2 - Faktoryzacja Ro-Pollarda

Friday, 21 June 2024 10:48

Chcemy zfaktoryzować N.

Ustalmy jakąś pseudolosową funkcję np. $f(x) = x^2 + 1$

Wylosujmy x_0 i rozpatrzmy ciąg $x_{n+1} = f(x_n)$

Po około $k^{\frac{1}{2}}$ krokach ciąg mod k się powtórzy (i zacyklimy).

Jeśli istnieje $p \mid N$ $(p < N^{\frac{1}{2}})$ to po $\sim p^{\frac{1}{2}}$ krokach

będziemy mieli i, j: $x_i = x_j \pmod p$ i $x_i \neq x_j \pmod N$

Wtedy $\gcd(x_i - x_j, N)$ da nietrywialny dzielnik N.

Jeśli coś nie wyjdzie: $x_i = x_j \pmod N$ itp. to resetujemy.

Jak znaleźć parę $x_i = x_j$?

Żółw i zając: trzymamy dwie wartości: x_{2k} i x_k i sprawdzamy gcd.

Złożoność: po $O(N^{\frac{1}{4}})$ krokach spodziewamy się znaleźć dzielnik N. □