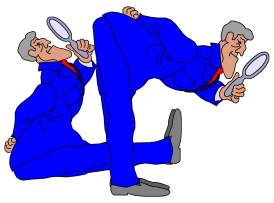
6. Asymetrické šifrovací systémy neboli systémy s veřejným klíčem - Systém s veřejným klíčem se složitostí stejnou jako faktorizace

Jan Paseka

Ústav matematiky a statistiky
Masarykova univerzita

8. listopadu 2021

O čem to bude



- Kongruenční rovnice a mocninné zbytky
- Grupa G_m

Úvod

Uveďme příklad systému s veřejným klíčem, o kterém lze ukázat, že jeho složitost je ekvivalentní s problémem faktorizace.

Tvůrcem systému je **Rabin** (1979).

Každý uživatel systému vybere dvojici (p, q) velkých různých prvočísel, které uchová v tajnosti. Zároveň si vybere přirozené číslo $B < N = p \cdot q$.

Veřejný klíč bude dvojice (B, N), ***soukromý klíč*** bude faktorizace (p, q) čísla N.

Šifrovací funkce e zprávy M, kde M je reprezentovatelná jako přirozené číslo v definičním oboru $\{1, \ldots, N-1\}$ (v případě potřeby se zpráva rozparceluje na více bloků), je

$$e(M) = M \cdot (M + B) \pmod{N}. \tag{1.1}$$

Faktorizace Kongruenční rovnice Grupa G_m

Úvod

Je-li C výsledný kryptogram, pak dešifrovací problém je nalézt M tak, že

$$M^2 + B \cdot M = C \pmod{N}. \tag{1.2}$$

Kongruenční rovnice a mocninné zbytky I

Poznamenejme nejprve, že platí následující tvrzení

Věta 1.1

Kongruenční rovnice

$$ax = b \ (mod\, m). \tag{1.3}$$

je řešitelná právě tehdy, když $(a, m)|b$.

V tomto případě má rovnice právě (a, m) *navzájem nekongruentních řešení modulo* m.

Důkaz. Výše uvedená podmínka je nutná, neboť v opačném případě nemůže platit rovnost $ax = b + km$ v oboru celých čísel. Buď tedy $d = (a, m)$ a nechť $d|b$.

Kongruenční rovnice a mocninné zbytky II

1. Nechť $d = 1$. Dle Bezoutovy věty existují celá čísla u, v taková, že $au + mv = 1$. Existují tedy celá čísla x, y splňující $ax + my = b$, tj. platí $ax = b \pmod m$. Řešení x je jednoznačně určeno modulo m, neboť je-li x' jiné řešení splňující $ax' = b \pmod m$, máme $a(x - x') = 0 \pmod m$ a tedy $x = x' \pmod m$.
2. Nechť $d > 1$. Protože nutně $d|b$, máme po dosazení do vztahu $ax = b + km$ za $a = a'd$, $b = b'd$, $m = m'd$ a po vydělení číslem d kongruenční rovnici

   $$a'x = b' \pmod{m'}.$$

   Z případu 1 víme, že tato kongruenční rovnice má jediné řešení $x = x_0 \pmod{m'}$. Všechna řešení modulo m tvoří právě d následujících čísel

   $$x = x_0, x_0 + m', \ldots, x_0 + (d-1)m', \pmod m.$$

Kongruenční rovnice a mocninné zbytky III

Budeme chtít vyřešit resp. zjistit, zda následující kongruenční rovnice má řešení v celých číslech pro $n \geq 2$:

$$ax^n = b \pmod{m}. \tag{1.4}$$

Podobně jako v případě lineárních kongruečních rovnic se lze omezit na případ, kdy $(a, m) = 1$. Použitím Eulerovy věty pak obdržíme rovnici $x^n = ba^{\varphi(m)-1} \pmod{m}$.

Buďte tedy m, n přirozená čísla taková, že $m \geq 2$, $n \geq 2$, a celé číslo takové, že $(a, m) = 1$.

Číslo a se nazývá ***n*-tý mocninný zbytek** modulo m, je-li řešitelná kongruence

$$x^n = a \pmod{m}. \tag{1.5}$$

Kongruenční rovnice a mocninné zbytky IV

Pro zkoumání takovýchto kongruenčních rovnic využijeme následujících tvrzení.

Věta 1.2

Buďte čísla $m_1, m_2, \ldots, m_r$ navzájem nesoudělná, $a_1, a_2, \ldots, a_r$ a $b_1, b_2, \ldots, b_r$ libovolná celá čísla taková, že $(a_1, m_1) = (a_2, m_2) = \cdots = (a_r, m_r) = 1$.

Pak má systém

$$a_i x = b_i \pmod{m_i} \tag{1.6}$$

pro $1 \leq i \leq r$ právě jedno řešení modulo $m = m_1 \cdot m_2, \cdot \cdots \cdot m_r$.

