Míjení involucí. Toto je technická pasáž, jejíž užitečnost vyvstane v souvislosti s Rabinovým-Millerovým testem prvočíselnosti. Můžete se tedy k ní vrátit teprve později.

Řekneme, že prvky a a b nějaké konečné grupy $(G, \cdot)$ se *míjejí* v grupě G, pokud

- a neleží v podgrupě generované b a
- b neleží v podgrupě generované a.

Jinak řečeno, neexistuje žádné $i \in \mathbb{Z}$ takové, že $a^i = b$ nebo $b^i = a$.

Involuce je prvek řádu dva. Všimněme si, že cyklická grupa $\mathbb{Z}_n$, kde n je sudé, obsahuje právě jednu involuci, a to $\frac{n}{2}$. Pro n liché neexistuje v $\mathbb{Z}_n$ žádná involuce.

Nás bude speciálně zajímat kolik prvků grupy

$$G = \mathbb{Z}_{2^{e_1}} \times \cdots \times \mathbb{Z}_{2^{e_r}}$$

se míjí s involucí

$$e = (2^{e_1-1}, \ldots, 2^{e_r-1}).$$

Uvědomme si nejprve některé vlastnosti okruhu $\mathbb{Z}_{2^k}$. Invertibilní prvky jsou právě všechna lichá čísla. Násobení lichým číslem je tedy automorfismus grupy $(\mathbb{Z}_{2^k}, +)$ a prvky se stejnou 2-valuací jsou asociované. Neformálně řečeno, dělitelnost prvků závisí pouze na jejich 2-valuaci, nikoli na "liché složce".

Zejména platí, že řád prvku a je roven $2^{k-\mathrm{val}_2(a)}$. Počet nenulových prvků, pro které $\mathrm{val}_2(a) = s$, je přitom 2^{k-s-1} (2-valuace nuly je nejasná, z definice je ∞). To je vidět např. z toho, že tyto prvky generují stejnou cyklickou grupu řádu 2^{k-s} (podgrupa daného řádu je v cyklické grupě vždy jen jedna), v níž je každý druhý prvek generátorem.

Pro $\mathbb{Z}_{16}$ např. máme:

val_2	řád	počet prvků	prvky
∞	1	1	0
3	2	$1 = \frac{1}{16}\lvert\mathbb{Z}_{16}\rvert$	8
2	4	$2 = \frac{1}{8}\lvert\mathbb{Z}_{16}\rvert$	4,12
1	8	$4 = \frac{1}{4}\lvert\mathbb{Z}_{16}\rvert$	2,6,10,14
0	16	$8 = \frac{1}{2}\lvert\mathbb{Z}_{16}\rvert$	1,3,5,7,9,11,13,15

Obecně, pro $\mathbb{Z}_{2^e}$ je

val_2	řád	počet prvků
∞	1	1
s	2^{k-s}	$2^{k-s-1} = \frac{1}{2^{s+1}}\lvert\mathbb{Z}_{2^e}\rvert$

Tvrzení. Nechť $r \geq 2$.

- Pokud $r = 2$ a $e_1 = e_2$, pak je nejvýše $\frac{1}{2}|G|$ prvků grupy G, které se nemíjejí s e (asymptoticky je jich $\frac{1}{3}|G|$).
- V ostatních případech je nejvýše $\frac{1}{4}|G|$ prvků grupy G, které se nemíjejí s e.

Důkaz. Všechny prvky jsou řádu mocniny dvojky. Nechť je tedy $a = (a_1, \ldots, a_r)$ prvek řádu 2^t, pro který platí $2^{t-1} \cdot a = e$. Z toho je vidět, že pro všechna $i = 1, \ldots, r$ je řád prvku a_i v $\mathbb{Z}_{2^{e_i}}$ stejný, a to právě 2^t.

Můžeme nyní přesně vyčíslit kolik je prvků, které "trefují" e. Pro každé $1 \leq t \leq \min\{e_1, \ldots, e_r\}$ existuje právě $(2^{t-1})^r$ prvků řádu 2^t; navíc nula. Označíme-li tedy $h = \min\{e_1, \ldots, e_r\}$, je hledaných prvků

$$1 + \sum_{j=0}^{h-1} (2^r)^j = \frac{2^{rh} - 1}{2^r - 1} + 1.$$

Velikost grupy je

$$2^{\sum_{i=1}^{r} e_i},$$

což je nejméně 2^{rh}, takže podíl prvků trefujících e je nejvýše

$$\frac{1}{2^r - 1} + \frac{1}{2^{rh}} - \frac{1}{(2^r - 1)2^{rh}}$$

Pro $r = 2$ dostáváme podíl těchto prvků v grupě G

$$\frac{1}{3} + \frac{2}{3 \cdot 4^h},$$

což je v nejhorším možném případě $h = 1$, tedy v grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$, přesně $\frac{1}{2}$.

Pro $r = 3$ a $h = 1$, tedy pro grupu $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, dostáváme $\frac{1}{4}$.

