Konečné grupy

9. a 10. přednáška z kryptografie

Obsah

Řád prvku v grupě

Podle Eulerovy věty pro každý prvek a v n-prvkové grupě G platí: $a^n = 1$ v G. Pro konkrétní prvek a ale nemusí být n tím nejmenším exponentem, na který musíme umocnit, aby vyšlo 1.

Definice

Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$.
Nejmenší přirozené číslo $r > 0$ takové, že $a^r = 1$ v grupě G, se nazývá *řád prvku* a v grupě G. Značíme $\mathrm{r}(a)$.
Pokud takové r neexistuje, řekneme, že prvek a má nekonečný řád.

Příklad

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$
$\mathrm{r}(8) = 2$, $\mathrm{r}(4) = 3$, $\mathrm{r}(2) = 6$

Řád prvku v grupě

Poznámky

- Známe-li $\mathrm{r}(a)$ v grupě G, usnadní nám to umocňování: při výpočtu a^k můžeme v exponentu počítat modulo $\mathrm{r}(a)$.
- Je-li grupa aditivní $(G, +)$ s neutrálním prvkem 0, pak řád je nejmenší $r > 0$ takové, že $ra = \underbrace{a + \ldots + a}_{r\text{-krát}} = 0$.
- Řád prvku a v grupě G je roven řádu cyklické podgrupy $\langle a \rangle$. (Toto tvrzení je vlastně alternativní definicí.)

Řád prvku v grupě

Tvrzení

Nechť G je konečná grupa.
Pro každé $a \in G$ platí: $\mathrm{r}(a) \mid |G|$

Eulerova věta

Nechť G je konečná grupa.
Pro každé $a \in G$ platí: $a^{|G|} = 1$.

Poznámka: Zatím jsme podali důkaz Eulerovy věty pro komutativní grupy, ale v Lagrangeově větě jsme komutativitu nepotřebovali. Díky ní (a předchozímu tvrzení, které z ní bezprostředně vyplývá) máme Eulerovu větu dokázánu i pro nekomutativní grupy.

Řád prvku v grupě

Tvrzení

Nechť G je konečná grupa, $a, b \in G$.

- $a^k = 1$ v grupě G právě, když $\mathrm{r}(a) \mid k$
- $\mathrm{r}(a^{-1}) = \mathrm{r}(a)$
- Nechť navíc G je Abelova grupa (nebo aspoň $ab = ba$). Pokud jsou $\mathrm{r}(a)$, $\mathrm{r}(b)$ nesoudělné, pak $\mathrm{r}(ab) = \mathrm{r}(a)\,\mathrm{r}(b)$.

Tvrzení

Nechť G_1, G_2 jsou konečné grupy, $(a_1, a_2) \in G_1 \times G_2$.

- $\mathrm{r}(a_1, a_2) = \mathrm{lcm}(\mathrm{r}(a_1), \mathrm{r}(a_2))$

Řád prvku v grupě

Tvrzení

Nechť G je konečná grupa, $a \in G$.

- $\mathrm{r}(a^k) = \frac{\mathrm{r}(a)}{\gcd(k, \mathrm{r}(a))}$
- speciálně, pokud $d \mid \mathrm{r}(a)$, pak $r(a^d) = \frac{\mathrm{r}(a)}{d}$

Důsledky

- $\mathrm{r}(a^k) = \mathrm{r}(a)$ právě, když $\gcd(k, \mathrm{r}(a)) = 1$
- cyklická podgrupa $\langle a \rangle$ má celkem $\varphi(\mathrm{r}(a))$ generátorů

Příklad

$\mathbb{Z}_9^* = \langle 2 \rangle$, protože $\mathrm{r}(2) = 6 = |\mathbb{Z}_9^*|$.
Všechny prvky řádu 6 v $\mathbb{Z}_9^*$ jsou tvaru 2^k, kde $\gcd(k, 6) = 1$.
Odtud $k \in \{1, 5\}$ a prvky řádu 6 jsou $2^1 = 2$ a $2^5 = 5$.

Cyklické grupy

Definice

Grupa G se nazývá *cyklická grupa*, pokud pro nějaký prvek $a \in G$ je $G = \langle a \rangle$. Prvek a je *generátor* grupy G.

Tvrzení

- Cyklické grupy jsou Abelovy.
- Konečná grupa G řádu n je cyklická právě, když obsahuje prvek a řádu $\mathrm{r}(a) = n$.
- Cyklická grupa řádu n má celkem $\varphi(n)$ generátorů. Pravděpodobnost, že při náhodné volbě prvku $a \in G$ najdeme generátor, je $\frac{\varphi(n)}{n}$.

Cyklické grupy

Tvrzení

Prvek $a \in G$ je generátor konečné grupy G řádu n právě, když je splněna některá z podmínek:

- $a^r \neq 1$ pro každé $r < n$, kde $r \mid n$
- $a^r \neq 1$ pro každé $r = \frac{n}{p}$, kde p je prvočíslo a $p \mid n$

Příklady

- Grupy $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ jsou cyklické s generátorem 1.
- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$
  $\mathrm{r}(2) = 6$, tedy grupa $(\mathbb{Z}_9^*, \cdot)$ je cyklická s generátorem 2.
- $(\mathbb{Z}_8^* = \{\pm 1, \pm 3\}, \cdot)$ není cyklická grupa, neboť $a^2 = 1$ pro každé $a \in \mathbb{Z}_8^*$.

