

(éta: Pro n liché složené je $|L_n| \leq \frac{1}{4} |\mathbb{Z}_n^*|$)

Dоказ: 1) pro $n = p^e$, kde p je prvočíslo, $p > 2$
 \mathbb{Z}_{p^e} je cyklická, proto $L_n = K_n \Rightarrow |L_n| = |K_n|$

$$L_n = K_n = \{a \in \mathbb{Z}_{p^e}^*, a^{n-1} = 1\}$$

Chceme zjistit, kolik řešení má rovnice $x^{n-1} = 1$ v \mathbb{Z}_{p^e} .

Počet řešení je $\gcd(n-1, |\mathbb{Z}_{p^e}|) = d$, rovnice se redukuje: $x^d = 1$, všechna řešení leží v Pd , kde Pd je jediná d -pruková podgrupa.

$$\gcd(n-1, |\mathbb{Z}_{p^e}|) = \gcd(p^e-1, \varphi(p^e)) = p^{e-1}(p-1) = \gcd(p^e-1, p^{e-1}(p-1))$$

Dalo by se namířit když $(p-1)/(p^{e-1})$

$$p^{e-1} = (p-1)(p^{e-1} + p^{e-2} + \dots + p + 1) \quad \leftarrow \text{platí třeba?}$$

$$\begin{aligned} &\left(\begin{array}{l} \text{nasobíme } p \times \text{závorku: } p^{e-1} + p^{e-2} + \dots + p \\ \text{nasobíme } (-1) \times \text{závorku: } -p^{e-1} - p^{e-2} - \dots - p-1 \end{array} \right) \text{ sečteme, dostaneme } p^{e-1} \end{aligned}$$

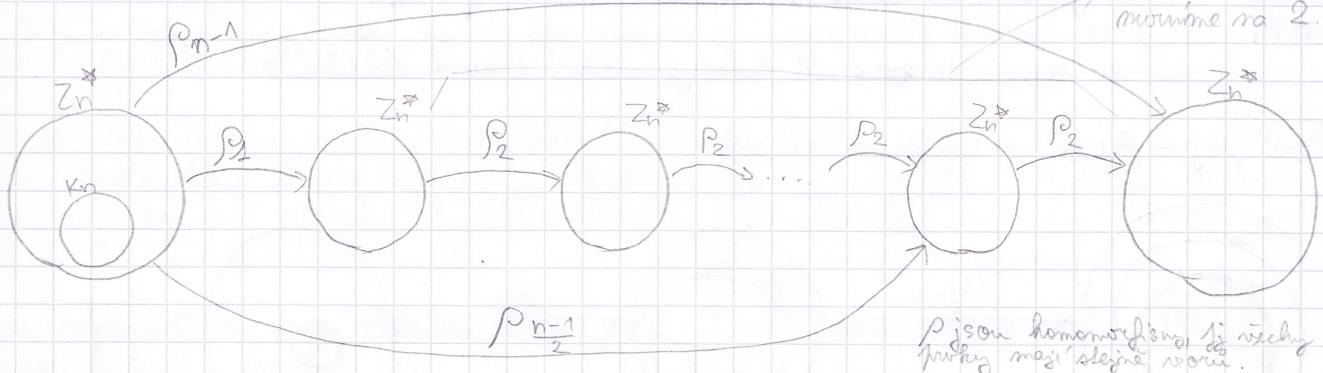
Oto, tento vztah skutečně platí, proto $\gcd(p^{e-1}, p^{e-1}(p-1)) = p-1 = d$

$$|L_n| = |K_n| = p-1 \quad \frac{|L_n|}{|\mathbb{Z}_n^*|} = \frac{p-1}{p^{e-1}(p-1)} = \frac{1}{p^{e-1}} \leq \frac{1}{p} \leq \frac{1}{4} \quad \text{pro } p \neq 3 \rightarrow p^e > 3^2 = 9$$

2) pro $m = \prod_{i=1}^r p_i^{e_i}$, $p_i > 2$, p_i jsou prvočísla, r je jejich počet, $r \geq 2$

Nejdříve provedeme sčátky dleží důkaz, aby chom pochopili princip.

celkem h -krát
mocniny na 2.



Gulerova věta rovnou mocniny $n-1$, tj. chová se stejně jako horní skok, proto vlastně $K_n = \text{Ker } P_{n-1}$. Kolik mocniny postupně, nějaké výšky vystoupíme, takže víme, že $L_n \subseteq K_n$.

Budeme pracovat s posledním P_2 , tj. nejdříve udeříme $P_{\frac{n-1}{2}}$.
 Po libovolné $a \in K_n$ bude:

$$\left(a^{\frac{n-1}{2}}\right)^2 = 1, \text{ tj. } a^{\frac{n-1}{2}} \in \text{Ker } P_2$$

Na kolik různých způsobů v \mathbb{Z}_n^* se dokážeme s K_n dostat? Budou jich nejméně $|\text{Ker } P_2|$,

tj. počet řešení $x^2 = 1$ v \mathbb{Z}_n^* .

