13. Z teorie čísel

(zapsali L. Banáková, O. Hoferek, J. Břečka)

Na této přednášce se budeme zabývat různými problémy okolo teorie čísel. Zopakujme si některé ze základních pojmů:

- $a \setminus b$ (a dělí b) $\Leftrightarrow \exists c : b = a \cdot c$.
- $\gcd(a, b)$ je označení největšího společného dělitele čísel a a b.
- $a \equiv_n b \Leftrightarrow n \perp (a - b)$ (nebo také $a \bmod n = b \bmod n$).
- $a \perp b$ (a a b jsou nesoudělná) $\Leftrightarrow \gcd(a, b) = 1$.

Dále si zopakujeme, jakou časovou složitost mají základní operace s čísly, které budeme potřebovat. Pro N-bitová čísla:

- $a + b$, $a - b \ldots \mathcal{O}(N)$
- $a * b$, a/b, $a \bmod b \ldots \mathcal{O}(N^2)$
- $\gcd(a, b) \ldots \mathcal{O}(N^3)$

Definice: *Komutativní (Abelovská) grupa* je čtveřice $(G, \cdot, 1, ^{-1})$, kde G je nosná množina prvků, $\cdot$ je binární operace $G^2 \to G$, 1 je prvkem G, $^{-1}$ je unární operace $G \to G$ a platí následující axiomy:

1. $\cdot$ je komutativní a asociativní
2. $\forall a \in G : a \cdot 1 = a$
3. $\forall a \in G : a \cdot a^{-1} = 1$

Zkusme si pro následujících několik kandidátů určit, zda jsou komutativními grupami:

- $(\mathbb{Z}, +, 0, -x)$ (sčítání na množině celých čísel, nula a změna znaménka) je komutativní grupa.
- $(\mathbb{Z}_n, + \bmod n, 0, -x)$ ($\mathbb{Z}_n = \{0, \ldots, n-1\}$, sčítání modulo n) je komutativní grupa, navíc konečná.
- $(\mathbb{Q} - \{0\}, *, 1, 1/x)$ (násobení nad racionálními čísly) je komutativní grupa.
- $(\mathbb{Z}_n - \{0\}, * \bmod n, 1, ?)$ (násobení modulo n) nemusí být vždy grupa, protože se nám nepovede vždy najít inverzní prvek. (např. pro $n = 4$ neexistuje inverzní prvek pro dvojku).
- (permutace na $\{1, \ldots, n\}, \circ, \mathrm{id}, ^{-1}$) (permutace se skládáním a inverzní permutací) je grupa, ale není komutativní.

Definice: $(H, \cdot, 1, ^{-1})$ je *podgrupa* grupy $(G, \cdot, 1, ^{-1})$ právě tehdy, pokud $H \subseteq G$ a H je grupa.

Příkladem podgrupy může být $(2 * \mathbb{Z}_n, + \bmod n, 0, -x) \subseteq (\mathbb{Z}_n, + \bmod n, 0, -x)$ (grupa tvořená jen sudými čísly).

Věta (Lagrangeova): Pokud H je podgrupa G, pak počet prvků G je dělitelný počtem prvků H.

Definice: Umocňování prvků grupy definujeme takto: $x^0 = 1$, $x^{n+1} = x^n \cdot x$.

Definice: Grupa G je *cyklická* právě tehdy, pokud $\exists g \in G : g^0, g^1, \ldots = G$. Pak g je *generátor* grupy G.

- $(\mathbb{Z}, +, 0, -x)$ není cyklická.
- $(\mathbb{Z}_n, + \bmod n, 0, -x)$ je cyklická, $g = 1$.
- $(\mathbb{Q}, \ldots)$ není cyklická.

Definice: *Multiplikativní grupa modulo n* je grupa $\mathbb{Z}_n^* = (\{x \mid 1 \leq x < n$ a zároveň $\exists y : xy \equiv_n 1\}, * \bmod n, 1, ^{-1})$

Multiplikativní grupa $\mathbb{Z}_n^*$ obsahuje pouze invertibilní prvky. Snadno lze nahlédnout, že toto je opravdu grupa, pokud ověříme, že množina prvků je uzavřená na násobení:

$x_1, x_2 \in \mathbb{Z}_n^* \Rightarrow \exists y_1, y_2 \in \mathbb{Z}_n^* : x_1 y_1 \equiv_n 1, x_2 y_2 \equiv_n 1$

$x \equiv_n x_1 x_2, y \equiv_n y_1 y_2 \ldots xy \equiv_n x_1 x_2 y_1 y_2 \equiv_n 1 \cdot 1 = 1 \Rightarrow$ množina je uzavřená vzhledem k operaci $* \bmod n$.

