Struktura grup $\mathbb{Z}_n^*$

11. a 12. přednáška z kryptografie

Obsah

Exponent grupy

Podle Eulerovy věty je $a^{|G|} = 1$ pro každý prvek $a \in G$. Avšak $|G|$ nemusí být tím nejmenším exponentem, na který musíme umocnit dokonce libovolný prvek $a \in G$, aby vyšlo 1.

Definice

Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1. Nejmenší přirozené číslo $m > 0$ takové, že pro každé $a \in G$ je $a^m = 1$, se nazývá *exponent grupy* G. Značíme jej $\exp(G)$.
Pokud takové m neexistuje, položíme $\exp(G) = 0$.

Příklady

- $\exp(\mathbb{Z}_n) = n$, $\exp(\mathbb{Z}) = 0$
- $\exp(\mathbb{Z}_9^*) = 6 = \varphi(9)$
- $\exp(\mathbb{Z}_8^*) = 2 < \varphi(8)$

Exponent grupy

Tvrzení

- Je-li G konečná grupa, pak má kladný exponent a platí $\exp(G) \mid |G|$.
- Má-li grupa G kladný exponent, pak každý prvek $a \in G$ má konečný řád a platí $\mathrm{r}(a) \mid \exp(G)$.
- Je-li grupa G cyklická, pak $\exp(G) = 0$, právě když je G nekonečná, a $\exp(G) = |G|$, právě když je G konečná.
- Jsou-li G_1, G_2 grupy, pak $\exp(G_1 \times G_2) = \mathrm{lcm}(\exp(G_1), \exp(G_2))$

Exponent grupy

Věta

Má-li Abelova grupa G exponent $\exp(G) = m > 0$,
pak obsahuje prvek řádu m.

Důkaz: Buď $m = \prod_{i=1}^{k} p_i^{e_i}$.

Pro každé $1 \leq i \leq k$ najdeme v G prvek b_i takový, že $b_i^{\frac{m}{p_i}} \neq 1$,
jinak by $\exp(G) \leq \frac{m}{p_i} < m$.
Označme $m_i = \frac{m}{(p_i^{e_i})}$. Prvek $a_i = b_i^{m_i}$ má řád $\mathrm{r}(a_i) = p_i^{e_i}$.
Buď $a = \prod_{i=1}^{k} a_i$. Díky nesoudělnosti řádů prvků a_i je $\mathrm{r}(a) = m$.

Důsledek

Konečná Abelova grupa G je cyklická, právě když $\exp(G) = |G|$.

Struktura grup $\mathbb{Z}_n^*$

Otázka: Pro jaká $n \in \mathbb{N}$ je grupa $\mathbb{Z}_n^*$ cyklická?
Pro grupy $\mathbb{Z}_p^*$, p prvočíslo, využijeme faktu, že $(\mathbb{Z}_p, +, \cdot)$ je těleso.

Tvrzení

Nenulový polynom nad tělesem má nejvýše tolik různých kořenů, kolik je jeho stupeň.

Poznámka

Totéž platí pro polynomy nad oborem integrity (tj. okruhem bez dělitelů nuly), ale už ne nad libovolným okruhem.
Např. polynom $x^2 - 1$ má čtyři kořeny v $\mathbb{Z}_8$ a to $\pm 1, \pm 3$.

Struktura grup $\mathbb{Z}_n^*$

Tvrzení

Grupa $\mathbb{Z}_p^*$ je cyklická pro každé prvočíslo p.

Důkaz: Označme $\exp(\mathbb{Z}_p^*) = m \leq p - 1$.
Každý prvek $a \in \mathbb{Z}_p^*$ splňuje $a^m = 1$, aneb je kořenem $x^m - 1$.
Protože $\mathbb{Z}_p$ je těleso, musí být $m = p - 1$.
Prvek řádu m (který existuje) je generátorem grupy $\mathbb{Z}_p^*$.

Tvrzení

Grupa T^* je cyklická pro každé konečné těleso T (nebo pro každý konečný obor integrity).

Struktura grup $\mathbb{Z}_n^*$

Dále prozkoumáme grupy $\mathbb{Z}_{p^e}^*$, kde p je prvočíslo.