Pro rostoucí r i h se poměr zmenšuje. Uvědomme si konečně, že pokud $e_i > h$, roste velikost grupy (exponenciálně s $e_i - h$) a počet prvků zasahujících involuci se nemění. □

Fermatův a Wilsonův test. Abychom mohli testovat, zda dané číslo je prvočíslo, potřebujeme vlastnosti, které prvočísla splňují, ale složená čísla nikoli. Jedním z kandidátů je *Malá Fermatova věta*:

Tvrzení. Pokud je n prvočíslo, platí

$$a^{n-1} \equiv 1 \mod n,$$

pro každé $1 \leq a \leq p - 1$.

Pokud n složené není a rovnost přesto platí pro nějaké a, řekneme, že n je (Fermatovo) pseudoprvočíslo v bázi a. Prvek a se také někdy nazývá (Fermatův) *lhář* pro n. V opačném případě říkáme, že a je pro n (Fermatův) *svědek*. Pro Carmichaelova [čti: karmajkl] čísla jsou všechna a lháři.

Jiná charakteristika, výpočetně nepoužitelná, je Wilsonova věta.

Rabinův-Millerův test. Tento test je pro praxi nejdůležitější.

Pozorování. $\mathbb{Z}_p^*$ obsahuje jedinou involuci, a to -1.

To plyne z cykličnosti $\mathbb{Z}_p^*$ nebo také z toho, že

$$a^2 \equiv 1 \mod p \quad \text{implikuje} \quad p \mid a^2 - 1 = (a + 1)(a - 1).$$

Nechť je $p - 1 = 2^e m$, kde m je liché. Platí $a^{2^e m} \equiv 1 \mod p$. Buď je

- $a^m \equiv 1 \mod p$,

nebo najdeme postupným odmocňováním nejmenší $j \in \{0, \ldots, e - 1\}$ takové, že $a^{2^{j+1} m} \equiv 1 \mod p$. Protože pak $a^{2^j m}$ je involuce, máme

- $a^{2^j m} \equiv -1 \mod p$.

Je-li n složené a pro nějaké a platí jedna z výše uvedených možností, řekneme, že a je *silný* lhář pro n nebo že n je *silné pseudoprvočíslo* v bázi a. *Silný* svědek je takové a, pro které ani jedna z uvedených podmínek neplatí. To znamená, že buď $a^{n-1} \not\equiv 1 \mod n$ (pak je a i Fermatův svědek), nebo je $a^m \not\equiv \pm 1 \mod n$ a jedničku dostaneme postupným umocňováním na druhou, aniž bychom narazili na -1 (tj. našli jsme jinou involuci než -1).

Nechť n je nadále **liché** složené číslo. Budeme zkoumat vlastnosti silných lhářů, abychom dokázali, že jich není příliš mnoho.

Všimněme si nejprve, že každý lhář a musí splňovat

- $a \in \mathbb{Z}_n^*$ a
- řád a dělí $n - 1 = 2^e m$.

Oboje plyne z $a^{n-1} \equiv 1 \mod n$.

Je užitečné si všimnout, že řád prvku $(a_1, a_2, \ldots, a_r)$ grupy $H_1 \times H_2 \times \cdots \times H_r$ je roven nejmenšímu společnému násobku řádů a_i, $i = 1, \ldots, r$.

1. *První případ*: $p^2 \mid n$, pro nějaké prvočíslo p.

Nechť $k = \mathrm{val}_p(n)$. Pak

$$\mathbb{Z}_n \cong \mathbb{Z}_{p^k} \times H,$$

a

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p^k}^* \times H^*,$$

kde H je grupa odpovídající ostatním prvočíslům. Díky znalosti $\mathbb{Z}_{p^k}^*$ můžeme dále psát

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{k-1}} \times H^*.$$

(Všimněme si, že první dvě grupy posledního direktního součinu jsou aditivní, ta třetí multiplikativní.)

Předpokládejme nyní, že a je lhář. Jak bylo řečeno, musí a ležet v $\mathbb{Z}_n^*$. Nechť poslední uvedený isomorfismus zobrazuje $a \mapsto (x, y, z)$. Předpokládejme, že $y \neq 0$. Pak je řád y, a tedy i řád a, dělitelný p. Protože p nedělí $n - 1$, ani řád a nedělí $n - 1$, a tedy a není lhář, spor. Musí tedy být $y = 0$ a lhářů je nejvýše $(p-1) \cdot |H^*|$. Snadno ověříme, že $4(p-1) < p^k$ pro každé $p \geq 3$ a $k \geq 2$. Lhářů je tedy nejvýše

$$\frac{1}{4} p^k |H^*| < \frac{1}{4} |\mathbb{Z}_n|.$$

2. *Druhý případ*: $n = p_1 p_2 \cdots p_r$, kde $r \geq 2$ a p_i jsou prvočísla. Z Čínské věty o zbytcích máme

