Teorie čísel: Cvičení 13 – výsledky a vybraná řešení

16. května 2022

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

Výsledky a řešení:

-2. Budeme postupně používat vlastnosti Jacobiho symbolů, viz věta 4.14 ze skript.

$$\left(\frac{477}{247}\right) = \left(\frac{230}{247}\right) = \left(\frac{2}{247}\right)\left(\frac{115}{247}\right) = (-1)^{\frac{247^2-1}{8}}(-1)^{\frac{247-1}{2}\frac{115-1}{2}}\left(\frac{247}{115}\right) = -\left(\frac{17}{115}\right) =$$

$$= -(-1)^{\frac{115-1}{2}\frac{17-1}{2}}\left(\frac{115}{17}\right) = -\left(\frac{13}{17}\right) = -(-1)^{\frac{13-1}{2}\frac{17-1}{2}}\left(\frac{17}{13}\right) = -\left(\frac{4}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = -1.$$

Všimněte si, že jsme se při výpočtu úplně vyhnuli rozkladu na prvočísla (kromě dělitelnosti 2).

-1. Díky čínské zbytkové větě je zadaný problém ekvivalentní s dvojící podmínek $x^2 \equiv 9 \pmod{11}$ a $x^2 \equiv 4 \pmod{7}$. Snadno ověříme, že obě tyto kongruence už mají řešení. První z nich konkrétně $x \equiv \pm 3 \pmod{11}$ a druhá z nich $x \equiv \pm 2 \pmod{7}$. Nyní akorát potřebujeme zpětně najít odpovídající zbytky modulo 77.

(a) $x \equiv 3 \pmod{11}$ a $x \equiv 2 \pmod{7}$. To odpovídá prvkům $x \equiv 58 \pmod{77}$.

(b) $x \equiv 3 \pmod{11}$ a $x \equiv -2 \pmod{7}$. To odpovídá prvkům $x \equiv 47 \pmod{77}$.

(c) $x \equiv -3 \pmod{11}$ a $x \equiv 2 \pmod{7}$. To odpovídá prvkům $x \equiv 30 \pmod{77}$.

(d) $x \equiv -3 \pmod{11}$ a $x \equiv -2 \pmod{7}$. To odpovídá prvkům $x \equiv 19 \pmod{77}$.

Řešením tedy jsou $x \equiv 19, 30, 47, 58 \pmod{77}$.

(Řešení 30 a 19 jsme mohli najít už z předchozích znalostí jako -47 a -58.)

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

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 $\mathbb{Z}_{17}^*$ (viz minulé cvičení 12). Tedy tato větev postupu dává pouze lháře $a \equiv 1 \pmod{51}$, kterého jsme nechtěli.

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

Stejně jako v předchozím případě získáme dvojici kongruencí $a \equiv -1 \equiv 2 \pmod{3}$ a $a^9 \equiv -1 \pmod{17}$. Můžeme si všimnout, že druhou z podmínek splňuje například (a pouze) $a \equiv -1 \pmod{17}$. Dohromady tak dostaneme lháře $a = 50 \equiv -1 \pmod{51}$.

Pokud bychom naopak chtěli svědka, tak musíme nesplnit alespoň jednu z podmínek $a \equiv -1 \equiv 2 \pmod{3}$ a $a^9 \equiv -1 \pmod{17}$. Můžeme tedy zvolit například $a \equiv 1 \pmod{3}$, tj. například $a = 4$ a dostaneme svědka složenosti 51.

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 $a \equiv \pm 1 \pmod{221}$. Třetí podmínku můžeme obdobně analogicky upravit na $a^2 \equiv -1 \pmod{13}$ a $a^{14} \equiv -1 \pmod{17}$.

K nalezení svědka si můžeme například všimnout, že volba $a \equiv 1 \pmod{13}$ a $a \equiv -1 \pmod{17}$ nesplňuje ani jednu z těchto tří podmínek a dostáváme tak svědka $a = 118$.

K nalezení lháře bychom opět mohli použít $221 - 1 = 220$ z druhé podmínky, nebo se můžeme pokusit splnit podmínku třetí podmínku. To už je ovšem pouze jednoduché řešení kongruencí (viz minulé cvičení) a funguje mimo jiné například volba $a \equiv 8 \pmod{13}$ a $a \equiv 13 \pmod{17}$, což nám dá lháře $a = 47$.

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

1. a) -1

   b) -1

   c) -1

   d) -1

2. a) Jacobiho symboly v tomto případě splývají s Legendreovými a pomocí nich můžeme zjistit, že první kongruence má řešení, zatímco druhá ne.

   b) $x \equiv 39, 94, 115, 170 \pmod{209}$

   c) Ačkoliv Jacobiho symbol vyjde 1, kongruence nemá řešení.

3. $a = 1, 8$

4. a) Jediní lháři jsou $1, 38$. Svědka lze zvolit jakkoliv jinak.

   b) Například 2 je svědek a 81 je lhář. Řešení je více.

5. Jediní lháři jsou 1 a 76.

6. Ukažte, že neexistuje svědek.