Hledá se lhář

Zadání: Popište všechny svědky a silné lháře pro 9, 21, 49 a 105.

Řešení: Lháři pro složené $n = 2^r s + 1$ jsou čísla $a \in \{1, \ldots, n-1\}$ taková, že Rabin-Millerův test prvočíselnosti dá falešný pozitivní výsledek: Buď $a^s \equiv 1 \pmod{n}$ nebo existuje $i \in \{0, \ldots, r-1\}$, že $a^{2^i s} \equiv -1 \pmod{n}$. Pokud číslo není lhář, je svědek, stačí tedy popsat lháře.

Postup je napsat sadu rovnic, z nichž každý lhář musí jednu splňovat, a tyto rovnice pak vyřešit s použitím Čínské zbytkové věty a struktury grup $\mathbb{Z}^\star_{p^n}$ (jde to samozřejmě i hrubou silou, ale to bychom se zapotili). Budeme všechno počítat modulo n, takže třeba lhář -1 je ve skutečnosti $n-1$.

$9 = 2^3 \cdot 1 + 1$ Lhář splňuje jednu z rovnic:

$$\begin{aligned} a^1 &\equiv 1 \pmod{9} \\ a^1 &\equiv -1 \pmod{9} \\ a^2 &\equiv -1 \pmod{9} \\ a^4 &\equiv -1 \pmod{9} \end{aligned}$$

První dvě rovnice mají jasná řešení 1 a -1, tato čísla jsou lháři vždycky. Má třetí rovnice řešení a, tak nutně $a \in \mathbb{Z}^\star_9$, tedy protože $\mathbb{Z}^\star_9 = \langle 2 \rangle$, tak platí $a = 2^k$ pro nějaké $k \in \{0, 1, \ldots, 5\}$. Máme tedy rovnici

$$(2^k)^2 \equiv -1 \equiv 2^3 \pmod{9}.$$

Rozmyslete si, že protože řád 2 v $\mathbb{Z}^\star_9$ je 6, je tato rovnice ekvivalentní $2k \equiv 3 \pmod{6}$. Dále si všimněte, že tato rovnice nemá řešení, protože levá strana a modul jsou dělitelné 2, zatímco pravá strana je lichá.

Podobně zjistíme, že ani čtvrtá rovnice nemá řešení; rozmyslete si, že aby mohlo nastat $a^{2^i s} \equiv -1 \pmod{n}$ pro $i > 0$, tak -1 musí být tzv. kvadratický zbytek modulo n: Musí existovat b takové, že $b^2 \equiv -1 \pmod{n}$.

$21 = 2^2 \cdot 5 + 1$ Hledejme nejprve a která řeší rovnici $a^5 \equiv 1 \pmod{21}$. Pomocí čínské zbytkové věty si rovnici přepíšeme jako soustavu:

$$\begin{aligned} a^5 &\equiv 1 \pmod{3} \\ a^5 &\equiv 1 \pmod{7}, \end{aligned}$$

ze které snadno dostaneme $a \equiv 1 \pmod 3$. Dále 3 je primitivní prvek modulo 7, takže $a \equiv 3^k \pmod 7$ pro $5k \equiv 0 \pmod 6$, takže $k = 6$, takže $a \equiv 1 \pmod 7$. Jediné řešení tedy je $a = 1$.

Obdobně prozkoumáme rovnici $a^5 \equiv -1 \pmod{21}$, kterou ČZV přepíše do tvaru:

$$\begin{aligned} a^5 &\equiv -1 \pmod 3 \\ a^5 &\equiv -1 \pmod 7, \end{aligned}$$

První rovnici splňuje $a \equiv -1 \pmod 3$, druhou pak $a = 3^k$, kde $5k \equiv 3 \pmod 6$, tedy $k = 5$ a $a = -1$ je druhý lhář.

Protože už víme, že -1 není kvadratický zbytek modulo 7, nemůže mít rovnice $a^{10} \equiv -1 \pmod{21}$ řešení. Jediní silní lháři jsou tedy opět $\pm 1 \pmod{21}$, zbytek čísel jsou svědci neprvočíselnosti 21.

$49 = 2^4 \cdot 3 + 1$ Hledejme nejprve a která řeší rovnici $a^3 \equiv 1 \pmod{49}$.

