Domácí úkol z 16. března 2017

Předpokládejme, že (na nějaké dané eliptické křivce) bod P generuje cyklickou grupu řádu N a že je dán bod $Q \in \langle P \rangle$. Naším úkolem je najít celé číslo k splňující $kP = Q$. Pro jednoduchost předpokládejme, že N je liché prvočíslo.

Při Pollardově ρ-metodě jsme používali funkci $f : \langle P \rangle \to \langle P \rangle$, která byla definovaná jako přičítání některého z několika konstantních bodů v závislosti na tom, ve které části definičního oboru jsme právě byli. Pro každou z následujících dvou variant vysvětlete, co by způsobilo „zjednodušení“ této definice takto: zvolíme pevně libovolná celá čísla u, v, spočítáme bod

$$R = uP + vQ$$

a pro každý bod $X \in \langle P \rangle$ definujeme funkci $f : \langle P \rangle \to \langle P \rangle$ tímto předpisem:

1. položíme $f(X) = X + R$;
2. položíme $f(X) = 2X + R$.

Jeden efekt je jasný: ve druhé variantě musíme při každé iteraci provést dvě sčítání bodů místo jednoho, což výpočet zpomalí. Ale důležitější je promyslet funkčnost metody: připomeňme, že jsme zvolili startovní bod

$$P_0 = a_0 P + b_0 Q$$

a počítali iterace $P_{j+1} = f(P_j)$, pro každé $j = 0, 1, 2, \ldots$, dokud jsme neobjevili $j < i$ splňující $P_j = P_i$. Protože jsme si průběžně počítali pro každý získaný bod také jeho vyjádření lineární kombinací bodů P a Q, ze shody $P_j = P_i$ jsme odvodili nějakou informaci o hledaném k.

Jak to dopadne v našich dvou variantách definice funkce f?