77

Pollard's - Rho Method for factorization (Monte- Carlo Method)

Let n be a composite positive odd integers. Let p be its prime divisor. choose a fairly simple polynomial of degree atleast 2 with integer coefficients such as quadratic polynomial.

$$f(x) = x^2 + a, \quad a \neq 0, -2$$

→ Start with initial value x_0

→ A random sequence $x_1, x_2, x_3 \ldots$ is generated using the relation

$$x_{k+1} = f(x_k) \pmod{n},$$

$k = 0, 1, 2, \ldots$

78

→ $\exists$ a nontrivial divisor d of n $(d < n)$ such that $\exists$ integers x_j and x_k that lie in the same congruence class modulo d but belong to different modulo class modulo n; ie,

$$x_k \equiv x_j \pmod{d}$$

but $x_k \not\equiv x_j \pmod{n}$

$\Rightarrow$ $\gcd(x_k - x_j, n)$ is a nontrivial divisor of n.

79

Exc: $n = 91$, $x_0 = 1$

$f(x) = x^2 + 1$

$x_1 = 2$

$x_2 = 5$

$x_3 = 26$

$\vdots$

$\gcd(x_1 - x_0, 9) = (1, 91) = 1$

$\gcd(x_2 - x_1, 91) = (3, 91) = 1$

$\gcd(x_3 - x_2, 91) = (21, 91) = 7$

$\Rightarrow$ n is composite.

<u>Note:</u> As K increases, the task of computing $\gcd(x_K - x_j, n)$ for each $j < K$ becomes very time consuming. Reduce the number of steps by taking $K = 2j$.

80

<u>Exc:</u> $n = 2189$

$f(x) = x^2 + 1$

$x_0 = 1$

$x_1 = 2$

$x_2 = 5$

$x_3 = 26$

$x_4 = 677$

$x_5 = 829$

$\vdots$

$\gcd(x_2 - x_0, 2189) = (4, 2189) = 1$

$\gcd(x_3 - x_1, 2189) = (25, 2189) = 1$

$\gcd(x_4 - x_2, 2189) = (672, 2189) = 1$

$\gcd(x_5 - x_3, 2189) = (803, 2189) = 11$

$\Rightarrow$ 2189 is Composite.