Tato rovnice se dá řešit více způsoby, my ukážeme postup podobný důkazu z přednášky, že lhářů je málo.

Pokud $a^3 \equiv 1 \pmod{49}$, tak nutně $a \in \mathbb{Z}_{49}^\star$. Jaký může být řád prvku a v této grupě? Buď je $a = 1$ řád je 1, nebo má a řád přesně 3. Hledáme tedy prvky řádu 3 v $\mathbb{Z}_{49}^\star \simeq \mathbb{Z}_6 \times \mathbb{Z}_7$. Prvky řádu 3 pak mají v součinu grup $\mathbb{Z}_6 \times \mathbb{Z}_7$ souřadnice $(2, 0)$ a $(4, 0)$. Kdybychom tedy měli popsaný isomorfismus $\mathbb{Z}_{49}^\star$ a $\mathbb{Z}_6 \times \mathbb{Z}_7$, stačilo by nám zjistit, jaké prvky $\mathbb{Z}_{49}^\star$ odpovídají $(2, 0)$ a $(4, 0)$. My ale tento isomorfismus známe (viz přednáška o struktuře grup $\mathbb{Z}_{p^e}^\star$): Souřadnicím (i, j) v $\mathbb{Z}_6 \times \mathbb{Z}_7$ odpovídá v $\mathbb{Z}_{49}^\star$ číslo $31^i \cdot 8^j$ (první základ je 3^7, druhý $7 + 1$). Vyjdou nám tedy řešení $1, 30$ a 18.

Alternativně a méně elegantně se dá řešení rovnice $a^3 - 1 \equiv 0 \pmod{49}$ najít i tak, že rovnici vydělíme $a - 1$ a vyřešíme jako kvadratickou rovnici.

Rovnice $a^3 \equiv -1$ se řeší velmi podobně jako ta výše uvedená. Krom jasného řešení -1 hledáme prvky $\mathbb{Z}_{49}^\star$, které mají řád 6, čili souřadnice $(1, 0)$ nebo $(5, 0)$ v $\mathbb{Z}_6 \times \mathbb{Z}_7$. Vyjdou lháři $a \equiv 48, 19, 31$.

Protože -1 není kvadratický zbytek modulo 7 (to se ukáže tak, že si napíšeme $b = 3^k \pmod 7$ a hledáme řešení rovnice $3^{2k} \equiv 3^3 \pmod 7$), neexistují a taková, že $a^6 \equiv -1$, $a^{12} \equiv -1$ nebo $a^{24} \equiv -1$ modulo 7, tedy ani modulo 49.

Závěr: Silní lháři jsou $1, 48, 18, 31, 19, 30 \pmod{49}$, ostatní čísla jsou svědci.

$105 = 2^3 \cdot 13 + 1$ Chceme $a^{13} \equiv 1 \pmod{105}$, což si můžeme pomocí ČZV přepsat jako:

$$\begin{aligned} a^{13} &\equiv 1 \pmod 3 \\ a^{13} &\equiv 1 \pmod 5 \\ a^{13} &\equiv 1 \pmod 7. \end{aligned}$$

Řády grupy $\mathbb{Z}_3^\star, \mathbb{Z}_5^\star, \mathbb{Z}_7^\star$ dělí číslo 12, takže platí $a^{12} \equiv 1 \pmod{105}$ pro každé a nesoudělné se 105 (to je lepší než Eulerova věta!). Proto naše soustava ve skutečnosti říká:

$$\begin{aligned} a^1 &\equiv 1 \pmod 3 \\ a^1 &\equiv 1 \pmod 5 \\ a^1 &\equiv 1 \pmod 7. \end{aligned}$$

Jediný takový lhář je tedy $a = 1$.

Podobně jediný lhář splňující $a^{13} \equiv -1 \pmod{105}$ je -1.

Víme, že je užitečné vědět, jestli -1 je kvadratický zbytek modulo 105. Na to je snadná odpověď: Není, protože neexistuje a takové, aby $a^2 \equiv -1 \pmod 3$ (ostatně to samé platí modulo 7). Tedy žádná další čísla nemohou být lháři.

Lháři jsou tedy opět jenom $\pm 1 \pmod{45}$.