Lecture 22 Lenstra's Elliptic curve factorization §66

Recall Pollard's $(p-1)$-method:

Suppose we want to factor $N = pq$ a product of primes.

Choose $a \in \mathbb{Z}/N$ and compute $a^{n!}$ mod N

until we get $\gcd(a^{n!}-1, N) \neq 1$.

This works if $p-1$ (say) is smooth b/c

then $(p-1) \mid n!$ for a modest value of n

so $a^{n!} \equiv 1 \mod p$ for this n

$\Rightarrow \gcd(a^{n!}-1, N) = p$.

Idea order of $a \in \mathbb{F}_p^\times$ $\neq$ order of $a \in \mathbb{F}_q^\times$

so find k s.t. $\text{ord}_{\mathbb{F}_p^\times}(a) \mid k$ but $\text{ord}_{\mathbb{F}_q^\times}(a) \nmid k$.

Lenstra's plan Do this w/ an elliptic curve instead.

Pick $E: Y^2 = X^3 + AX + B$ over $\mathbb{Z}/N\mathbb{Z}$, $P \in E(\mathbb{Z}/N\mathbb{Z})$.

Need $\gcd(4A^3 - 27B^2, N) = 1$, if it is N, try again, if it is not 1 or N, we factored N and can stop!

Idea order of P in $E(\mathbb{F}_p)$ $\neq$ order of $P \in E(\mathbb{F}_q)$.

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(\mathbb{Z}/N\mathbb{Z})$

$$\begin{cases} x(P_1 + P_2) = m^2 - x_1 - x_2 \\ y(P_1 + P_2) = -(m(x - x_1) + y_1) \end{cases} \qquad m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

Issue If $\gcd(x_2 - x_1, N) \neq 1$, cannot divide by $x_2 - x_1$

$\Rightarrow$ cannot use this formula to compute $P_1 + P_2$.

$$\gcd(x_1 - x_2, N) = \begin{cases} p & \Leftrightarrow \quad P_1 + P_2 = \mathcal{O} \in E(\mathbb{F}_p) \\ q & \Leftrightarrow \quad P_1 + P_2 = \mathcal{O} \in E(\mathbb{F}_q) \\ N & \Leftrightarrow \quad \text{both} \end{cases}$$

Rmk $E(\mathbb{Z}/N)$ is a bit subtle.

If defined correctly, $E(\mathbb{Z}/N)$ is a group.

But the correct definition is not

$$E(\mathbb{Z}/N) \neq \{(x,y) \in (\mathbb{Z}/N)^{\times 2} \mid y^2 = x^3 + Ax + B\} \cup \mathcal{O}$$

This incorrect definition gives only a partially defined addition. This works out fine for us because when we discover we've screwed up we'll factor N...

Correct definition makes $E(\mathbb{Z}/N) = E(\mathbb{Z}/p) \times E(\mathbb{Z}/q)$

(but in a more natural way!)

Lenstra's Factorization Algorithm

Set $E: Y^2 = X^3 + AX + B$, $P \in E(\mathbb{Z}/N\mathbb{Z})$.

For $j = 1, 2, \cdots$, Compute $(j!) \cdot P$.

If we fail to compute it, it's b/c we found

$$d = \begin{cases} x_1 - x_2 \\ y_1 \end{cases} \quad \text{s.t. } \gcd(d, N) \neq 1.$$

If $\gcd(d, N) \neq N$ (most likely) then we've factored N. If $\gcd(d, N) = N$, try again.

How to find E & P?

Choose $P = (a, b) \in (\mathbb{Z}/N)^{\times 2}$, $A \in \mathbb{Z}/N$.

Set $B = b^2 - a^3 - Aa$ to make $P \in E(\mathbb{Z}/N\mathbb{Z})$.

$$x(P_1+P_2) = m^2 - x_1 - x_2$$

$$y(P_1+P_2) = -\left(m(x-x_1)+y_1\right)$$

$$m = \begin{cases} \dfrac{y_2-y_1}{x_2-x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2+A}{2y_1} & \text{if } P = P_2 \end{cases}$$

Note: These formulas do not depend on B!

Example $N = 611$.

Choose $P = (1, 306)$ $A = 1$.

$\left(306 = \frac{611+1}{2}\right)$

Then $B = b^2 - a^3 - Aa$

$= 153 - 1 - 1$

$= 151$.

$2P$: $m = \dfrac{3 \cdot 1^2 + 1}{2 \cdot 306} = 4$

$x(2P) = m^2 - 2x = 16 - 2 \cdot 1 = 14$

$y(2P) = -(4(14-1) + 306) = -(4 \cdot 13 + 306) = -350 = 253$

$3 \cdot P$:

$2 \cdot (2P)$: $m = \dfrac{3 \cdot 14^2 + 1}{2 \cdot 253} = \dfrac{3 \cdot 196 + 1}{506} = (3 \cdot 196 + 1) \cdot 64 = 425$

$$x(2 \cdot 2P) = 425^2 - 2 \cdot 14 = 352$$

$$y(2 \cdot 2P) = -(425(352 - 14) + 253) = 293$$

$$3(2P) = 2(2P) + (2P)$$

$$m = \frac{293 - 253}{352 - 14} = \frac{40}{338}$$

$$\gcd(611, 338) = 13 \Rightarrow 611 = 13 \cdot 47 \quad \square$$

Factorization Algorithms

$N = pm$ p smallest prime divisor of N.

① Difference of squares + Quadratic Sieve

$$O\left(\exp\left(\sqrt{\log N \log\log N}\right)\right)$$ sub exponential.

(1') Number field sieve (not covered)

$$O\left(\exp\left(\sqrt[3]{\log N \log\log N}\right)\right)$$ fastest for general purposes

(2) Lenstra's Elliptic Curve factorization

$$O\left(\exp\left(\sqrt{2 \log p \log \log p}\right)\right)$$

Best for factoring out moderately large prime factors of enormous numbers.

(3) Pollard's $(p-1)$ – method.

Best if $p-1$ is smooth.