Women in Mathematics

Advanced Course : Review Session 1

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ given by a Weierstrass form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Then given a subgroup $\mathbb{G}$, there is a unique isogeny (up to isomorphism) $I_{\mathbb{G}} : E \to E_{\mathbb{G}}$ with kernel $\mathbb{G}$. Vélu gave the following formulae for $(x, y) \in E \setminus \mathbb{G}$:

$$\begin{aligned} I_{\mathbb{G}}(x,y) = \big(x \quad &+ \quad \sum_{P \in \mathbb{G}\setminus\{O_E\}} \frac{3x_P^2 + 2a_2x_P + a_4}{x - x_P} + 2\frac{x_P^3 + a_2x_P^2 + a_4x_P + a_6}{(x - x_P)^2}, \\ y \quad &- \quad y\big(\sum_{P \in \mathbb{G}\setminus\{O_E\}} \frac{3x_P^2 + 2a_2x_P + a_4}{(x - x_P)^2} + 4\frac{x_P^3 + a_2x_P^2 + a_4x + a_6}{(x - x_P)^3}\big)\big), \end{aligned}$$

and

$$E_{\mathbb{G}} : y^2 = x^3 + a_2x^2 + (a_4 - 5t)x + a_6 - 4a_2t - 7w,$$

where

$$\begin{aligned} t &= \sum_{P \in \mathbb{G}\setminus\{O_E\}} (3x_P^2 + 2a_2x_P + a_4), \\ u &= 2\sum_{P \in \mathbb{G}\setminus\{O_E\}} (x_P^3 + a_2x_P^2 + a_4x_P + a_6) \\ w &= u + \sum_{P \in \mathbb{G}\setminus\{O_E\}} x_P(3x_P^2 + 2a_2x_P + a_4). \end{aligned}$$

Exercice 1.

1. Let $E : y^2 = (x^2 + b_1x + b_0)(x - a)$. The point $(a, 0)$ has order 2. Compute the isogeny of kernel $\langle (a, 0) \rangle$ starting from E.
2. What is the complexity of an algorithm for computing an isogeny with kernel a group of order ℓ, based on this formula ?
3. Let $\pi_q : E \to E$ be the Frobenius endomorphism of E. Show that if $\pi(\mathbb{G}) \subseteq \mathbb{G}$, then the isogeny is defined over $\mathbb{F}_q$.

Exercice 2. Let ℓ be a prime such that $(\ell, q) = 1$. Show that there are $\ell + 1$ size ℓ subgroups of $E[\ell]$. Show that there are $\ell+1$ non-isomorphic degree ℓ-isogenies (defined over $\bar{\mathbb{F}}_p$) from every elliptic curve $E/\mathbb{F}_q$. What about ℓ^r ?

Exercice 3. [Galbraith's algorithm] Let $X_{q,\ell}$ be the isogeny graph whose vertices are supersingular curves defined over ℓ and whose edges are ℓ-isogenies, for some prime number ℓ. To find a path between two elliptic curves E_1 and E_2 in this graph, we start with $X_0 = j(E_1)$ and $Y_0 = j(E_2)$ and at every step i we compute $X_i = X_{i-1} \cup \delta_v(X_{i-1})$ and $Y_i = Y_{i-1} \cup \delta_v(Y_{i-1})$, where $\delta_v(X)$ is the set of vertices in the graph which are connected to a vertex in X by an edge of degree ℓ. The algorithm stops when $X_i \cap Y_i \neq 0$.

1. Give the pseudo-code for this algorithm.
2. Using the birthday paradox, show that the complexity of the algorithm is $O(\sqrt{q})$.