Kongruenční rovnice a mocninné zbytky V

Důkaz. Zřejmě mají jednotlivé kongruenční rovnice právě jedno řešení, které získáme z Euklidova algoritmu pro čísla a_i a m_i - $a_i \cdot u_i + m_i \cdot v_i = 1$.

Pronásobíme-li b_i máme $a_i \cdot x_i + m_i \cdot y_i = b_i$, tj.

$$a_i x = b_i \pmod{m_i})$$

Předpokládejme, že toto řešení je ve tvaru

$$x = c_i \pmod{m_i} \tag{1.7}$$

pro $1 \leq i \leq r$.

Protože máme $(m_i, m_j) = 1$ pro $i \neq j$, máme $(\frac{m}{m_1}, \frac{m}{m_2}, \ldots, \frac{m}{m_r}) = 1$.

Zejména tedy existují čísla $y_1, y_2, \ldots, y_r$ tak, že

$$\frac{m}{m_1} \cdot y_1 + \frac{m}{m_2} \cdot y_2 + \cdots + \frac{m}{m_r} \cdot y_r = 1.$$

Kongruenční rovnice a mocninné zbytky VI

Položme $e_i = \frac{m}{m_i} \cdot y_i$ pro $1 \leq i \leq r$.

Zřejmě platí

$$e_1 + e_2 + \cdots + e_r = 1 \pmod{m}, \tag{1.8}$$

$$e_i \cdot e_j = 0 \pmod{m} \text{ pro } i \neq j, \tag{1.9}$$

$$e_i \cdot e_i = e_i \pmod{m}, \tag{1.10}$$

$$e_i = \begin{cases} 0 \pmod{m_i} & \text{pro } i \neq j, \\ 1 \pmod{m_i} & \text{pro } i = j. \end{cases} \tag{1.11}$$

Totiž $e_i \cdot e_j = m \cdot c$, $e_i \cdot e_i = \sum_i^r e_j \cdot e_i = 1 \cdot e_i = e_i \pmod{m}$, $e_j = m_i \cdot c'$, $(e_i, m_i) = 1$.

Položme

$$x_0 = c_1 e_1 + c_2 e_2 + \cdots + c_r e_r.$$

Kongruenční rovnice a mocninné zbytky VII

Máme pak z 1.11, že

$$x_0 = c_i \pmod{m_i}$$

pro $1 \leq i \leq r$.

Je tedy x_0 společné řešení modulo m. Pro každé jiné řešení x_0' modulo m systému 1.7 máme

$$x_0 = x_0' \pmod{m_i}$$

pro $1 \leq i \leq r$ a tedy také $x_0 = x_0' \pmod{m}$.

Připomeňme, že pro všechna přirozená čísla m tvoří zbytkové třídy $[a]_m$ pro $(a, m) = 1$ multiplikativní abelovskou grupu modulo m.

Přitom počet prvků této grupy je právě $\varphi(m)$. Tuto grupu budeme v dalším označovat jako G_m.

Grupa G_m I

Věnujme se pro chvíli zkoumání její algebraické struktury. Nechť $m = m_1 m_2 \dots m_r$, kde čísla $m_1, m_2, \dots, m_r$ jsou navzájem nesoudělná.

Podle Věty 1.2 má systém kongruencí

$$x = a_i \pmod{m_i}$$

pro $1 \leq i \leq r$ právě jedno řešení a modulo m.

Přitom platí, že $(a, m_i) = (a_i, m_i)$ pro $1 \leq i \leq r$.

Zejména tedy $(a, m_i) = 1$ právě tehdy, když $(a_i, m_i) = 1$. Opět podle věty 1.2 máme jednoznačně určený rozklad na základě rovností 1.8, 1.9, 1.10, 1.11 tvaru

$$[a]_m = [a_1 e_1]_m + \dots + [a_r e_r]_m. \qquad (1.12)$$

Grupa G_m II

Označme jakožto $[a_i^*]_m$ zbytkovou třídu

$$[e_1 + \cdots + e_{i-1} + a_i e_i + e_{i+1} + \cdots + e_r]_m.$$

Pak pro pevné i tvoří množina $G_{m_i}^*$ zbytkových tříd $[a_i^*]_m$ podgrupu grupy G_m.

Z rovnosti 1.12 obdržíme jednoznačně určený rozklad

$$[a]_m = [a_1^*]_m \dots [a_r^*]_m. \tag{1.13}$$

Provedeme-li tento rozklad pro všechna $[a]_m \in G_m$, lze výše uvedené formulovat tak, že grupa G_m je přímý součin podgrup $G_{m_1}^*, \dots, G_{m_r}^*$.

