Endomorfismy cyklických grup

Pozorování. Identita je jediný endomorfismus okruhu $\mathbb{Z}_n$.

Pozorování. Endomorfismy grupy $(\mathbb{Z}_n, +)$ jsou $i \mapsto i \cdot a$. Automorfismus dostáváme pro a invertibilní.

Pozorování. Ekvivalentní charakteristiky invertibilních prvků v Z_n:

- $\mathrm{NSD}(a, n) = 1$;
- $z\mathbb{Z}_n = \mathbb{Z}_n$;
- a je invertibilní;
- $i \mapsto i \cdot a$ je automorfismus.
- a je generátor grupy $\mathbb{Z}_n$.

Definice. Eulerova funkce, $\varphi(n)$.

Tvrzení.

$$n = \sum_{d \mid n} \varphi(d)$$

Důkaz. Ukážeme, že suma odpovídá rozkladu prvků grupy $\mathbb{Z}_n$ na třídy prvků podle jejich řádu (který musí dělit řád grupy). Označme A_d množinu prvků, které mají řád d. Každý prvek A_d generuje cyklickou podgrupu řádu d. Taková podgrupa je ale v $\mathbb{Z}_n$ jen jedna. Množina A_d je tedy množinou generátorů cyklické grupy řádu d, a proto má velikost $\varphi(d)$. □

Množiny A_d uvedené v předchozím důkazu mají řadu ekvivalentních charakteristik, které odpovídají charakteristice invertibilních prvků. Jsou to:

- třídy vzájemně asociovaných prvků (prvky A_d se vzájemně dělí),
- množiny prvků a, pro které je $\mathrm{NSD}(a, n) = \frac{n}{d}$,
- množiny prvků řádu d,
- množiny generátorů podgrupy $d\mathbb{Z}_n$,
- prvky tvaru $j \cdot \frac{n}{d}$, kde $j \in \mathbb{Z}_n^*$.

Připomeňme, že nad každým tělesem platí:

Lemma. Polynom stupně d má nejvýše d kořenů.

Je to důsledek toho, že okruh polynomů nad tělesem je eukleidovský (norma odpovídá stupni polynomu).

Výše uvedené tvrzení nyní umožňuje dokázat poměrně silnou větu o multiplikativní grupě *libovolného* tělesa.

Věta. Každá konečná multiplikativní podgrupa komutativního tělesa je cyklická.

Důkaz. Nechť G je n-prvková multiplikativní podgrupa tělesa T. Rozdělme si prvky G do tříd A_d podle jejich řádu jako v důkazu Tvrzení. Předpokládejme, že G není cyklická, tedy že A_n je prázdná množina. Z Tvrzení nyní plyne, že alespoň jedna množina A_d obsahuje více než $\varphi(d)$ prvků. Nechť t leží v A_d. Cyklická grupa $\langle t \rangle$ generovaná t obsahuje $\varphi(d)$ prvků A_d. Existuje tedy ještě alespoň jeden prvek $t' \in A_d$, který neleží v $\langle t \rangle$. Tím dostáváme $d+1$ kořenů polynomu x^d+1; jsou to všechny prvky grupy $\langle t \rangle$ a prvek t'. To je ale spor s Lemmatem. □

Lemma. Pokud $d \mid n$, pak zobrazení $\mathbb{Z}_n \to \mathbb{Z}_d$ dané $a \mapsto a \mod d$ je homomorfismus okruhů.

Věta. Čínská věta o zbytcích pro $\mathbb{Z}_n$.

Lemma. Invertibilní prvky kartézského součinu.

Tvrzení.

$$\varphi(n) = \prod_i p_i^{e_i - 1}(p_i - 1) = n \cdot \prod_{p \mid n}(1 - \frac{1}{p})$$