Cyklické grupy

Příklad

Je dána grupa $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} \setminus \{0\}$.

- $|\mathbb{Z}_{19}^*| = \varphi(19) = 18 = 2 \cdot 3^2$. Možné řády jsou $1, 2, 3, 6, 9, 18$.
- Najděte generátor v $\mathbb{Z}_{19}^*$:
  Zkusíme $a = 2$: $2^6 = 7 \neq 1$ (odtud také $2^2 \neq 1$, $2^3 \neq 1$),
  $2^9 = -1 \neq 1$, tudíž $\mathrm{r}(2) = 18$ a 2 je generátor v $\mathbb{Z}_{19}^*$.
- Pravděpodobnost trefy do generátoru je $P = \frac{\varphi(18)}{18} = \frac{1}{3}$.
- Určete $\mathrm{r}(8)$ a použijte ho při výpočtu 8^{195} v $\mathbb{Z}_{19}$:
  $\mathrm{r}(8) = \mathrm{r}(2^3) = \frac{18}{3} = 6$, $8^{195} = 8^3 = 18$ v $\mathbb{Z}_{19}$.

Cyklické grupy

Věta

- Každá nekonečná cyklická grupa je izomorfní s grupou $(\mathbb{Z}, +)$.
- Každá cyklická grupa řádu n je izomorfní s grupou $(\mathbb{Z}_n, +)$.

Příslušný isomorfismus je $f : k \mapsto a^k$, kde a je generátor grupy.

Podgrupy konečných cyklických grup

- Podgrupy v $(\mathbb{Z}_n, +)$ jsou tvaru $d\mathbb{Z}_n = \langle d \rangle$, kde $d \mid n$. Přitom podgrupa $d\mathbb{Z}_n = \{di, 1 \leq i \leq \frac{n}{d}\}$ má $\frac{n}{d}$ prvků.
  Navíc: $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$, právě když $d_2 \mid d_1$, právě když $\frac{n}{d_1} \mid \frac{n}{d_2}$.
- Nechť $G = \langle a \rangle$ je cyklická grupa řádu n.
  Podgrupy v $(G, \cdot)$ jsou tvaru $G^d = \langle a^d \rangle$, kde $d \mid n$. Přitom podgrupa $G^d = \{a^{id}, 1 \leq i \leq \frac{n}{d}\}$ má $\frac{n}{d}$ prvků.
  Navíc: $G^{d_1} \subseteq G^{d_2}$, právě když $d_2 \mid d_1$, právě když $\frac{n}{d_1} \mid \frac{n}{d_2}$.

Cyklické grupy

Tvrzení

Nechť $G = \langle a \rangle$ je cyklická grupa řádu n.

- Každá podgrupa cyklické grupy je cyklická.
- Pro každé $r \mid n$ je v G jediná podgrupa řádu r.
  Je to podgrupa $H_r = \langle b \rangle$, kde $b = a^{\frac{n}{r}}$ je prvek řádu r.
- Nechť H_r je podgrupa řádu r a H_s podgrupa řádu s v G.
  Pak $H_r \subseteq H_s$, právě když $r \mid s$.

Důsledek

- Nechť $G = \langle a \rangle$ je cyklická grupa řádu n.
  Pokud $r \mid n$, pak je v grupě G právě $\varphi(r)$ prvků řádu r.
- Pro Eulerovu funkci platí vzorec: $\sum_{r \mid n} \varphi(r) = n$.

Cyklické grupy

Řešení rovnic $x^k = 1$

Nechť $G = \langle a \rangle$ je cyklická grupa řádu n.

- Pokud $r \mid n$, pak má rovnice $x^r = 1$ právě r řešení v grupě G. Řešením jsou všechny prvky z jediné r-prvkové podgrupy v G, jsou tedy tvaru $x = b^i$, kde $b = a^{\frac{n}{r}}$ je prvek řádu r, $1 \leq i \leq r$.
- Pro libovolné $k \in \mathbb{N}$ má rovnice $x^k = 1$ v grupě G právě $d = \gcd(k, n)$ řešení a redukuje se na rovnici $x^d = 1$.

Důsledek

Pokud je grupa $(\mathbb{Z}_n^*, \cdot)$ cyklická a $n > 2$, pak má rovnice $x^2 = 1$ právě dvě řešení v $\mathbb{Z}_n$ a to $x = \pm 1$.
Poznámka: V $\mathbb{Z}_2$ má rovnice $x^2 = 1$ jediné řešení $x = 1 = -1$.

Cyklické grupy

Příklad

Řešte rovnici $x^{21} = 1$ v grupě $\mathbb{Z}_{19}^*$.

