1.4 Testování prvočíselnosti

1.4.1 Jazyky L_p a L_s. Jazyk L_p obsahuje všechna prvočísla, jazyk L_s obsahuje všechna složená čísla; přesněji:

$$L_p = \{w \,|\, w \text{ je binární zápis prvočísla}\}$$

$$L_s = \{w \,|\, w \text{ je binární zápis složeného čísla}\}.$$

Jazyk L_s je (až na číslo 1) doplňkem jazyka L_p; přidáme-li 1 do jazyka L_s, pak dostáváme

$$L_s = \overline{L_p}, \;\; L_p = \overline{L_s}.$$

1.4.2 Tvrzení. Jazyk L_s leží ve třídě $\mathcal{NP}$.

Zdůvodněni: Jestliže číslo n je složené, znamená to, že má dělitele r, pro nějž platí $1 < r < n$. Známe-li některého (tzv. vlastního) dělitele r, jsme schopni dělením čísla n číslem r zjistit, že n je opravdu složené číslo. Pro prvočíslo žádný takový vlastní dělitel neexistuje.

Nyní si stačí uvědomit, že vlastní dělitel je hledaný certifikát s polynomiální velkostí. Ano, délka binárního slova odpovídajícího n, je $k = \lg n$, délka dělitele r je $\mathcal{O}(k)$ a celočíselné dělení dvou binárních čísel délky k lze provést v polynomiáním čase vzhledem k délce binárního zápisu čísel.

1.4.3 Tvrzení. Jazyk L_s leží ve třídě $\mathcal{RP}$.

Ke zdůvodnění této věty využijeme Millerův test prvočíselnosti. Dříve než test formulujeme, připomeneme, že

- Množina $\mathbb{Z}_n$ tzv. zbyktových tříd modulo n je

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

- Na množině $\mathbb{Z}_n$ jsou definovány operace $\oplus$ a $\odot$ takto

$$a \oplus b = c, \;\; \text{kde } c \text{ je zbytek při dělení čísla } a + b \text{ číslem } n,$$

$$a \odot b = c, \;\; \text{kde } c \text{ je zbytek při dělení čísla } a.b \text{ číslem } n.$$

- $(\mathbb{Z}_n, \oplus, 0)$ je komutativní grupa, $(\mathbb{Z}_n, \oplus, 0)$ je komutativní monoid a platí distributivní zákony

  Navíc, prvek $a \in \mathbb{Z}_n$ má inverzi právě tehdy, když a a n jsou nesoudělná čísla.

  Proto $(\mathbb{Z}_n, \oplus, \odot, 0, 1)$ pro n prvočíslo je těleso; pro složená n, tělesem není.

- Podle malé Fermatovy věty pro a nesoudělné s prvočíslem p platí

$$a^{p-1} \;\equiv\; 1 \,(\mathrm{mod} n).$$

- Operace sčítání, násobení, umocňování a dělení v $\mathbb{Z}_n$ je možné provést v polynomiálním čase vzhledem k velikosti čísel, se kterými se operace provádějí.

1.4.4 Millerův test prvočíselnosti.

Vstup: velké liché přirozené číslo n.

Výstup: „prvočíslo“ nebo „složené“.

1. Spočítáme $n - 1 = 2^l\, m$, kde m je liché číslo.

2. Náhodně vybereme $a \in \{1, 2, \dots, n-1\}$.

3. Spočítáme $a^m \pmod n$,
   jestliže $a^m \equiv 1 \pmod n$, stop, výstup „prvočíslo“.

4. Opakovaným umocňováním počítáme
   $a^{2\,m} \pmod n, a^{2^2\,m} \pmod n, \dots, a^{2^l\,m} \pmod n$.

5. Jestliže $a^{2^l\,m} \not\equiv 1 \pmod n$, stop, výstup „složené“.

6. Vezmeme k takové, že $a^{2^k\,m} \not\equiv 1 \pmod n$ a $a^{2^{k+1}\,m} \equiv 1 \pmod n$.
   Jestliže $a^{2^k\,m} \equiv -1 \pmod n$, stop, výstup „prvočíslo“.
   Jestliže $a^{2^k\,m} \not\equiv -1 \pmod n$, stop, výstup „složené“.

