Struktura $\mathbb{Z}_{p^e}^*$

Liché prvočíslo p. Okruh $\mathbb{Z}_{p^e}$ obsahuje ideál $p\mathbb{Z}_{p^e}$, což je přesně množina neinvertibilních prvků. Faktorokruh $\mathbb{Z}_{p^e}/_{p\mathbb{Z}_{p^e}}$ je isomorfní $\mathbb{Z}_p$. Jednotlivé rozkladové třídy $i + p\mathbb{Z}_{p^e}$ obsahují prvky kongruentní i modulo p.

Multiplikativní grupa $\mathbb{Z}_{p^e}^*$, která nás zajímá, sestává z nenulových rozkladových tříd faktorokruhu. Zatímco nulová rozkladová třída, tedy ideál $p\mathbb{Z}_{p^e}$, je aditivní grupa, je rozkladová třída $1 + p\mathbb{Z}_{p^e}$ grupa multiplikativní. Navíc ukážeme, že je cyklická, generovaná prvkem $p + 1$.

Řád grupy $1 + p\mathbb{Z}_{p^e}$ je p^{e-1}, a řád prvku $p + 1$ je tedy p^k pro nějaké k. Pokud $k < e - 1$, platí také

$$((p+1)^{p^k})^{p^{e-2-k}} = (p+1)^{p^{e-2}} = 1.$$

Pokud tedy

$$(p+1)^{p^{e-2}} \neq 1,$$

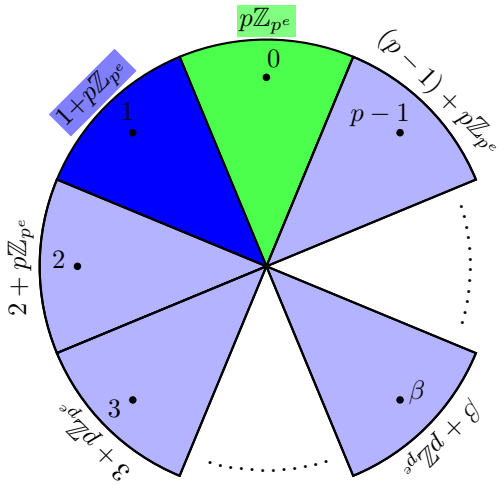
je řád prvku $(p+1)$ roven p^{e-1} a jedná se o generátor. Nerovnost lze ověřit přímým výpočtem (viz níže).

Protože je $1+p\mathbb{Z}_{p^e}$ podgrupa $\mathbb{Z}_{p^e}^*$, lze podle ní faktorizovat. Rozkladové třídy této (multiplikativní) grupy budou přitom splývat s nenulovými rozkladovými třídami (aditivní) grupy (a současně ideálu) $p\mathbb{Z}_{p^e}$. Platí totiž $i \cdot (1 + p\mathbb{Z}_{p^e}) = i + ip\mathbb{Z}_{p^e}$, přičemž $ip\mathbb{Z}_{p^e} = p\mathbb{Z}_{p^e}$, protože i je invertibilní. Faktorová grupa $\mathbb{Z}_{p^e}^*/_{(1+p\mathbb{Z}_{p^e})}$ je tedy isomorfní cyklické grupě $\mathbb{Z}_p^*$.

Nechť je α nějaký generátor $\mathbb{Z}_p^*$. Pak prvek α^{p-1} leží v grupě $1+p\mathbb{Z}_{p^e}$ a je-li r jeho řád, dostáváme $(\alpha^{p-1})^r = 1$ a prvek $\beta = \alpha^r$ má řád $p-1$. Prvky $\beta, \beta^2, \ldots, \beta^{p-1} = 1$ tvoří reprezentanty nenulových rozkladových tříd. Každý prvek grupy $\mathbb{Z}_p^*$ lze tedy zapsat jako $(p+1)^i\beta^j$, kde $i = 1, 2, \ldots, p^{e-1}$ a $j = 1, 2, \ldots, p-1$.

Dokázali jsme, že

$$\mathbb{Z}_p^* \cong \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p-1} \cong \mathbb{Z}_{(p-1)p^{e-1}}.$$



V důkazu jsme použili konstrukci, kterou lze obecně popsat takto. Nechť je H podgrupa nějaké Abelovy grupy $(G, \cdot)$ (pro Abelovy grupy častěji používáme aditivní zápis, ale náš případ je multiplikativní, používejme tedy multiplikativní notaci).

Uvažujme faktorgrupu G/H (srov. Drápal, oddíl 1.6). Ta má prvky tvaru aH. Pokud z každé třídy aH vybereme jednoho reprezentanta tak, aby tito reprezentanti tvořili podgrupu K grupy G, pak je G isomorfní direktnímu součinu $K \times H$.