- Už víme, že $|\mathbb{Z}_{19}^*| = \varphi(19) = 18$ a 2 je generátor v $\mathbb{Z}_{19}^*$.
- Prvek a řeší rovnici $x^{21} = 1$ právě, když $\mathrm{r}(a) \mid 21$. Navíc $a \in \mathbb{Z}_{19}^*$, tudíž $\mathrm{r}(a) \mid 18$. Odtud $\mathrm{r}(a) \mid \gcd(21, 18) = 3$ a rovnice se redukuje na rovnici $x^3 = 1$.
- Najdeme prvek b řádu 3: $b = 2^{\frac{18}{3}} = 2^6 = 7$. Rovnice má tři řešení $x_1 = 7$, $x_2 = 7^2 = 11$, $x_3 = 7^3 = 1$.

Cyklické grupy

Tvrzení

Každá grupa prvočíselného řádu je cyklická.

Poznámka

Předchozí tvrzení ale nic neříká o cykličnosti/necykličnosti grup $\mathbb{Z}_n^*$.
Např. grupa $\mathbb{Z}_p^*$ má řád $\varphi(p) = p - 1$, což není prvočíslo!

Strukturou grup $\mathbb{Z}_n^*$ se budeme zabývat na další přednášce.
Prozraďme dopředu tvrzení, které se opírá o fakt, že $\mathbb{Z}_p$ je těleso.

Tvrzení

Pro každé prvočíslo p je grupa $\mathbb{Z}_p^*$ cyklická.

$m-$té mocniny a odmocniny

Tvrzení

Nechť $G = \langle a \rangle$ je cyklická grupa řádu n a nechť $m \in \mathbb{N}$.
Zobrazení $\rho_m : G \to G : x \mapsto x^m$ je grupový homomorfismus.
Nechť $d \mid n$, aneb $n = rd$.

- $Ker\, \rho_d = \{g \in G, g^d = 1\} = \langle a^{\frac{n}{d}} \rangle = \langle a^r \rangle$ a má d prvků.
- $Im\, \rho_d = \{g^d, g \in G\} = \langle a^d \rangle$ a má $\frac{n}{d} = r$ prvků.

Obě podgrupy mají stejnou strukturu, aneb pro $|G| = rd$ je

- $Ker\, \rho_r = Im\, \rho_d$, $Im\, \rho_r = Ker\, \rho_d$.

Pro obecné $m \in \mathbb{N}$ je $\rho_m = \rho_d$, kde $d = \gcd(m, |G|)$.

m−té mocniny a odmocniny

Důsledek

Nechť G je cyklická grupa řádu n a nechť $d \mid n$.
Prvek $b \in G$ je d−tou mocninou ($b = c^d$ pro nějaké $c \in G$), právě když $b^{\frac{n}{d}} = 1$.

Eulerovo kritérium pro $\mathbb{Z}_p^*$

Nechť p je liché prvočíslo.

- Prvek $b \in \mathbb{Z}_p^*$ je čtverec ($b = c^2$), právě když $b^{\frac{p-1}{2}} = 1$.
  V tomto případě má b dvě druhé odmocniny $\pm c$.
- Prvek $b \in \mathbb{Z}_p^*$ je nečtverec ($b \neq c^2$), právě když $b^{\frac{p-1}{2}} = -1$.
- Součin dvou prvků je čtverec, právě když buď oba jsou čtverce nebo oba jsou nečtverce.

m−té mocniny a odmocniny

Důsledek

Nechť p je liché prvočíslo.

- $-1 \in \mathbb{Z}_p^*$ je čtverec, právě když $p \equiv 1 \pmod 4$.
- $-1 \in \mathbb{Z}_p^*$ je nečtverec, právě když $p \equiv 3 \pmod 4$.

Poznámka mimo hru

Komplexní čísla nad $\mathbb{Z}_p$ tvoří těleso, právě když $p \equiv 3 \pmod 4$.
$\mathbb{Z}_p[i] = \mathbb{Z}_p[x]/x^2 + 1$ a polynom $x^2 + 1$ je ireducibilní nad $\mathbb{Z}_p$, právě když nemá kořen v $\mathbb{Z}_p$, tj. právě když -1 je zde nečtverec.

m−té mocniny a odmocniny

Příklad

Grupa $\mathbb{Z}_{19}^*$ má řád 18 a generátorem je $a = 2$.

- Rovnici $x^3 = 1$ řeší $x \in \{2^{6i} = 7^i, 1 \leq i \leq 3\} = \{7, 11, 1\}$.
- Toto jsou právě všechny prvky z $(\mathbb{Z}_{19}^*)^6$.
- Prvek $b = 3$ je nečtverec, neboť $3^9 = -1$ v $\mathbb{Z}_{19}^*$.
- Prvek $b = 5$ je čtverec, neboť $5^9 = 1$ v $\mathbb{Z}_{19}^*$.
  Rovnice $x^2 = 5$ má tedy dvě řešení $x = \pm c$, kde hrubou silou najdeme $c = 9$. Tedy $x_1 = 9$, $x_2 = -9 = 10$.

Konečné grupy

Literatura

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