Lecture 20 Elliptic Curve DLP §6.3 & 6.3.1

Last time Computed # of pts on $E: y^2 = x(x+3)(x-1)$ is 8, computed group structure is $\mathbb{Z}/2 \times \mathbb{Z}/4$.

To decide group structure:

Step 1 Count # of points

Step 2 Use structure thm of finite abelian gps to list possibilities

Step 3 Do enough computation to distinguish the possibilities.

Question Given an Elliptic curve $E: y^2 = x^3 + Ax + B$, $A \& B \in \mathbb{Q}$, p not dividing denominator of A, B, & $4A^3 + 27B^2$.

How many points are there on $E(\mathbb{F}_p)$?

Idea For $x \in \mathbb{F}_p$

for $\sim$ half of x, $x^3 + Ax + B$ is a QR $\Rightarrow$ 2 solns for y

for $\sim$ half of x, $x^3 + Ax + B$ a QNR $\Rightarrow$ 0 solns for y

for $\sim$ no x, $x^3 + Ax + B = 0$ $\Rightarrow$ 1 soln for y

$\Rightarrow$ Expect $\# E(\mathbb{F}_p) = p + 1$

$\mathcal{O}$.

Thm (Hasse's thm) $\left| \# E(\mathbb{F}_p) - (p+1) \right| \leq 2\sqrt{p}$.

There exists algorithms to count the points on an Elliptic curve in polynomial time: Schoof, Elkies, & Atkins.

Too advanced for this class (or for me).

As always, we prefer elliptic curves where $\# E(\mathbb{F}_p)$ has a large prime divisor q.

The Elliptic Curve discrete log problem

Given $P \in E(\mathbb{F}_p)$, have an exponential map

$$\mathbb{Z}/\mathrm{ord}(P) \underset{\log_P}{\overset{\exp_P}{\rightleftarrows}} \{\mathcal{O}, P, 2P, \cdots\} \subseteq E(\mathbb{F}_p)$$

$\log_P$ is the inverse to the exponential map.

$\rightsquigarrow$ Elliptic curve DLP.

Double & Add Algorithm (cf Fast powering)

We need to compute $\exp_P$ a lot for Elliptic curve cryptography. We can start by directly using fast powering algorithm:

To compute nP, write $n = \sum n_i 2^i$.

$$\Rightarrow nP = n_0 P + n_1 \cdot 2P + n_2 \cdot 4P + \cdots + n_k 2^k P.$$

If n has $k = \lceil \log_2 n \rceil$ bits, then at most k doublings, at most k additions. Time complexity $O(\log_2 n)$ is linear.

In Elliptic Curves, computing inverses is very easy:

$P: (x, y) \Rightarrow -P: (x, -y)$

$\Rightarrow$ improvement:

Double & Add & Subtract

Ex $7P = P + 2P + 4P$

$\rightarrow 7P = 8P - P$

Question Given n an integer how to write

$n = \sum a_i 2^i$ where $a_i \in \{-1, 0, 1\}$ w/ as few nonzero entries as possible?

Answer Can ensure no two consecutive coefficients are nonzero $\Rightarrow$ at most $1/2$ of coeffs nonzero.

$\Rightarrow \frac{3k}{2}$ steps: k doublings & $1/2 k$ additions.

Ex $11 = 1 + 2 + 2^3$

$1011 \Rightarrow 110(-1) \Rightarrow 10(-1)0(-1)$

Ex $10111 \Rightarrow 1100(-1) \Rightarrow 10(-1)00(-1)$

Algorithms for Elliptic curve DLP

(1) Brute force: Compute $P, 2P, \cdots$ $O(p)$ time.

(2) Baby-step Giant step

$N = ord(P)$, $n = \lfloor \sqrt{N} \rfloor + 1$

List 1 $O, P, 2P, \cdots, (n-1)P$

List 2 $Q, Q - nP, Q - 2nP, \cdots, Q - (n-1)nP$.

Time Complexity: $O(\sqrt{N})$ exponential time.

Fastest known algorithm is about this slow!

(3) Chinese Remander Theorem / index calculus based approach.