Sample title

Anonymous

Overleaf

2021

Background 1-2 min

- Hendrik Lenstra Jr. recieved his doctorate from the University of Amsterdam in 1977.
- Discovered Elliptic Curve Factorization (ECM) in 1987.
- ECM is third-fastest known factoring algorithm and the best algorithm for finding divisors not exceeding 50-60 digits.
- The largest factor found using ECM has 83 digits.

Preliminaries 2 mins

- Let E be an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ of the form

$$y^2 = x^3 + ax + 1$$

such that $4a^3 + 27 \in (\mathbb{Z}/N\mathbb{Z})^*$. This forces non singularity and ensures $P = (0, 1)$ is on the curve.

- Definition 6.3.1 (Power Smooth). Let B be a positive integer. If n is a positive integer with prime factorization

$$n = \prod p_i^{e_i},$$

then n is B-power smooth if $p_i^{e_i} \leq B$ for all i.

- Example $30 = 2 \cdot 3 \cdot 5$ is B power smooth for $B \geq 5$, but $150 = 2 \cdot 3 \cdot 5^2$ is not 5-power smooth.

Motivation 1-2 mins

- Fix $B \in \mathbb{N}$. Let $p \in \mathbb{N}$ such that $p-1$ is not B- power smooth.
- Recall, in Pollard $p-1$, this would be equivalent to not having $p-1|m = \text{lcm}(1, 2, \ldots, B)$; i.e. $a^m \not\equiv 1 \pmod{p}$.
- On the interval $[10^{15}, 10^{15} + 10000]$ 15 percent of the primes p are such that $p-1$ is not 10^6-power smooth.
- The idea of ECM is to replace modular exponentiation on $(\mathbb{Z}/N\mathbb{Z})^*$ by repeated addition of points on $E\left((\mathbb{Z}/N\mathbb{Z})^*\right)$
- Recall, by the Hasse-Weil bound we can reduce the size of our group by $2 \cdot \sqrt{p}$.

Elliptic Curve Factorization 2 mins

Algorithm 6.3.10 (Elliptic Curve Factorization Method). Let N and B be positive integers.

1. Compute $m = \text{lcm}(1, 2, \ldots, B)$.
2. Choose $a \in \mathbb{Z}/N\mathbb{Z}$ such that $4a^3 + 27 \in (\mathbb{Z}/N\mathbb{Z})^*$. This forces $P = (0, 1)$ to be a point on $y^2 = x^3 + ax + 1$ over $\mathbb{Z}/N\mathbb{Z}$.
3. Try to compute mP. If at somepoint we cannot compute a sum of points some denominator g is not coprime to N, then $gcd(g, N)$ is a nontrivial divisor of N.

Analogy to Pollard p-1 1 min

Table: Let E be an elliptic curve, and $m = lcm(1, 2, \ldots, B)$ for some B

Pollard $p-1$	**ECM**
$\mathbb{Z}/N\mathbb{Z}$	$E(\mathbb{Z}/N\mathbb{Z})$
$g \in (\mathbb{Z}/N\mathbb{Z})^*$	$(0, 1)$
$g^m \equiv 1 \pmod{N}$	$mP \notin E(\mathbb{Z}/N\mathbb{Z})$
$gcd(g^m - 1, N)$	$gcd(m, N)$

- If Pollard $p-1$ fails, we have no choice but to increase B.
- However, ECM has a second option. We can choose another random elliptic curve.

Why it works 1-2 mins

Example by hand 2 mins

Implementation 2 mins

Run Time Analysis/Comparison 2 mins

Coded Example 2 mins

Animation 1 min