{3}$ a $a^{25} \equiv 1 \pmod{17}$. To za pomocí Malé Fermatovy věty můžeme ekvivalentně upravit na $a \equiv 1 \pmod{3}$ a $a^9 \equiv 1 \pmod{17}$. Podmínka $a^9 \equiv 1$ je ovšem ekvivalentní $a \equiv 1 \pmod{17}$, neboť 9 nedělí řád grupy $\mathbb{Z}_{17}^*$. Tedy tato větev postupu dává pouze lháře $a \equiv 1 \pmod{51}$, kterého jsme nechtěli.
- $a^{25} \equiv -1 \pmod{51}$

  Stejně jako v předchozím případě získáme dvojici kongruencí $a \equiv -1 \pmod{3}$ a $a^9 \equiv -1 \pmod{17}$. Druhou z podmínek zjevně splňuje $a \equiv -1 \pmod{17}$. Ukážeme, že jiné řešení ani existovat nemůže. Obecně totiž umíme zdůvodnit jednoznačnost řešení každé kongruence tvaru $a^r \equiv c \pmod{17}$ pro r nesoudělné s $|\mathbb{Z}_{17}^*| = 16$: Například z Bézoutovy věty dostaneme, že existují k, l splňující $kr = 16l + 1$, čímž dostaneme $a \equiv a^{16l+1} \equiv c^k \pmod{17}$, tj. hodnota a modulo 17 je jednoznačně určena. Dohromady tak dostaneme, že jediným řešením $a^{25} \equiv -1 \pmod{51}$ je $a \equiv -1 \pmod{51}$.

Ukázalo se, že lháři jsou pouze 1 a $N-1$; jako svědka lze tedy volit krerékoli jiné číslo. Pokud bychom chtěli svědka najít rychleji, stačí se postarat o porušení alespoň jedné z podmínek $a \equiv -1 \pmod 3$ a $a^9 \equiv -1 \pmod{17}$. Lze tedy zvolit například $a \equiv 1 \pmod 3$, tj. kupříkladu $a = 4$ je svědek.

b) $221 = 13 \cdot 17$, $N - 1 = 220 = 2^2 \cdot 55$

Lháři tedy v tomto případě musí splňovat některou ze tří podmínek $a^{55} \equiv 1 \pmod{221}$, $a^{55} \equiv -1 \pmod{221}$, $a^{110} \equiv -1 \pmod{221}$.

Analogicky jako v předchozím případě (převedením na kongruence modulo prvočísla za použití ČZV, aplikací MFV a uvažování nesoudělnosti exponentu a řádu grupy) dostaneme, že první dva případy odpovídají přesně lhářům $a \equiv \pm 1 \pmod{221}$.

Když už víme, že jediným řešení $a^5 5 \equiv -1 \pmod{221}$ je $a \equiv -1 \pmod{221}$, lze třetí možnost ekvivalentně přepsat jako $a^2 \equiv -1 \pmod{221}$. Pomocí ČZV to rozdělíme na $a^2 \equiv -1 \pmod{13}$ a $a^2 \equiv -1 \pmod{17}$. První z podmínek dává $a \equiv \pm 5 \pmod{13}$ a druhá $a \equiv \pm 4 \pmod{17}$. To lze dohromady přepsat jako $a \equiv \pm 21, \pm 47$. Tím jsme našli všechny lháře.

Poznámka: Čísla 1 a $N-1$ budou lháři vždycky; část a) ukazuje, že někdy ani jiní neexistují. Podobně čísla soudělná s N budou vždycky svědci.