1.4.5 Věta.

1. Jestliže pro vstup n dá Millerův test prvočíselnosti odpověď „složené“, pak je číslo n složené.

2. Jestliže pro vstup n dá Millerův test prvočíselnosti odpověď „prvočíslo“, pak n je prvočíslo s pravděpodobností větší než $\frac{1}{2}$.

Add 1. Jestliže je číslo n prvočíslo, tak nemůžeme dostat výstup „složené“. Malá Fermatova věta totiž zaručuje, že nemůžeme skončit v kroku 5 s tímto výstupem. Dále pro n prvočíslo je $(\mathbb{Z}_n, \oplus, \odot)$ konečné těleso. V tělese existují pouze dva prvky, které umocněné na druhou dávají 1 — totiž číslo 1 a -1. Proto nemůžeme skončit v kroku 6 výstupem „složené“.

Add 2. Ukázat druhou vlastnost je obtížnější. Důkaz není těžký pro taková složená n, pro která existuje $a \in \mathbb{Z}_n$, a nesoudělné s n, a $a^{n-1} \not\equiv 1 \pmod n$. Pro ostatní složená čísla, tzv. „Carmichaelova čísla“, je důkaz dost obtížný.

Ukážeme základní myšlenku důkazu pro složená n: Spočítáme počet takových a vybraných v kroku 2, pro která dostaneme jistě správnou odpověď (tj. nedostaneme odpověď prvočíslo). Protože každé a má stejnou pravděpodobnost být vybráno, stačí, abychom ukázali, že jich je aspoň tolik, kolik jich může dát odpověď špatnou (prvočíslo).

Vybereme-li v kroku 2 neinvertibilní číslo a, určitě dostaneme odpověď složené, protože žádná mocnina neivertibilního čísla nemůže být rovna 1.

Předokládejme, že složené číslo n není Carmichaelovo, tj. existuje $a \in \mathbb{Z}_n$, a nesoudělné s n, a $a^{n-1} \not\equiv 1 \pmod n$. Označme

$$\mathbb{Z}_n^\star = \{a \in \mathbb{Z}_n \mid a \text{ je invertibilní}\}$$

$$K = \{a \in \mathbb{Z}_n \mid a^{n-1} = 1\}.$$

Víme, že $K \neq \mathbb{Z}_n^\star$, přitom $(K, \odot)$ je podgrupa grupy $(\mathbb{Z}_n^\star, \odot)$. Proto počet prvků K dělí počet prvků $\mathbb{Z}_n^{star}$. Proto prvků v množině K je nejvýše dvakrát méně než prvků v množině $\mathbb{Z}_n^\star$; jinými slovy

$$|\mathbb{Z}_n^\star \setminus K| \geq |K|.$$

Vybereme-li $a \in \mathbb{Z}_n^\star \setminus K$, dostaneme správnou odpověď „složené“, protože $a^{n-1} \neq 1$.

Špatnou odpověď můžeme dostat pouze pro $a \in K$ a těch je méně než nebo stejně jako $a \in \mathbb{Z}_n^\star \setminus K$.

Pro Carmichaelova čísla platí $|K| = |\mathbb{Z}_n^\star|$ a musíme argumentovat krokem 6, kde se dá ukázat, že počet a, která vedou v kroku 6 na odmocninu z 1 různou od -1 je aspoň tak velký jako počet těch a, která vedou na -1.

1.4.6 Tvrzení. Jazyk L_p je ve třídě $\mathcal{NP}$.

Najít polynomiální certifikát pro jazyk obsahující prvočísla je podstatně lepší než pro jazyk obsahující složená čísla. V tomto případě se jedná o generátor grupy $(\mathbb{Z}_p \setminus \{0\}, \odot, 1)$ (p prvočíslo); tj primitivní prvek konečného tělesa $(\mathbb{Z}_p, \oplus, \odot, 0, 1)$.

1.4.7 Důsledek. Jazyky L_p a l_s patří do průniku tříd $\mathcal{NP}$ a co-$\mathcal{NP}$.

Je tedy velmi nepravděpodobné, že by některý z nich byl $\mathcal{NP}$ úplný. V takovém případě by třídy $\mathcal{NP}$ a co-$\mathcal{NP}$ byly stejné.