Cvičení k Pollardově ρ-metodě

Vysvětlete, proč není vhodné pro Pollardovu ϱ-metodu volit lineární funkci. Konkrétně: Máme prvočíslo p a funkci $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ danou předpisem $f(x) = ax + b$, kde $a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p$. Pomocí funkce f generujeme v $\mathbb{Z}_p$ posloupnost $y_0, y_1, \ldots$ tak, že $y_0 \in \mathbb{Z}_p$ zvolíme náhodně a $y_{i+1} = f(y_i)$. Určete preperiodu a periodu takto vzniklé posloupnosti, pokud

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

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

c) $a \neq 1$, $b \neq 0$.

Řešení: a) posloupnost $y_0, y_1, \ldots$ lze spočítat přímo $y_i = y_0 + ib \bmod p$. Tedy pro $b = 0$ je posloupnost konstantní (v tomto případě metoda Pollard-ϱ bude vždy neúspěšná), pro $b \neq 0$ je preperioda posloupnosti 0 a perioda je p (v tomto případě algoritmus Pollard-Floyd odhalí dělitele p až po p iteracích, tedy nedostaneme nic lepšího než zkusmé dělení).

b) Opět můžeme snadno spočítat, jak bude vypadat posloupnost $y_0, y_1, \ldots$ Platí $y_i = a^i y_0 \bmod p$. Pro $y_0 = 0$ je posloupnost konstantní, pro $y_0 \neq 0$ bude preperioda 0 a perioda je dána řádem a v grupě $\mathbb{Z}_p^*$. Připomeňme, že $\mathbb{Z}_p^*$ je cyklická grupa řádu $p-1$. Pokud je p tzv. bezpečné prvočíslo, tedy $p = 2q+1$, kde q je prvočíslo, má grupa $\mathbb{Z}_p^*$ prvky řádu $1, 2, q, 2q$, tedy až na dvě výjimky jde o prvky relativně velkého řádu a pro odhalení dělitele p by algoritmus Pollard-Floyd typicky potřeboval $p-1$ nebo $(p-1)/2$ iterací. Pro metodu Pollard-ρ tak volba polynomu $f = \pm x$ povede pro lichá N vždy k neúspěchu, pro $f = ax$ by jedna konkrétní volba $a \in \{2, \ldots, N-2\}$ mohla vést k úspěšné faktorizaci. Bohužel nevíme, která to je.

c) Preperiodu a periodu by šlo opět spočítat, zkusme se na problém podívat optikou teorie grup. Grupa, která nás zajímá, je grupa lineárních transformací $\mathbb{Z}_p$. Tedy $G = \{ux + v \mid u \in \mathbb{Z}_p^*, v \in \mathbb{Z}_p\}$. Násobení je dáno vztahem $(ux + v)(u'x + v') = uu'x + uv' + v$ (formule odpovídá skládání lineárních polynomů), jednotkovým prvkem G je x a $(ux+v)^{-1} = u^{-1}x - u^{-1}v$. Asociativitu grupové operace není třeba ověřovat, G je podgrupou symetrické grupy $S(\mathbb{Z}_p)$ (prvku $ux + v$ odpovídá zobrazení $y \mapsto uy + v$).

Pro daný prvek $f = ax + b \in G$ zkusíme najít $g \in G$ tak, aby $f_0 := gfg^{-1} = a'x$ pro nějaké $a' \in \mathbb{Z}_p^*$. Zkusíme g najít ve tvaru $g = x + c$, kde $c \in \mathbb{Z}_p$. Pak $g^{-1} = x - c$ a

$$gfg^{-1} = (x + c)(ax + b)(x - c) = (x + c)(ax - ac + b) = ax - ac + b + c$$

Pro $a \neq 1$ tedy stačí volit $c = b/(a-1)$.

Vrat'me se k našemu problému: Máme zvoleno y_0, další prvky posloupnosti jsou $y_i = f^i(y_0) = [g^{-1}f_0 g]^i(y_0) = g^{-1}f_0^i(g(y_0))$. Takže $y_i = y_j$ právě když $f_0^i(g(y_0)) = f_0^j(g(y_0))$. Takže preperiodu a periodu posloupnosti $y_0, y_1, \ldots$ lze získat z posloupnosti $z_0, z_1, \ldots$, kde $z_0 = g(y_0)$ a $z_i = f_0^i(z_0)$. S využitím b) pak

máme pro $y_0 = -c$ je preperioda 0 a perioda 1 a jinak je preperioda 0 a perioda dána řádem prvku a v $\mathbb{Z}_p^*$.

Podívejme se ještě na kvadratické polynomy. Připomeňme, že zatímco $f = x^2 + 1, f = x^2 - 1, f = x^2 + 2$ jsou obecně doporučované volby f, volby $f = x^2$ a $f = x^2 - 2$ nejsou považovány za vhodné.

Podívejme se nejprve na případ $f = x^2$. Posloupnost, která nás zajímá, je $y_0, y_1, \ldots \in \mathbb{Z}_p$, y_0 volíme náhodně a $y_{i+1} = f(y_i), i \in \mathbb{N}$. Předpokládejme, že $y_0 \neq 0, 1$. Máme $y_i = y_j$ právě když je $o(y_0)|(2^j - 2^i)$, kde $o(y_0)$ je řád prvku y_0 v grupě $\mathbb{Z}_p^*$. Označme $o(y_0) = 2^e l$, kde $e \in \mathbb{N}_0$ a $l \in \mathbb{N}$ je liché. Pro $j > i$ je $y_i = y_j$ právě když $i \geq e$ a $l|(2^{j-i} - 1)$. Takže preperioda posloupnosti je e a perioda posloupnosti je daná řádem prvku 2 v $\mathbb{Z}_l^*$. Je asi jasné, že chování preperiody a periody má hodně daleko k narozeninovému paradoxu. Lepší představu si zase uděláme pro bezpečná prvočísla: Je-li $p = 2q + 1$, kde q je prvočíslo, je řád y_0 v $\mathbb{Z}_p^*$ typicky $2q$ nebo q. Pak $e = 0$ nebo $e = 1$ a $l = q$. Délka periody tedy nezávisí na volbě y_0, ale na řádu 2 v $\mathbb{Z}_q^*$. Asi není důvod, proč by měl být tento řád malý (např. $p = 23$ je perioda 10, ale třeba pro $p = 47$ je perioda 11).

Nakonec ještě naznačme, proč se nepovažuje vhodná volba polynomu $f = x^2 - 2$. Předpokládejme, že existuje $z_0 \in \mathbb{Z}_p^*$ takové, že $y_0 = z_0 + 1/z_0$. Pak $y_1 = f(y_0) = z_0^2 + 1/z_0^2$, $y_2 = z_0^4 + 1/z_0^4, \ldots$. Tedy posloupnost $y_0, y_1, \ldots$ je určená posloupností $z_0, z_1, \ldots$, která splňuje rekurenci $z_{i+1} = z_i^2$. Vidíme, že $y_i = y_j$ právě když $z_i = z_j$ nebo $z_i z_j = 1$. Případ $z_i = z_j$ je analyzován výše, případ $z_i z_j = 1$ zatím nechme jako problém k zamyšlení.

Dodejme, že existence z_0 není garantovaná pro všechna y_0, k tomuto problému se ještě vrátíme, až budeme probírat odmocňování v $\mathbb{Z}_p$.