Otázkou zůstavá, jak najít tyto invertibilní prvky v $\mathbb{Z}_n$. Předpokládejme nejprve, že n je prvočíslo. Pomůžeme si větou, kterou dokážeme později.

Věta (Malá Fermatova): Pro každé prvočíslo n a každé číslo a, které je nesoudělné s n, platí: $a^{n-1} \equiv_n 1$.

Pokud je tedy n prvočíslo, tak z *Malé Fermatovy věty* vyplývá, že invertibilní jsou všechny prvky $1, \ldots, n-1$. Snadno totiž nahlédneme, že $\forall a \in \mathbb{Z}_n$ platí $a^{-1} \equiv_n a^{n-2}$, protože $a \cdot a^{-1} \equiv_n 1 \equiv_n a^{n-1} \equiv_n a \cdot a^{n-2}$. Jak to však bude s n, která nejsou prvočísla? Invertibilní jsou prvky $a \in \mathbb{Z}_n$, pro které existuje $x \in \mathbb{Z}_n$ tak, že $a \cdot x \equiv_n 1$. Jejich zkoumání začneme následující větou:

Věta: Rovnice $a \cdot x \equiv_n b$ má řešení pro $a, b, n \in \mathbb{Z} \iff g = \gcd(a, n) \perp b$. Navíc existuje algoritmus s časovou složitostí $\mathcal{O}(N^3)$, který řešení najde.

Důkaz: Rovnice $a \cdot x \equiv_n b$ je ekvivalentní s rovnicí $a \cdot x - n \cdot y = b$.

„$\Rightarrow$“: Dokážeme sporem. $g \setminus a \cdot x$ a $g \setminus n \cdot y \Rightarrow g \setminus a \cdot x - n \cdot y$. Zároveň však platí g nedělí b, což vede ke sporu.

„$\Leftarrow$“: Pokud $b = g$, pak lze úlohu hledání x, y řešení rovnice $a \cdot x - n \cdot y = g$ převést na Eukleidův algoritmus. V Eukleidově algoritmu se vstupem (x, y) jsou totiž všechny mezivýsledky i konečný výsledek lineární kombinace typu $\alpha \cdot x - \beta \cdot y$. Pokud $b = k \cdot g$, pak najdeme x_0, y_0 taková, že $a \cdot x_0 - n \cdot y_0 = g$. Pro $x = k \cdot x_0$ a $y = k \cdot y_0$ pak platí $a \cdot x - n \cdot y = b$. ♡

Z předchozí věty vyplývá, že invertibilní jsou právě taková $a \in \mathbb{Z}_n$, která jsou nesoudělná s n. Zbývá už jenom určit, jak vypadají prvky k nim inverzní.

Definice: *Eulerova funkce* $\varphi(n) = |\{x \mid 1 \leq x < n$ a zároveň $x \perp n\}|$.

Pozorování: *(vlastnosti Eulerovy funkce)*

- Je-li n prvočíslo, pak $\varphi(n) = n - 1$.
- $\varphi(n^k) = (n-1) \cdot n^{k-1}$.
- Pro $a \perp b$ platí $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
- $|\mathbb{Z}_n^*| = \varphi(n)$.

Věta (Eulerova): Pro každá dvě přirozená čísla n a a nesoudělná platí: $a^{\varphi(n)} \equiv_n 1$.

Důkaz: Uvažme posloupnost $a^0, a^1, a^2, \ldots$. V této posloupnosti se určitě vyskytuje jednička, protože možných hodnot a^m je nejvýše n. Proto existují i a j $(i < j)$ taková, že $a^i \equiv_n a^j$, tedy $a^{j-i} \equiv_n 1$. Zvolme $m > 0$ nejmenší takové, že $a^m \equiv_n 1$. Čísla $a^0, a^1, \ldots, a^{m-1}$ tvoří podgrupu multiplikativní grupy $\mathbb{Z}_n^*$. Proto podle Lagrangeovy věty platí m dělí $\varphi(n)$, tedy $\varphi(n) = k \cdot m$ pro nějaké k. Snadno nahlédneme, že $a^{\varphi(n)} \equiv_n a^{k \cdot m} \equiv_n 1^k = 1$. ♡

Tato věta nám dokázala i dříve zmíněnou Malou Fermatovu větu a snadno díky ní nahlédneme, že pro $a \perp n$ platí $a^{-1} \equiv_n a^{\varphi(n)-1}$.

