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

Elliptic Curve Factorization 2 mins

Analogy to Pollard p-1 1 min

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