CRT námí, že $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^e}^* \times \dots \times \mathbb{Z}_{p_r^e}^*$, a $\mathbb{Z}_{p_i^e}^*$ jsou cyklické, tj. v každé je řešení $\{\pm 1\}$.
 \Rightarrow v \mathbb{Z}_n^* bude 2^r řešení, diskutujeme jí jako $x \leftrightarrow \{\pm 1, \pm 1, \dots, \pm 1\}$, a tato řešení lze zapsat jako $\{\pm 1, \pm a, \pm b, \dots\}$.

krát

L_n musí mít několik podmožitních prvků, které se v $P_{\frac{n-1}{2}}$ obrací na ± 1 . Konkrétně obsahuje celý rovnou $p-1$ a část rovnou pro 1.

$$\frac{|L_n|}{|K_n|} \leq \frac{\text{(2) počet možn. v } P_{\frac{n-1}{2}}}{\text{(2) počet možn. v } P_{\frac{n-1}{2}}} = \frac{2}{2^r} = \frac{1}{2^{r-1}} < \frac{1}{2}$$

$\Rightarrow K_n$ má 2^r "různy"

$\Rightarrow L_n$ bude jen 1 a -1, tedy dva různou

prostředí $r \geq 2$

Kdyby vše platilo, tak je hoso, protože $|L_n| \leq \frac{1}{2} |K_n| \leq \frac{1}{2} \cdot \frac{1}{2} |\mathbb{Z}_n^*| = \frac{1}{4} |\mathbb{Z}_n^*$, ale n nesmí být Carmichaelovo.

v rozkladu jsou všechny pi reditelné

Při n Carmichaelovo: $n = p_1 \cdot p_2 \cdots p_r$, je square free, $r \geq 3$.

Tento důkaz byl špatně. Proč? Co když se to něco spojí mnohem déle, a v předposledním \mathbb{Z}_n^* mám jen $\{1\}$ a zádaď další výsledky, když ne celé jádro posledního čtvrtce.

Musím najít, kde ještě všechny vory jsou:

- a) aspoň na jedničku β_2 to bude - nemůže, aby K_n^r pro libké r se celé sobcvičilo na jedničku. Nejdnuje to pro -1 , $(-1)^r = -1$, kdežto mívá $\text{Im } \beta_2 \neq \{1\}$.
- b) hledáme hladiru, kde $\beta_{1,2,g}$ (tj máme g čtvrtce), aby těsně předtím byly pokryty všechny \mathbb{F}_1 .

$$\text{Ker } \beta_2 \subseteq \beta_{1,2,g^{-1}}(K_n)$$

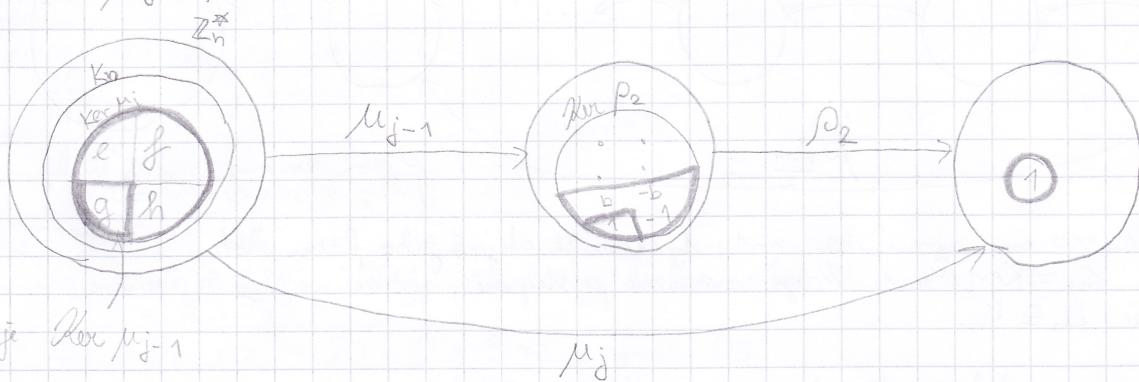


Zde uvažujeme, že když vyhovuje $g = \min\{h, h_1, h_2, \dots, h_m\}$, kde: $|\mathbb{Z}_{p_i^{e_i}}^*| = \varphi(p_i^{e_i}) = 1 \cdot 2^{e_i}$.

Přednáška
25.4.2019 Pokračujeme v důkazu a minula: $|L_n| \leq \frac{1}{4} |\mathbb{Z}_n^*$

V jaké hladině čtvrtcování je umístěn naš obrazek, který jsme mylně umístili až na konec čtvrtcování? Existuje některá taková hladina?