Tvrzení

Pro každé $1 \leq k \leq p - 1$ platí: $p \mid \binom{p}{k}$

Lemma 1

Nechť p je prvočíslo a $e \geq 1$ přirozené číslo.
Když $a \equiv b \pmod{p^e}$, pak $a^p \equiv b^p \pmod{p^{e+1}}$.

Lemma 2

Nechť p je prvočíslo a $e \geq 1$ přirozené číslo a nechť $p^e > 2$.
Když $a \equiv 1 + p^e \pmod{p^{e+1}}$, pak $a^p \equiv 1 + p^{e+1} \pmod{p^{e+2}}$.

Struktura grup $\mathbb{Z}_n^*$

Tvrzení

Grupa $\mathbb{Z}_{p^e}^*$ je cyklická pro každé liché prvočíslo p (tj. $p > 2$)
a každé přirozené číslo $e \geq 1$.
Tedy $\exp(\mathbb{Z}_{p^e}^*) = |\mathbb{Z}_{p^e}^*| = p^{e-1}(p-1)$.

Důkaz: Buď a generátor grupy $\mathbb{Z}_p^*$ a označme r řád a v grupě $\mathbb{Z}_{p^e}^*$.
Pak $b = a^{\frac{r}{p-1}}$ má řád $p-1$ v grupě $\mathbb{Z}_{p^e}^*$.
Z lemmatu 2 lze dokázat, že $c = 1 + p$ má řád p^{e-1} v grupě $\mathbb{Z}_{p^e}^*$.
Protože $\gcd(p^{e-1}, p-1) = 1$, tak $\mathrm{r}(bc) = p^{e-1}(p-1)$
a prvek bc je generátor grupy $\mathbb{Z}_{p^e}^*$.

Struktura grup $\mathbb{Z}_n^*$

Tvrzení

Grupy $\mathbb{Z}_2^*$ a $\mathbb{Z}_4^*$ jsou cyklické.
Grupa $Z_{2^e}^*$ není cyklická pro každé přirozené číslo $e \geq 3$.
Přitom $\exp(\mathbb{Z}_{2^e}^*) = \frac{|\mathbb{Z}_{2^e}^*|}{2} = 2^{e-2}$.

Důkaz: Z lemmatu 2 lze dokázat, že $c = 5$ má řád 2^{e-2}.
Dále platí, že $-1 \notin \langle 5 \rangle$.
Odtud $\mathbb{Z}_{2^e}^*$ je vnitřním ditektním součinem podgrup $\langle -1 \rangle \dot{\times} \langle 5 \rangle$,
$\exp(\mathbb{Z}_{2^e}^*) = \mathrm{lcm}(2, 2^{e-2}) = 2^{e-2}$ a grupa $\mathbb{Z}_{2^e}^*$ není cyklická.

Struktura grup $\mathbb{Z}_n^*$

Zbývají grupy $\mathbb{Z}_n^*$, kde n je dělitelné aspoň dvěma různými prvočísly.

Tvrzení

Grupa $\mathbb{Z}_{2p^e}^*$ je cyklická pro každé liché prvočíslo $p > 2$
a každé přirozené číslo $e \geq 1$.

Tvrzení

Grupa $\mathbb{Z}_n^*$ není cyklická pro každé složené číslo $n = n_1 n_2$,
kde $2 < n_1 < n_2$ a $\gcd(n_1, n_2) = 1$.
V tomto případě je $\exp(\mathbb{Z}_n^*) = \mathrm{lcm}(\exp(\mathbb{Z}_{n_1}^*), \exp(\mathbb{Z}_{n_2}^*)) \leq \frac{|\mathbb{Z}_n^*|}{2}$.

Důkaz: Nechť $n = n_1 n_2$, kde $\gcd(n_1, n_2) = 1$, pak z Čínské věty
o zbytcích $\mathbb{Z}_n^* \cong \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$.

Struktura grup $\mathbb{Z}_n^*$

Shrnutí

Grupa $\mathbb{Z}_n^*$ je cyklická, právě když

$$n = 1, 2, 4, p^e, 2p^e,$$

kde p je liché prvočíslo a e kladné přirozené číslo.

