

WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com


Foundational Mathematics for Web3 Builders

Lecture 20

June 4, 2024

1 Integer Factorization

The problem of factoring huge integers is significant in cryptography. Many cryptographic methods, like RSA (Rivest-Shamir-Adleman), depend on the difficulty of factoring big composite numbers. The security of these systems is predicated on the fact that, while multiplying two huge prime numbers is computationally simple, factoring the resulting product back into its prime components is tremendously difficult. In this chapter, we explore some notable contemporary algorithms for factoring huge numbers, including:

- Pollard's Rho Algorithm
 - Pollard's $p - 1$ method
 - Lenstra's Elliptic Curve Factorization
 - Quadratic Sieve factorization method
 - General Number Field Sieve (GNFS)
 - Quantum algorithms such as Shor's algorithm
- 

1.1 Pollard's Rho Method

The Pollard factorization algorithm is based on congruence with a polynomial function and has a set initial value. This approach is primarily used for factoring a medium-large integer $n = pq$, where p and q are primes with $p \leq q$.

Let n be the number to be factored, and assume $n = pq$, where p is a prime factor not larger than \sqrt{n} .

The factor q does not need to be prime in this case, especially if n has more than two prime factors. Note that p is unknown to us; nevertheless, once we know p , the factorization is complete.

Given an integer n , begin with a random x and c and set initial value of y equal to initial value of x and $f(x) = x^2 + c$.

Consider $x_0 = 2$, $f(x) = x^2 + 3$, and $y_0 = x_0$. Consider the two sequences x_k and y_k , $k \in \mathbb{N}$ as specified by

$$x_k = f(x_{k-1}) \bmod n$$

$$y_k = f(f(y_{k-1})) \bmod n$$

We get $x_1 = f(x_0) \bmod n$, $y_1 = f(f(y_0)) \bmod n$, $x_2 = f(x_1) \bmod n$, $y_2 = f(f(y_1)) \bmod n$ and so on.

At each stage, we use the Euclidean Algorithm to calculate $g = \gcd(y_k - x_k, n)$ and instantly if the result exceeds 1 we stop.

Algorithm

To factor the number n , set $x = 2$ and $y = x^2 + 3$.

1. Calculate $g = \gcd(|x_k - y_k|, n)$
2. If $g = 1$, replace x with $x_k^2 + 3$, and y with $(y_k^2 + 3)^2 + 3$ reduced mod n .
3. If $1 < g < n$, then stop: g represents a proper factor of n .
4. If $g = n$ the algorithm fails and should be initialized. This is uncommon for a large n .

The gcd we found may not be the hypothesized p , but it is a divisor of it, and it is extremely usual to get a prime.

Example 1

Let's assume $n = 2021$. We define $x_0 = 2$ and $f(x) = x^2 + 3$. We then calculate:

k	x_k	y_k	$\gcd(x_k - y_k , n)$
1	7	52	$\gcd(45, 2021) = 1$
2	52	1727	$\gcd(1675, 2021) = 1$
3	686	1073	$\gcd(387, 2021) = 43$

Thus 43 is a factor of $n = 2021$ and we're done.

Example 2

Let's factor $n = 2929$. We set $x_0 = 2$ and $f(x) = x^2 + 3$. We then calculate:

k	x_k	y_k	$\gcd(x_k - y_k , n)$
1	7	52	$\gcd(45, 2929) = 1$
2	52	2423	$\gcd(2371, 2929) = 1$
3	2707	2443	$\gcd(264, 2929) = 1$
4	2423	1199	$\gcd(1224, 2929) = 1$
5	1216	2115	$\gcd(899, 2929) = 29$

Thus 29 is a factor of $n = 2929$ and we're done.

mod. 2929
clid?
 $\Rightarrow x = x^2 + 3$
3