Cvičení 10. 5. 2012 – řešení, co se nestihla na cvičení

Příklad 4. Dokažte, že pokud G je konečná komutativní grupa, tak existuje $g \in G$, že řád g je roven exponentu G. Pomocí tohoto zjištění a faktu, že $\mathbb{Z}_p$ je těleso pro p prvočíslo, dokažte, že $\mathbb{Z}_p^\star$ je cyklická pro každé p.

Řešení: Buď G je konečná komutativní grupa a a, b prvky G. Buďte řády $k = |a|$, $l = |b|$ nesoudělné. Potom řád ab je roven kl. Pokud totiž $a^n b^n = e$, tak platí $a^{nk} b^{nk} = e$, tedy $a^{nk} = e$, což je možné jenom tak, že $l|nk$, tedy $l|n$. Podobně $k|n$ a tedy nejmenší přirozené n je rovno kl.

Nyní si stačí uvědomit, že kdykoli exponent G obsahuje p^n pro p prvočíslo, tak v G existuje prvek g_p stupně přesně p^n. Vynásobením všech g_p pro různá p tedy dostaneme prvek g řádu přesně $\exp(G)$.

Pokud by $\mathbb{Z}_p^\star$ nebyla cyklická, žádný prvek $\mathbb{Z}_p^\star$ by neměl řád $p - 1$. Podle předchozího tvrzení by potom exponent $\mathbb{Z}_p^\star$ musel být roven $n < p - 1$. Přitom z definice exponentu platí $x^n = 1 \pmod{p}$ pro každé $x \in \{1, \ldots, p - 1\}$. Ale potom je $x^n - 1$ nenulový polynom nad tělesem, který má víc kořenů, než je jeho stupeň, spor.

Příklad 5. Faktorizujte číslo $N = 6557$, víte-li, že je součinem dvou prvočísel p, q splňujících $|p - q| < 10$ (jde to bez kalkulačky!).

Řešení: Budeme předpokládat $q = p + k$ pro $k = 0, 2, 4, 6, 8$ (prvočíla p, q jsou evidentně obě lichá) a řešit kvadratickou rovnici $p(p + k) = 6557$.

Pokud $k = 0$, tak $p^2 = 6657$. Ale my víme, že $80^2 = 6400 < 6557 < 6561 = 81^2$ (tohle se dá ještě tipnout a vynásobit písemně).

Pokud $k = 2$, potřebujeme $p(p+2) = 6557$, což po doplnění na čtverec dává $(p + 1)^2 = p + 2p + 1 = 6558$, což už víme, že není čtverec.

Pokud $k = 4$, potřebujeme $p(p + 4) = 6557$. Tedy $p^2 + 4p + 4 = 6561 = 81^1$, tedy $p + 2 = 81$ funguje (a nutně $q = 83$).

Celý postup výše je ekvivalentní tomu, že zkoušíme napsat 6557 ve tvaru $a^2 - b^2 = (a + b)(a - b)$ pro malé b, tj. zjišťujeme, zda $6557 + b^2$ není náhodou čtverec pro $b = 0, 1, 2, 3, 5$. Pro $b = 2$ máme $6557 + 4 = 6561 = 81^2$. Zapsáno takhle je to takzvaná Fermatova faktorizace.

Příklad 6. Tři malá prasátka mají každé svůj privátní klíč (d_1, N_1), (d_2, N_2) a (d_3, N_3) a všechna používají veřejný exponent $e = 3$. Červená Karkulka poslala každému prasátku identickou pozvánku M na narozeninovou oslavu zašifrovanou pomocí jeho veřejného klíče, tj. zprávy mají tvar $C_1 = M^e \pmod{N_1}$, $C_2 = M^e \pmod{N_2}$, $C_3 = M^e \pmod{N_3}$.

Velký zlý vlk všechny tři zašifrované zprávy zachytil a zná veřejné klíče. Poraďte mu, jak z C_1, C_2, C_3 získat M.

Řešení: Vlk snadno může ověřit, že čísla N_1, N_2, N_3 jsou nesoudělná – spustí na každou z jejich dvojic Euklidův algoritmus a pokud dostane výsledek větší než jedna, už z něj vypadne faktorizace nějakého N_i.

Aby posílání zprávy mělo smysl, musí být $M < N_1, N_2, N_3$, takže $0 \leq M^3 < N_1N_2N_3$. Číslo M^3 pak lze snadno dopočítat z Čínské zbytkové věty a sady rovnic:

$$M^3 \equiv C_1 \pmod N_1$$
$$M^3 \equiv C_2 \pmod N_2$$
$$M^3 \equiv C_3 \pmod N_3.$$

Vlk tedy určil M^3 v $\mathbb{Z}$. Nyní mu stačí spočítat běžnou třetí odmocninu z M^3, aby dostal M.

