Understanding Pollard's Rho Algorithm for Integer Factorization

ABOUABID HAMZA

February 4, 2024

1 Introduction

Pollard's Rho algorithm is a probabilistic method for integer factorization, which is particularly effective for large semi-primes. Developed by John Pollard in 1975, this algorithm is based on the principles of the birthday paradox and cycle detection.

2 Mathematical Foundation

The algorithm's efficiency comes from the birthday paradox in probability theory. The paradox implies that in a set of randomly chosen elements, there is a high probability that some pair of them will collide (be the same) much sooner than intuitively expected.

2.1 Birthday Paradox

The birthday paradox states that in a set of just 23 people, there's approximately a 50% chance that at least two people will have the same birthday. In the context of factorization, this principle helps in finding cycles or repetitions in sequences of numbers, which leads to discovering factors of a composite number.

3 The Algorithm

Pollard's Rho algorithm is based on the fact that sequences generated by a polynomial function modulo n (the number to be factored) will eventually enter a cycle. Detecting this cycle can reveal a non-trivial factor of n.

3.1 Function Selection

A polynomial function, typically $f(x) = x^2 + 1 \mod n$, is chosen. This function generates a sequence of values that are used to find a factor.

3.2 Initialization

Select initial values for x and y, commonly both set to 2. These values are iteratively updated based on the function $f(x)$.

3.3 Iteration and Cycle Detection

The key to the algorithm is the iterative process:

$$x \leftarrow f(x)$$
$$y \leftarrow f(f(y))$$

Here, y is updated twice as fast as x, aiding in cycle detection (Floyd's cycle-finding algorithm).

3.4 GCD Computation

After each update, the algorithm computes $\gcd(|x - y|, n)$. A non-trivial factor is found when this GCD is greater than 1.

4 Example

Consider factorizing $n = 8051$. The steps would be as follows:

1. Choose $f(x) = x^2 + 1 \mod 8051$, with $x = 2$ and $y = 2$.
2. Iteratively update x and y and compute $\gcd(|x - y|, 8051)$.
3. The process continues until a non-trivial factor is found.

5 Conclusion

Pollard's Rho algorithm offers a probabilistic approach to factorization. It is highly effective for large numbers, especially semi-primes, and forms an important part of computational number theory and cryptography.