Testování prvočíselnosti

Nyní využijeme naše nově získané poznatky k ověřování prvočíselnosti. Tzv. *faktorizace*, neboli rozklad čísla na součet prvočísel, je určitě v NP, avšak zatím se neví, zda to je nebo není NP-úplný problém. Naproti tomu je již znám polynomiální algoritmus, který přesně ověří, zda je zadané číslo prvočíslem (s časovou složitostí $\mathcal{O}(N^{6,5})$). Tento algoritmus je však velmi komplikovaný a stejně tak odhad jeho časové složitosti. My se proto spokojíme s tzv. Monte Carlo testováním prvočísel. Pokud takto označený test prvočíselnosti odpoví, že číslo n zadané na vstupu je složené, je to pravda. Pokud odpoví, že se jedná o prvočíslo, mýlí se s pravděpodobností menší, než $\frac{1}{2}$, čili celková pravděpodobnost, že se mýlí je menší než $\frac{1}{4}$. Pokud takový test opakujeme k-krát za sebou, je pravděpodobnost, že se test zmýlil $(\frac{1}{4})^k$, což je už pro $k = 100$ dostačující. Ukažme si tedy první z takových testů.

Algoritmus: *(Fermatův test)*

1. Zvolme náhodně $a \in \{2, \ldots, n-1\}$.
2. Pokud $\gcd(a, n) \neq 1$, je n složené.
3. Pokud $a^{n-1} \not\equiv_n 1$, je n složené (a a je *Fermatův svěděk*).
4. Jinak je n prvočíslo.

Pozorování: Pokud odpoví Fermatův test, že zadané číslo je složené, nemýlí se.

Poznámka: Všimněme si, že druhý krok algoritmu je zbytečný. Pokud totiž není $a \perp n$, neboli existuje $g > 1$ společný dělitel n a a, pak g dělí i $a^{n-1} \bmod n$ nebo $a^{n-1} \bmod n = 0$ a třetí krok algoritmu prohlásí n za složené číslo.

Špatná zpráva pro tento algoritmus je, že existují tzv. *Carmichaelova čísla*, což jsou složená čísla, která Fermatova svědka nemají. Je jich sice „řídko“, ale zato nekonečně mnoho. Pokud se ale zrovna do Carmichaelova čísla nestrefíme, mají složená čísla Fermatových svědků dostatek.

Věta: Pokud n není Carmichaelovo číslo ani prvočíslo, pak existuje alespoň $\frac{\varphi(n)}{2}$ Fermatových svědků.

Důkaz: Zvolme $H = \{a \in \{1, \ldots, n-1\} \mid a^{n-1} \equiv_n 1, a \perp n\}$, tedy množinu všech čísel, která nejsou Fermatovými svědky. Všechna čísla v H jsou invertibilní a jejich součin je opět v H. H je tedy podgrupa multiplikativní grupy $\mathbb{Z}_n^*$. Podle Lagrangeovy věty tak existuje k tak, že $|\mathbb{Z}_n^*| = \varphi(n) = k \cdot |H|$. Navíc n není Carmichaelovo, takže platí $|\mathbb{Z}_n^*| \neq |H|$. Proto $k \geq 2$ a čísel, která nemají Fermatova svědka, je $|H| \leq \frac{\varphi(n)}{2}$. ♡

Vidíme tedy, že pokud n není Carmichaelovo číslo, pak je Fermatův test Monte Carlo test prvočíselnosti. Na závěr přednášky si uvedeme Monte Carlo test, který řeší problém Carmichaelových čísel (což není zrovna jednoduché):

Algoritmus: *(Rabin-Millerův test)*

1. Zvolme náhodně $a \in \{2, \ldots, n-1\}$.
2. Pokud $a^{n-1} \not\equiv_n 1$, je n složené (a a je *Fermatův svěděk*).
3. Pro $i = 1, 2, \ldots$ dokud 2^i dělí $n-1$:
4. Spočteme $t_i \equiv_n a^{(n-1)/2^i}$.
5. Pokud je $t_i \equiv_n -1$, je n prvočíslo.
6. Pokud je $t_i \not\equiv_n 1$, je n složené (a a je *Riemannův svěděk*).
7. Jinak je n prvočíslo.