Máme zejména izomorfismus mezi grupami G_{m_i} a $G_{m_i}^*$ pomocí zobrazení $[a_i^*]_m \longleftrightarrow [a_i]_{m_i}$.

Grupa G_m III

Řekneme, že ***a patří modulo m k exponentu d***, pokud

$$(a, m) = 1,\ a^d = 1 \pmod m,$$

$$\text{ale } a^n \neq 1 \pmod n \text{ pro } 1 \leq n < d.$$

To ale není nic jiného, než že a je prvek řádu d v multiplikativní grupě G_m.

Grupa G_m III

Lemma 1.3

Patří-li a modulo m k exponentu d, jsou čísla $1, a, a^2, \ldots, a^{d-1}$ modulo m nekongruentní. Je-li dále $a^t = 1 \pmod m$, pak $d|t$.

Důkaz. Nechť $a^k = a^h \pmod m$, $0 \leq h < k < d$. Protože $(a, m) = 1$, je $a^{k-h} = 1 \pmod m$.

To je však spor s $0 < k - h < d$ a minimalitou d.

Položíme-li $t = dq + r$, $0 \leq r < d$, máme

$$1 = a^t = a^{dq+r} = a^r \pmod m,$$

tj. musí platit $r = 0$.

Grupa G_m IV

Lemma 1.4

Patří-li a modulo m k exponentu d a n je přirozené číslo s $(n, d) = 1$, patří a^n rovněž modulo m k exponentu d.

Důkaz. Nechť a^n patří k exponentu t. Pak z 1.3 a $(a^n)^t = 1 \pmod m$, obdržíme $d|nt$. Protože $(n, d) = 1$, je nutně $d|t$ a tedy i $d \leq t$. Protože $(a^n)^d = (a^d)^n = 1 \pmod m$, je nutně i $t \leq d$. Celkem $t = d$. ∎

Poznamenejme, že číslo g, které modulo m patří k exponentu $\varphi(m)$, se nazývá ***primitivní kořen*** modulo m.

Lze dokázat, že pro každé prvočíslo p vždy existuje primitivní kořen g modulo p, tedy každé číslo od 1 do $p - 1$ lze vyjádřit jakožto mocninu g.

Grupa G_m V

Speciálně lze ověřit, že pokud $t|\varphi(p)$, má kongruenční rovnice

$$x^t = 1 \pmod{p}, \tag{1.14}$$

právě t navzájem nekongruentních řešení.

Tvrzení 1.5

K modulu m existuje buď žádný nebo $\varphi(\varphi(m))$ modulo m nekongruentních primitivních kořenů.

Grupa G_m VI - Důkaz Věty 1.5

Důkaz. Nechť g je primitivní kořen modulo m.

Podle Lemmatu 1.4 je rovněž g^n primitivní kořen modulo m v případě, že platí $(n, \varphi(m)) = 1$.

Takovýchto čísel $n \leq \varphi(m)$ je právě $\varphi(\varphi(m))$.

Máme tedy v každém případě alespoň $\varphi(\varphi(m))$ primitivních kořenů.

To, že nelze nalézt žádné další primitivní kořeny, plyne z Lemmatu 1.3. Totiž, probíhá-li ν čísla mezi 0 a $\varphi(m) - 1$, probíhá pak g^ν grupu G_m. Zvolíme-li ν tak, že $(\nu, \varphi(m)) = t > 1$, pak platí $1 < \frac{\varphi(m)}{t} < \varphi(m)$

$$(g^\nu)^{\frac{\varphi(m)}{t}} = (g^{\varphi(m)})^{\frac{\nu}{t}} = 1 \pmod{m}.$$

Pak ale nemůže být g^ν primitivní kořen modulo m. ∎

Grupa G_m VII

Tvrzení 1.6

Buď p prvočíslo. Pak G_p je cyklická. Zejména tedy existuje primitivní kořen modulo p.

Důkaz. Pro $p = 2$ je tvrzení věty triviální.

Nechť p je v dalším liché prvočíslo.

Pro $d|(p-1)$ označme $\chi(d)$ počet zbytkových tříd z G_p, které patří k exponentu d modulo p.

Máme ukázat, že $\chi(p-1) > 0$. Podle Tvrzení 1.5 je pak dokonce $\varphi(p-1) = \chi(p-1)$.

Nechť tedy existuje nějaké číslo a, které patří k exponentu d.

Pak dle lemmatu 1.3 jsou čísla tvaru $1, a, a^2, \ldots, a^{d-1}$ navzájem nekongruentní řešení rovnice $x^d - 1 = 0 \pmod p$.