Definujme $\mu_j = \beta_{1,2,g} \approx \text{umocnění na } 12^j$



Uvídíte plati $\text{Ker } \beta_{1,2,g} \subseteq K_n$, to je jako včera.

Když po $j-1$ čtvrtcích padla 1, tak tam sestane i po j čtvrtcích: $\text{Ker } \mu_{j-1} \subseteq \text{Ker } \mu_j \subseteq K_n$

Uvídíte vše, co se po μ_j dostalo na jedno, ale podíváme se na to o μ_{j-1} , kdežto se dostane me na odmocninu z jedné. Protože μ_{j-1} je grupový homomorfismus, proto když \mathbb{F}_1 má stejně mnoho voriů pro 1, a těch je 1 $\text{Ker } \mu_{j-1}$.

$\text{Ker } \mu_j$ se rozdělí na kříd podle podgrupy $\text{Ker } \mu_{j-1}$:

$$g: \text{Ker } \mu_{j-1}, \text{ tj } \mu_{j-1}(g) = 1$$

$$b: \mu_{j-1}(b) = b$$

$$f: \mu_{j-1}(f) = -b$$

$$h: \mu_{j-1}(h) = -1$$

Náš kříd pojíma, kolik \mathbb{F}_1 je obrazem μ_{j-1} , tj na kolik kříd (písmenek e, f, g, b, ...) můžu rozdělit $\text{Ker } \mu_j$. Upočítá se to tak, že zjistíme, kolik má $\text{Ker } \mu_j$ kříd podle podgrupy $\text{Ker } \mu_{j-1}$, tj kolikrát je $\text{Ker } \mu_j$ větší než $\text{Ker } \mu_{j-1}$.

Jak vypadá $\ker \mu_j$?
 $a \in \ker \mu_j \iff a^{\frac{1}{2^j}} = 1 \iff \mathbb{Z}_n^* \cong \mathbb{Z}_{p_1}^{*} \times \dots \times \mathbb{Z}_{p_r}^{*}, r \geq 2$, kde $\mathbb{Z}_{p_i}^{*}$ jsou cyklické.

Jak to vypadá $\ker \mu_j$ je jednotlivých $\mathbb{Z}_{p_i}^{*}$? Resíme rovnici $x^{\frac{1}{2^j}} = 1$, redukujeme ji: (indexy i svedom)

$$\text{Oznáme } \varphi(p^e) = \varphi(2^h), \text{ kde } h \text{ je liché číslo, pak:} \\ \gcd(\varphi(2^h), \varphi(p^e)) = \gcd(\varphi(2^h), \varphi(2^r)) = \gcd(\varphi(2^h), 2^{\min\{h, r\}}) = \frac{\varphi(2^h)}{2^{\min\{h, r\}}}$$

$$\text{Celkově pak } \ker \mu_j = \prod_{i=1}^r d_i \cdot 2^{\min\{h_i, j\}} = d \cdot \prod_{i=1}^r 2^{\min\{h_i, j\}} = \\ = d \cdot \prod_{i=1}^r 2^j = d \cdot (2^j)^r = d \cdot 2^{jr}$$

Zvolili jsme $j \leq \min\{h_1, \dots, h_r, h\}$, $j \leq h$ platí následující, protože $a^{n-1} = a^{1 \cdot 2^h}$

Jak vypadá $\ker \mu_{j-1}$?

$$\text{Pokud } j \leq h_i, \text{ tak platí } |\ker \mu_j| = d_i \cdot 2^j = 2 \cdot (d_i \cdot 2^{j-1}) = 2 \cdot |\ker \mu_{j-1}|$$

$$\text{Tedy když } j \leq \min\{h_1, \dots, h_r, h\}, \text{ pak: } |\ker \mu_j| = d \cdot (2^j)^r = d \cdot 2^{jr} = d \cdot 2^{r(j-1)} \cdot 2^r =$$

V tomto případě má μ_{j-1} ($\ker \mu_j$) pokryje 2^r odmocin, tedy všechny:

$$\sqrt[2^r]{1} \leftarrow (\underbrace{\pm 1, \pm 1, \dots, \pm 1}_{r \text{ krát}}). \text{ Když někde bylo } j > h_i, \text{ tak by nám } \pm 1 \text{ mohla jít 1, takže bychom nějaké } \sqrt[2^r]{1} \text{ strávili.}$$

Máme se dat, že nám nějaký falešný svědku máte? Takhle ovědkové musí být na racionalu v jádru, protože obecně je na \mathbb{Z}_n^* (přes -1). Tore, co jede na 1 , je v jádru. Jak uvidíme odkazat P_2 , budou nám postupně užívat -1 . Jakmile miní první -1 v $\mathbb{Z}_{p_i}^*$, smíří i -1 v \mathbb{Z}_n^* , protože $-1 \leftrightarrow (-1, -1, -1, \dots, -1)$.