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$$

a platí

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*,$$

přičemž tento poslední isomorfismus můžeme zvolit jako restrikci toho předešlého (restrikci na podmnožinu a pouze na operaci násobení). Potom speciálně platí

$$-1 \mapsto (-1, \ldots, -1).$$

Opět můžeme rozepsat do aditivní notace takto:

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1 - 1} \times \cdots \times \mathbb{Z}_{p_r - 1}.$$

Protože -1 je jediná involuce v $\mathbb{Z}_{p_1}^*$, a $\frac{p_1 - 1}{2}$ je jediná involuce v $\mathbb{Z}_{p_1 - 1}$, máme pro posledně uvedený isomorfismus

$$-1 \mapsto \left(\frac{p_1 - 1}{2}, \ldots, \frac{p_r - 1}{2}\right).$$

Položme $e_i = \mathrm{val}_2(p_i - 1)$ a $p_i - 1 = 2^{e_i} m_i$. Pak $\mathbb{Z}_{p_i-1} \cong \mathbb{Z}_{2^{e_i}} \times \mathbb{Z}_{m_i}$, kde jediná involuce je $(2^{e_i-1}, 0)$, jak se snadno nahlédne. Označíme-li $M = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$, dostáváme

$$\alpha : \mathbb{Z}_n^* \cong \mathbb{Z}_{2^{e_1}} \times \cdots \times \mathbb{Z}_{2^{e_r}} \times M,$$

kde M je lichého řádu. Z předchozích úvah o involucích máme pro poslední isomorfismus (který jsme označili α)

$$\alpha : -1 \mapsto (2^{e_1-1}, \ldots, 2^{e_r-1}, 0); \quad 1 \mapsto (0, \ldots, 0, 0).$$

Číslo $a \in \mathbb{Z}_n^*$ je tedy lhář, právě když pro $\alpha(a) = (a_1, \ldots, a_r, a_{r+1})$ platí

$$\begin{aligned} m(a_1, \ldots, a_r, a_{r+1}) &= (0, \ldots, 0, 0), \quad \text{nebo} \\ 2^j m(a_1, \ldots, a_r, a_{r+1}) &= (2^{e_1-1}, \ldots, 2^{e_r-1}, 0) \quad \text{pro nějaké } j. \end{aligned}$$

To můžeme rozepsat do dvou podmínek (pro sudou a lichou část rozkladu):

- řád a_{r+1} dělí m
- $(a_1, \ldots, a_r)$ nemíjí involuci $(2^{e_1-1}, \ldots, 2^{e_r-1})$.

Víme, že druhou podmínku splňuje, s výjimkou případu $r = 2$ a $e_1 = e_2$, nejvýše $\frac{1}{4}$ prvků. Opět tedy dostáváme, že lhářů je nejvýše

$$\frac{1}{4}|\mathbb{Z}_n^*| < \frac{1}{4}|\mathbb{Z}_n|.$$

2. *Zvláštní případ*: $n = p_1 p_2$, $\mathbb{Z}_{p_i}^* \cong \mathbb{Z}_{2^k} \times \mathbb{Z}_{m_i}$, tedy $p_i - 1 = 2^k m_i$, $i = 1, 2$, pro nějaké k. V tomto případě splňuje druhou podmínku až $\frac{1}{2}$ prvků. Ukážeme tedy navíc, že grupa M, tj. $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, obsahuje málo prvků, jejichž řád dělí m. Budeme tak moci využít první z výše uvedených vlastností lháře.

Tvrzení. Buď m_1 nebo m_2 nedělí m.

Důkaz. Z

$$2^e m + 1 = n = p_1 \cdot p_2 = (2^k m_1 + 1) \cdot (2^k m_2 + 1)$$

dostáváme

$$2^e m = 2^{2k} m_1 m_2 + 2^k m_1 + 2^k m_2.$$

Odsud vidíme, že pokud by m_1 i m_2 dělilo m, budou se m_1 a m_2 dělit navzájem. To však není možné, neboť předpokládáme $p_1 \neq p_2$. □

Uvažujme nyní všechny prvky $c \in M$, jejichž řád dělí m. To znamená $mc = 0$, a je tedy zřejmé, že tyto prvky tvoří podgrupu C grupy M. Grupa M obsahuje nejméně jeden prvek, jehož řád nedělí m, jak plyne z výše uvedeného tvrzení (prvek $(1, 0) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ má řád m_1 a prvek $(0, 1)$ řád m_2). C je tedy vlastní podgrupa a její velikost dělí velikost M. Protože M je lichého řádu $m_1 m_2$, je $|C|$ nejvýše $\frac{1}{3}|M|$.

Obě podmínky pro lháře tedy splňuje nejvýše

$$\frac{|\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}|}{2} \cdot \frac{|\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}|}{3} = \frac{|\mathbb{Z}_n^*|}{6} < \frac{|\mathbb{Z}_n|}{6}$$

prvků.