POLLARD’S RHO ALGORITHM FOR PRIME FACTORISATION

SUJAYKUMAR KULKARNI

Prerequisites

- GCD
- Birthday Paradox: The probability of two persons having same birthday is unexpectedly high even for small set of people.
- Floyd’s cycle-finding algorithm: If tortoise and hare start at same point and move in a cycle such that speed of hare is twice the speed of tortoise, then they must meet at some point.

Algorithm

- Start
- Take random ‘x’ and ‘c’. Let y=x and $f(x)=x^2+c$
- While a divisor is not obtained.
    - Update x to f(x)(modulo n)
    - Update y to f(f(y))(modulo n)
    - Calculate GCD of |x-y| and n.
    - If GCD >=1:
        - If, GCD == n, Repeat the loop with new ‘x’, ’y’ and ‘c’.
        - Else, GCD is our answer.

References

- https://www.cs.colorado.edu/~srirams/courses/csci2824-spr14/pollardsRho.html
- https://en.wikipedia.org/wiki/Pollard's_rho_algorithm

THANK YOU