Carmichaelova funkce

Definice

Funkce $\lambda : \mathbb{N}^+ \to \mathbb{N}^+ : \lambda(n) = \exp(\mathbb{Z}_n^*)$ se nazývá *Carmichaelova funkce*. Aneb $\lambda(n)$ pro $n > 1$ je nejmenší $m > 0$ takové, že pro všechna a nesoudělná s n je $a^m = 1$ v $\mathbb{Z}_n$. Dále $\lambda(1) = 1$.

Vzorce

- $\lambda(p^e) = p^{e-1}(p-1) = \varphi(p^e)$ pro prvočísla $p > 2$
- $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^e) = 2^{e-2} = \frac{\varphi(2^e)}{2}$ pro $e \geq 3$
- $\lambda(n_1 \cdot n_2) = \mathrm{lcm}(\lambda(n_1), \lambda(n_2))$ pro n_1, n_2 nesoudělná

Carmichaelova funkce

Poznámka

RSA-šifrování bude fungovat i v případě, že klíče budou inverzní modulo $\lambda(n)$, resp. modulo celočíselný násobek $k\lambda(n)$, kde $k > 0$.

Důsledek: Pokud při tvorbě klíče použijeme místo prvočísel p, q Carmichaelova čísla, nevadí to, RSA-šifrování bude fungovat.

Carmichaelovo číslo je složené číslo n takové, že pro každé $a \in \mathbb{Z}_n^*$ platí: $a^{n-1} = 1$ v $\mathbb{Z}_n$. Aneb pro n Carmichaelovo $\lambda(n) \mid n - 1$.

Fermatův test prvočíselnosti Carmichaelova čísla od prvočísel nerozpozná.

Řešení rovnic $x^m = 1$ v $\mathbb{Z}_n$

Zbytkový isomorfismus

Nechť $n = \prod_{i=1}^k p_i^{e_i}$, kde prvočísla p_i jsou navzájem různá. Zobrazení $\theta : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}} : a \mapsto (a_1, \ldots, a_k)$, kde $0 \leq a_i < p_i^{e_i}$ splňují $a \equiv a_i \pmod{p_i^{e_i}}$, je okruhový isomorfismus (tzv. čínský zbytkový isomorfismus): $\mathbb{Z}_n \cong \prod_{i=1}^k \mathbb{Z}_{p_i^{e_i}}$

Restrikce zobrazení θ na množinu $\mathbb{Z}_n^*$ je grupový isomorfismus multiplikativních grup: $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_k^{e_k}}^*$

Důsledek

Rovnice $x^m = 1$ můžeme řešit residuálně, neboť $a^m = 1$ v $\mathbb{Z}_n$,právě když $a_i^m = 1$ v $\mathbb{Z}_{p_i^{e_i}}$ pro každé $1 \leq i \leq k$.

Řešení rovnic $x^m = 1$ v $\mathbb{Z}_n$

Tvrzení

Pokud $a \in \mathbb{Z}_n$ řeší rovnici $x^m = 1$, pak a je invertibilní, tj. $a \in \mathbb{Z}_n^*$.

Rovnici $x^m = 1$ tedy stačí řešit v grupě $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_k^{e_k}}^*$.

- V cyklických grupách $\mathbb{Z}_{p_i^{e_i}}^*$, kde $p_i > 2$, umíme najít všechna řešení rovnice $x^m = 1$ přes generátor grupy (viz minule). Počet řešení je $d_i = \gcd(m, \varphi(p_i^{e_i}))$.
- V grupě $\mathbb{Z}_{2^e}^*$ najdeme všechna řešení rovnice $x^m = 1$ v cyklické podgrupě $\langle 5 \rangle$ řádu 2^{e-2}, bude jich $\gcd(m, 2^{e-2})$. Pro m liché už to budou všechna řešení, pro m sudé přibudou ještě opačná řešení (tvaru $-a$, kde a je již nalezené řešení).
- Počet všech řešení v $\mathbb{Z}_n^*$ pak bude $d = \prod_{i=1}^k d_i$ a mají tvar $a = a_1 q_1 + \cdots + a_k q_k$, kde q_i jsou z Čínské věty o zbytcích.

Řešení rovnic $x^m = 1$ v $\mathbb{Z}_n$

Příklad

Řešte rovnici $x^6 = 1$ v $\mathbb{Z}_{304}$.

Každé řešení leží v $\mathbb{Z}^*_{304} \cong \mathbb{Z}^*_{19} \times \mathbb{Z}^*_{16}$.