Důkaz. Isomorfismus $K \times H$ a G je dán předpisem $(k, h) \mapsto k \cdot h$. Z komutativity je zřejmé, že se jedná o homomorfismus, a z volby K je zřejmé, že je na. V konečném případě (který zde uvažujeme) pak stačí konstatovat, že obě grupy mají stejný počet prvků.

Injektivitu lze ovšem dokázat i obecně. Všimněme si nejprve, že ze třídy $H = 1 \cdot H$ musíme vybrat jako reprezentanta 1, jinak nemůže být K grupa. Nechť nyní $k_1 \cdot h_1 = k_2 \cdot h_2$. Protože $k_1 k_2^{-1} = h_1^{-1} h_2 \in H$, dostáváme $k_1 k_2^{-1} = 1$ a tedy $k_1 = k_2$ a $h_1 = h_2$. □

Valuace. Označme $\mathrm{val}_p(n)$ p-valuaci n definovanou jako největší k takové, že p^k dělí n (exponent p v prvočíselném rozkladu n). Je snadno vidět, že pro každé s a libovolné $a \in \{1, 2, \ldots, p^s - 1\}$ platí

$$\mathrm{val}_p(p^s - a) = \mathrm{val}_p(a).$$

Toto pozorování umožňuje spočítat p-valuaci kombinačního čísla $\binom{p^s}{k}$. Platí

$$\mathrm{val}_p\left(\binom{p^s}{k}\right) = \sum_{a=0}^{k-1} \mathrm{val}_p(p^s - a) - \sum_{a=1}^{k} \mathrm{val}_p(a) = \mathrm{val}_p(p^s) - \mathrm{val}_p(k) = s - \mathrm{val}_p(k).$$

Nyní již můžeme přímočaře ověřit hodnotu $(p+1)^{e-2}$. Uvažme binomický rozvoj

$$(p+1)^{p^{e-2}} = 1 + \binom{p^{e-2}}{1} p + \binom{p^{e-2}}{2} p^2 + \binom{p^{e-2}}{3} p^3 + \cdots + p^{p^{e-2}}.$$

Snadno ověříme, že pro libovolné liché prvočíslo p platí, že

$$\mathrm{val}\binom{p^{e-2}}{k} p^k = e - 2 - \mathrm{val}_p(k) + k \geq e,$$

pokud $k \geq 2$. (Pro $p = 2$ platí nerovnost až od $k \geq 3$, což bude důležité později). Odtud je vidět, že

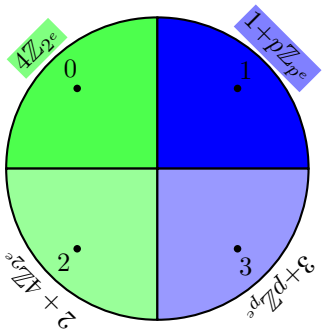
$$(p+1)^{p^{e-2}} = 1 + p^{e-1} \neq 1 \mod p^e,$$

což jsme chtěli ukázat.

Případ $p = 2$. Grupa $\mathbb{Z}_{2^e}^*$ má 2^{e-1} prvků (jsou to všechna lichá čísla). Ve faktorokruhu $\mathbb{Z}_{2^e}/_{2\mathbb{Z}_{2^e}}$ tvoří jedinou rozkladovou třídu (ze dvou). Grupa ale není cyklická. Je to vidět např. z toho, že obsahuje tři prvky řádu dva: -1, $2^{e-1} + 1$ a $2^{e-1} - 1$, tedy tři různé dvouprvkové podgrupy, zatímco cyklická grupa obsahuje nejvýše jednu grupu daného řádu. Prvek $p + 1$ (tedy trojka) nemá řád 2^{e-1}, protože platí

$$(1+2)^{2^{e-2}} = 1 + 2^{e-1} + \frac{2^{e-2}(2^{e-2} - 1)}{2} \cdot 2^2 = 1 + 2^e = 1 \mod 2^e.$$

Pro odhalení struktury $\mathbb{Z}_{2^e}^*$ proto použijeme ideál $4\mathbb{Z}_{2^e}$.



Podgrupa $1+4\mathbb{Z}_{2^e}$ má velikost 2^{e-2} a je cyklická s generátorem 5, protože pro $1+4$ platí, že

$$(1+4)^{2^{e-3}} = 1 + 2^{e-3}\cdot 4 + \frac{2^{e-3}(2^{e-3}-1)}{2}4^2 + \cdots = 1 + 2^{e-1} \neq 1 \mod 2^e.$$

Podobně jako v lichém případě dostáváme, že

$$\mathbb{Z}_{2^e}^* \cong \mathbb{Z}_{2^{e-2}} \times \mathbb{Z}_2.$$

Roli β hraje -1. Všimněme si, že prvek $3+4a$ lze také napsat jako $-1+4(a+1)$. Grupa $\mathbb{Z}_{2^e}^*$ tedy není cyklická, kromě případu $e=2$, kdy je první direktní činitel triviální, neboli $\mathbb{Z}_4^* = \{1,3\}$.