Grupa G_m VIII - Pokračování důkazu Tvrzení 1.6

Toto lze přepsát pomocí polynomiální kongruence následovně

$$x^d - 1 = (x-1)(x-a)\cdots(x-a^{d-1}) \pmod p.$$

Zároveň jsou výše uvedená čísla také všechna řešení této kongruence. Podle Lemmatu 1.4 pak i a^k patří k exponentu d, pokud $(d,k) = 1$. To znamená, že mezi řešení přináleží $\varphi(d)$ čísel, která patří k exponentu d. Nutně pak buď $\chi(d) = 0$ nebo $\chi(d) = \varphi(d)$.
Provedeme-li výčet všech prvků z G_p podle toho, ke kterému exponentu patří, je

$$\sum_{d|(p-1)} \chi(d) = p - 1.$$

Grupa G_m IX - Pokračování důkazu Tvrzení 1.6

Je ale dobře známo, že

$$\sum_{d|(p-1)} \varphi(d) = p - 1.$$

Nutně pak $\chi(d) = \varphi(d)$. ■

FI Buď g primitivní kořen modulo m, $(a, m) = 1$ a μ buď jednoznačně určené číslo mezi 0 a $\varphi(m) - 1$ z kongruenční rovnice

$$g^{\mu} = a \pmod{m}.$$

Pak říkáme, že μ je ***index (diskrétní logaritmus)*** čísla a vzhledem k bázi g.
Píšeme pak $\mu = \log_g a \bmod \varphi(m)$. Přitom platí pravidla pro logaritmování součinu, mocniny atd.

Grupa G_m X

Tvrzení 1.7

Pro diskrétní logaritmování platí následující zákony:

1. $\log_g ab = \log_g a + \log_g b \pmod{\varphi(m)}$,
2. $\log_g a^n = n \log_g a \pmod{\varphi(m)}$,
3. $\log_g 1 = 0 \pmod{\varphi(m)}$,
4. $\log_g g = 1 \pmod{\varphi(m)}$,
5. $\log_g(-1) = \frac{1}{2}\varphi(m) \pmod{\varphi(m)}, m > 2$.

Důkaz. **MA** Z $a = g^{\log_g a} \pmod m$ a $b = g^{\log_g b} \pmod m$ obdržíme $ab = g^{\log_g a + \log_g b} \pmod m$. Porovnáme-li toto s $ab = g^{\log_g ab} \pmod m$, obdržíme první vlastnost. Vlastnosti 2 a 3 plynou bezprostředně z vlastnosti 1. Z $g = g^{\log_g g} \pmod m$ obdržíme 4.

Grupa G_m XI

Pátá vlastnost je založena na Fermat-Eulerově větě:

$$g^{\varphi(m)} - 1 = \left(g^{\frac{\varphi(m)}{2}} - 1\right)\left(g^{\frac{\varphi(m)}{2}} + 1\right) = 0 (\mathrm{mod}\, m).$$

■

Tvrzení 1.8

Buď p liché prvočíslo tak, že číslo a není dělitelné p. Kongruenční rovnice

$$x^n = a \,(\mathrm{mod}\, p^r)$$

má právě $d = (n, p^{r-1}(p-1))$ nekongruentních řešení, pokud d dělí $\log_g a$. Jinak je tato kongruence neřešitelná.

Důkaz. Tvrzení věty se logaritmováním převede na lineární kongruenční rovnici

$$n \log_g x = \log_g a \,(\mathrm{mod}\, p^{r-1}(p-1)).$$

Zbytek plyne z tvrzení 1.1. ■

Grupa G_m XII

Tvrzení 1.9

Buď p liché prvočíslo tak, že číslo a není dělitelné p, $d = (n, p^{r-1}(p-1))$. Kongruenční rovnice

$$x^n = a \,(\mathrm{mod}\, p^r)$$

má právě řešení právě tehdy, když platí kongruenční rovnice

$$a^{\frac{1}{d}p^{r-1}(p-1)} = 1 \,(\mathrm{mod}\, p^r). \qquad (1.15)$$

Důkaz. Buď g primitivní kořen modulo p^r. Podle věty 1.8 je výše uvedená kongruence řešitelná právě tehdy, když existuje číslo h tak, že $\log_g a = h \cdot d$. Pak platí $a = g^{\log_g a} = g^{h \cdot d} \,(\mathrm{mod}\, p^r)$. Tedy

$$a^{\frac{1}{d}p^{r-1}(p-1)} = g^{h \cdot p^{r-1}(p-1)} = 1 \,(\mathrm{mod}\, p^r).$$

Grupa G_m XIII

Nechť obráceně platí kongruenční rovnice 1.15. Položme $\mu = \log_g a$.

Protože $a = g^\mu \pmod{p^r}$, máme $g^{\frac{\mu}{d} \cdot p^{r-1}(p-1)} = 1 \pmod{p^r}$.

Protože g je primitivní kořen modulo p^r, je $\frac{\mu}{d}$ celé číslo, tj. d dělí μ.

Tedy dle tvrzení 1.8 je kongruenční rovnice řešitelná.