27.2.

1 Pollardova ρ-metoda

1.1. Určete periodu a preperiodu posloupnosti $\{s_n\}_{n\geq 0}$ určené polynomiálním zobrazením $f(x) = ax + b \in \mathbb{Z}_p$ pro $x \in \mathbb{Z}_p$, kde $p \in \mathbb{P}$, tj. $s_0 \in \mathbb{Z}_p$ a $s_{n+1} = f(s_n)$, pokud

(a) $a = 1$, $b \in \mathbb{Z}_p$,

(b) $a \in \mathbb{Z}_p^*$, $b = 0$.

(a) Nejprve vyjádříme přímo hodnotu $s_n = s_0 + nb$. Pro $b = 0$ je posloupnost konstantní, a proto má preperiodu $m = 0$ a periodu $t = 1$.

Pokud $b \neq 0$, máme $ib \neq 0$ pro $i = 1, \ldots, p-1$ a $pb = 0$, což znamená, že má posloupnost preperiodu $m = 0$ a periodu $t = p$.

Pollardova ρ-metoda bude v případě $b = 0$ úspěšná, jen tehdy, kdy $b = 0$ vzniklo modulením nenulové hodnoty $B \in \mathbb{Z}_N$, tedy když jsme uhodli násobek vlastního dělitele $p \mid N$, což se nedá očekávat často. V případě $b \neq 0$ je součet $t + m = p$, tedy v případech obou algoritmů musíme provést maximální možný počet iterací (p vně)

(b) Opět snadno určíme nerekurentní vzorec $s_n = a^n s_0$.Je-li $s_0 = 0$, posloupnost je konstantně nulová, tedy posloupnost s preperiodou $m = 0$ a periodou $t = 1$.

Pokud $s_0 \neq 0$, vidíme, že preperioda posloupnosti je nulová, neboť $a^{p-1} = 1$ a že nejmenší přirozené číslo t splňující $s_0 = s_0 a^t$, tedy perioda posloupnosti, je rovno právě řádu $o_{\mathbb{Z}_p^*}(a)$.

Všimněme si, že například pro bezpečné prvočíslo $p = 2q + 1$, kde $q \in \mathbb{P}$ obsahuje grupa $\mathbb{Z}_p^*$ jeden prvek řádu 1 a jeden prvek řádu 2, které pro Pollardovu ρ-metodu nejsou dobře použitelné a pak $(q-1)$ prvků řádu q a stejný pročet prvků řádu $2q$, které říkají, že procházka po různých číslech posloupnosti v Pollardových algoritmech by byla opět příliš dlouhá. □

6.3.

1.2. Označme $f_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$ afinní transformace daná vztahem $f_{a,b}(x) = ax + b$ a $\mathrm{Aff}(\mathbb{Z}_p) = \{f_{a,b} \mid a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$. Dokažte $\mathrm{Aff}(\mathbb{Z}_p)$ je podgrupou symetrické grupy $S(\mathbb{Z}_p)$ pro $p \in \mathbb{P}$, tedy grupa.

Stačí si rozmyslet, že

$$f_{1,0} = \mathrm{id}, \quad f_{a,b} f_{c,d} = f_{ac,ad+b}, \quad f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}$$

odkud plyne, že $f_{a,b}$ je invertibilní, tedy permutace na $\mathbb{Z}_p$ a množina $\mathrm{Aff}(\mathbb{Z}_p)$ je uzavřená na operace skládání a invertování a jedná s etudíž o podgrupu. □

1.3. Určete periodu a preperiodu posloupnosti $\{s_n\}_{n\geq 0}$ určené polynomiálním zobrazením $f : \mathbb{Z}_p \to \mathbb{Z}_p$ pro $p \in \mathbb{P}$, pokud

(a) $f(x) = ax + b$, $a, b \in \mathbb{Z}_p^*$ a $a \neq 1$.

(b) $f(x) = x^2$.

(a) S využitím předchozí úlohy najdeme c tak, aby $f_{1,c} f_{a,b} f_{1,c}^{-1} = f_{u,0}$. Nejprve spočteme

$$f_{1,c} f_{a,b} f_{1,c}^{-1} = f_{1,c} f_{a,b} f_{1,-c} = f_{a,b+c} f_{1,-c} = f_{a,-ac+b+c},$$

z podmínky $-ac + b + c = 0$ plyne, že $c = b(a-1)^{-1}$.

Označme $g = f_{1,c}$, $f = f_{a,b}$ a $h = gfg^{-1}$. Protože $s_n = f^n(s_0) = g^{-1}h^n(g(s_0))$, vidíme, že $s_i = s_j$, právě když $h^i(g(s_0)) = h^j(g(s_0))$, tedy perioda i preperioda posloupností $\{s_n\}_{n\geq 0}$ a $\{h^n(g(s_0))\}_{n\geq 0}$ je stejná. Nyní zbývá využít 1.1, která říká, že pro $s_0 = -c$ jsou obě posloupnosti konstantní , tedy mají preperiodu $m = 0$ a periodu $t = 1$ a pro $s_0 \neq -c$ mají obě posloupnosti opět preperiodu $m = 0$ a periodu $t = o_{\mathbb{Z}_p^*}(a)$.

(b) Nejprve si uvědomíme, že ze vztahu $s_{n+1} = s_n^2$ okamžitě plyne nerekurentní vzoreček $s_n = s_0^{2^n}$. Dále si všimneme, že pro $s_0 = 0, 1$ je získaní posloupnost konstantní, tedy s preperiodou 0 a periodou 1 a můžeme se tak omezit na na hledáme nejmenšího i a nejmenšího $j > i$, pro která platí , že $s_i = s_j$ za předpokladu, že $s_0 \neq 0, 1$. Najdeme-li je, pak i bude právě preperioda a $j - i$ perioda této posloupnosti. Uvážíme řadu ekvivalentních překladů podmínky v grupě $\mathbb{Z}_p^*$

$$s_i = s_j \Leftrightarrow s_0^{2^i} = s_j^{2^j} \Leftrightarrow s_0^{2^{j-i}} = 1 \Leftrightarrow s_0^{2^{j-i}} = 1 \Leftrightarrow o_{\mathbb{Z}_p^*}(s_0) \mid 2^{j-i},$$

kde poslední ekvivalence plyne z faktu, že exponentem prvku jsou právě násobky řádu prvku. Nyní vyjádříme $o_{\mathbb{Z}_p^*}(s_0) = 2^e m$ pomocí $e = v_2(o_{\mathbb{Z}_p^*}(s_0))$, kde m je liché. Potom dostáváme ekvivalence

$$o_{\mathbb{Z}_p^*}(s_0) \mid 2^{j-i} \Leftrightarrow i \geq e,\ m \mid 2^{j-i} \Leftrightarrow i \geq e,\ 2^{j-i} \equiv 1 \pmod{m}.$$

Minimálních hodnot tedy dosahujeme pro preperiodu $i = e$ a periodu $j - i = o_{\mathbb{Z}_m^*}(2)$. □