Proti tomuto útoku existují dvě obrany: Větší e a padding.

Příklad 7 (bonus z minule)**.** Popište všechny svědky a silné lháře pro 49, 21, 25 a 45.

Řešení: Ve všech případech jsou lháři pro složené $n = 2^k m + 1$ čísla a taková, že Rabin-Millerův test prvočíselnosti dá falešný pozitivní výsledek: Buď $a^m \equiv 1 \pmod n$ nebo existuje $i \in \{0, \ldots, k-1\}$, že $a^{2^i m} \equiv -1 \pmod n$. Aby mohla nastat druhá podmínka pro $i > 0$, musí být -1 kvadratický zbytek modulo n, čímž vyloučíme mnoho případů.

Pokud číslo není lhář, je svědek, stačí tedy popsat lháře.

$49 = 2^4 \cdot 3 + 1$ Hledejme nejprve a která řeší rovnici $a^3 \equiv 1 \pmod 49$. Tuto rovnici přepíšeme jako $(a-1)(a^2+a+1) \equiv 0 \pmod 49$. Pokud $7 | a-1$, tak $a^2+a+1 \equiv 3 \pmod 7$. Proto $a^3 \equiv 1 \pmod 49$ má řešení $a \equiv 1 \pmod 49$ a pak všechna řešení rovnice $a^2+a+1 \equiv 0 \pmod 49$. Přitom:

$$a^2 + a + 1 \equiv (a+25)^2 + 13 \equiv 0 \pmod{49},$$

kde $13 = -6^2 \pmod{49}$, takže chceme najít a, aby $(a+25-6)(a+25+6) \equiv 0 \pmod{49}$. Tato rovnice má evidentně řešení $a = 18$ a $a = 30$. Další řešení mít nemůže, protože 7 nemůže současně dělit $a+19$ a $a+31$. (Děkuji Anežce Titěrové za opravu chyby, která byla v tomto místě v původním řešení.)

Rovnice $a^3 \equiv -1$ se řeší úplně stejně jako ta výše uvedená. Vyjdou řešení $a \equiv 48, 19, 31$.

Protože -1 není kvadratický zbytek modulo 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.

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

$$a^5 \equiv 1 \pmod 3$$
$$a^5 \equiv 1 \pmod 7,$$

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:

$$a^5 \equiv -1 \pmod 3$$
$$a^5 \equiv -1 \pmod 7,$$

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.

$25 = 2^3 \cdot 3 + 1$ Opět hledáme a, že $a^3 \equiv 1 \pmod{25}$. Grupa $\mathbb{Z}_{25}^{\star}$ má primitivní prvek 2, takže můžeme psát $a = 2^k$, kde $3k \equiv 0 \pmod{20}$. Tato rovnice má opět jediné řešení $a \equiv 1 \pmod 2$5.

Hledejme teď a, že $a^3 \equiv -1 \pmod{25}$. Obdobně jako výše nám vyjde, že $a \equiv -1 \pmod{25}$ je jediné řešení. Další možnost je $a^6 \equiv -1 \pmod{25}$. Protože -1 je kvadratický zbytek modulo 5, je i kvadratický zbytek modulo 25. Hledáme tedy opět a ve tvaru 2^k, kde $6k \equiv 10 \pmod{20}$. Tato rovnice má dvě řešení $k \equiv 5, 15 \pmod{20}$, kterým odpovídají $a \equiv 7, 18 \pmod{25}$.

Zbývá rovnice $a^{12} \equiv -1 \pmod{25}$. Opět dosadíme $a = 2^k$ a z $12k \equiv 10 \pmod{20}$ dostaneme rovnici $6k \equiv 5 \pmod{10}$, která nemá řešení.

Lháři jsou $\pm 1, 7, 18 \pmod{25}$, ostatní čísla jsou svědci.

$45 = 2^2 \cdot 11 + 1$ Chceme $a^{11} \equiv 1 \pmod{45}$, což si můžeme roztrhnout na dvě rovnice:

$$a^{11} \equiv 1 \pmod 5$$
$$a^{11} \equiv 1 \pmod 9,$$

Protože $\mathbb{Z}_5^{\star}, \mathbb{Z}_9^{\star}$ jsou cyklické řádů nesoudělných s 11, má tato soustava pouze triviální řešení $a = 1 \pmod{45}$. Podobně $a^{11} \equiv -1 \pmod{45}$ implikuje $a \equiv -1 \pmod{45}$.

Nyní si už stačí opět všimnout, že -1 není kvadratický zbytek modulo 3, abychom vyloučili existenci a, že $a^{22} \equiv -1 \pmod{45}$. Lháři jsou tedy opět jenom $\pm 1 \pmod{45}$.