- $\mathbb{Z}^*_{19} = \langle 2 \rangle$, $\varphi(19) = 18$. Rovnice má zde 6 řešení, a to $x \in \langle 2^3 \rangle = \{\pm 1, \pm 7, \pm 8\}$.
- $\mathbb{Z}^*_{16} = \langle 5 \rangle \dot{\times} \langle -1 \rangle$, přitom v podgrupě $\langle 5 \rangle$ se rovnice redukuje na $x^2 = 1$ a řeší ji $x \in \langle 5^2 \rangle = \{9, 1\}$. Exponent je sudý, tudíž všechna řešení jsou $x \in \{\pm 1, \pm 9\}$.

V $\mathbb{Z}^*_{304}$ bude $6 \cdot 4 = 24$ řešení $x \in \{\pm 1, \pm 7, \pm 8\} q_{19} + \{\pm 1, \pm 9\} q_{16}$, kde $q_{19} = 96$ a $q_{16} = -95$ (získáme je řešením Diofantické rovnice $16t + 19r = 1$).

Řešení rovnic $x^m = 1$ v $\mathbb{Z}_n$

Druhé mocniny a odmocniny v $\mathbb{Z}^*_n$

- Nechť p je liché prvočíslo, pak rovnice $x^2 = 1$ má dvě řešení v $\mathbb{Z}^*_{p^e}$ a to $x = \pm 1$.
  Grupový homomorfismus $\rho_2 : \mathbb{Z}^*_{p^e} \to \mathbb{Z}^*_{p^e} : a \mapsto a^2$ má $|Ker\, \rho_2| = 2$, $|Im\, \rho_2| = \frac{\varphi(p^e)}{2}$.
- Nechť $n = \prod_{i=1}^{k} p_i^{e_i}$ je liché číslo, pak rovnice $x^2 = 1$ má celkem 2^k řešení v $\mathbb{Z}^*_n$.
  Grupový homomorfismus $\rho_2 : \mathbb{Z}^*_n \to \mathbb{Z}^*_n : a \mapsto a^2$ má $|Ker\, \rho_2| = 2^k$, $|Im\, \rho_2| = \frac{\varphi(n)}{2^k}$.

Řešení rovnic $x^m = x$ v $\mathbb{Z}_n$

Pozorování

Pokud $n = n_1 n_2$, kde $\gcd(n_1, n_2) = 1$, tak rovnice $x^m = x$ může mít v monoidu $\mathbb{Z}_n$ i nenulová neinvertibilní řešení. Aneb rovnici nelze zkrátit (ani za předpokladu $x \neq 0$) a řešit v grupě $\mathbb{Z}^*_n$.
Např. $a \in \mathbb{Z}_n$, kde $\theta(a) = (0, 1)$, je nenulové řešení soudělné s n_1.

Tvrzení

Prvek a řeší rovnici $x^m = x$ v $\mathbb{Z}_{p^e}$, právě když je buď $a = 0$, anebo a řeší rovnici $x^{m-1} = 1$ v $\mathbb{Z}_{p^e}$.

Důsledek

Rovnice $x^m = x$ v $\mathbb{Z}_n$ umíme vyřešit reziduálně.
Např. umíme spočítat, které zprávy se při RSA šifrování nezmění.

Řešení rovnic $x^m = b$ v $\mathbb{Z}_n$

Poznámka

Všechna řešení rovnice $x^m = b$ v $\mathbb{Z}_n$ jsou tvaru $x = ac$, kde a je jedno partikulární řešení této rovnice, c je libovolné řešení rovnice $x^m = 1$ v $\mathbb{Z}_n$.

Návod na hledání partikulární $m-$té odmocniny z b jsme nepodali, postup pro nalezení všech $m-$tých odmocnin z 1 se opíral o fakt, že známe faktorizaci čísla n.

Věří se, že počítání $m-$tých odmocnin v $\mathbb{Z}_n$ je bez znalosti faktorizace n exponenciálně těžký problém (hrubá síla). Toho využívá bezpečnost RSA šifrování.

Struktura grup $\mathbb{Z}_n^*$

Literatura

- Shoup: A Computational Introduction to Number Theory and Algebra. Kapitoly 6.5. a 7.5.
  http://shoup.net/ntb/