Máme odpověď na první otázku: Kdy (jednou všechny) budou pokryty všechny $\sqrt[2^r]{1}$?
 Budou pokryty pro $j \leq \min\{h_1, \dots, h\}$.

Odpověď 2: Kde je L_n ? Po kolika čtvrticích chybají na 1 ?

Těž v L_n je na 1 přes -1 , ale -1 je první $\sqrt[2^r]{1}$, která přestane být pokryta, jakmile máme nějaký $i: j > h_i$. Dovolme $g = \min\{h_1, \dots, h_r, h\}$. Tj. $L_n \subseteq \ker \mu_g$, $L_n \subseteq \{ \text{záporné pro } 1 \text{ a } -1 \}$. Tedy máme kladnou g , když minulé čísla jsou díky s minula

$$\Rightarrow L_n \subseteq \frac{2^r}{2^r} |\ker \mu_g| \subseteq \frac{1}{2^{r-1}} |K_n|$$

Poznámka k důkazu: Odhad $|L_n| \leq \frac{1}{4} |\mathbb{Z}_n^*|$ je velmi hureš, falešných mědiček málo. **Cvičení**
 lze většinou mnohem méně
 25.4.2019

Př: $n = 6545 = 5 \cdot 7 \cdot 11 \cdot 17$. Odhadněte počet falešných mědiček pro EM i MR test.

$$\varphi(n) = \dots = 3840$$

$$|K_n|: \text{Resum } \times 6545^{\frac{1}{2^{r-1}}} = 1 \iff \mathbb{Z}_{6545}^*$$

$$\begin{aligned} &\sim \mathbb{Z}_5^*: \gcd(6544, 45) = \gcd(6544, 4) = 4 \\ &\sim \mathbb{Z}_7^*: \gcd(6544, 6) = 2 \\ &\sim \mathbb{Z}_{11}^*: \gcd(6544, 10) = 2 \\ &\sim \mathbb{Z}_{17}^*: \gcd(6544, 16) = 6 \end{aligned}$$

$\rightarrow 4$ řešení
 $\rightarrow 2$ řešení
 $\rightarrow 2$ řešení
 $\rightarrow 6$ řešení

$$|K_n| = 4 \cdot 2 \cdot 2 \cdot 16 = 256$$

Fermatov - test má 256 falešných svědků.

Uděláme hrubý odhad: $|L_n| \leq \frac{1}{4} |\mathbb{Z}_n^*| = \frac{3840}{4} = 960$

Zkoušme lepší odhad: $|L_n| \leq \frac{1}{2^{r-1}} \cdot |K_n| = \frac{1}{23} \cdot 256 = \frac{256}{8} = 32$, to je lepší odhad

Uzmíme ještě lepší odhad: $|L_n| \leq \frac{1}{2^{r-1}} \cdot |\text{Ker } \mu_g|$

$$\begin{aligned} n-1 &= 6544 = 2^4 \cdot 409 \\ |\mathbb{Z}_5^*| &= 4 = 2^2 \cdot 1 & h_1 &= 4 \\ |\mathbb{Z}_7^*| &= 6 = 2^1 \cdot 3 & h_2 &= 2 \\ |\mathbb{Z}_{11}^*| &= 10 = 2^1 \cdot 5 & h_3 &= 1 \\ |\mathbb{Z}_{17}^*| &= 16 = 2^4 \cdot 1 & h_4 &= 4 \end{aligned} \quad \left. \begin{array}{l} h_1 = 2 \\ h_2 = 1 \\ h_3 = 1 \\ h_4 = 4 \end{array} \right\} g = \min \{h_i : h_i \geq 1\} \Rightarrow \mu_g = \rho_{409 \cdot 2}$$

Najdeme $\rho_{409 \cdot 2}$: řešme $x^{409 \cdot 2^1} = x^{818} = 1 \pmod{2^n}$
 $\gcd(409 \cdot 2, |\mathbb{Z}_5^*|) = 2$, redukuje se to na $x^2 = 1$

(protože 409 je prvočíslo, a všechny velikosti \mathbb{Z}_p^* jsou sude, lze
sudé \gcd nerozložit a tříma komise se redukovat na $x^2 = 1$).

Řešení je $x \leftrightarrow \{\pm 1, \pm i, \pm j, \pm k\}$, celkem je 16 různých řešení, tj. $|\text{Ker } \rho_{409 \cdot 2}| = 16$

$$|L_n| \leq \frac{|\text{Ker } \mu_g|}{2^{r-1}} = \frac{16}{8} = 2, \text{ ve skutečnosti jsou falešná vzdělkové pouze dva, a to 1 a -1, které lyčkou stejně nebořeli.}$$