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 $G$, there is a unique isogeny (up to isomorphism) $I_G : E \to E_G$ with kernel $G$. Velu gave the following formulae for $(x, y) \in E \setminus G$:

$$I_G(x, y) = \left(x + \sum_{P \in G \setminus \{O_E\}} \frac{3x^2_p + 2a_2xp + a_4}{x - x_P} + \frac{2x^3 + a_2x^2p + a_4xp + a_6}{(x - x_P)^2} \right),$$

$$y = y\left(\sum_{P \in G \setminus \{O_E\}} \frac{3x^2_p + 2a_2xp + a_4}{(x - x_P)^2} + \frac{4x^3 + a_2x^2p + a_4x + a_6}{(x - x_P)^3}\right),$$

and

$$E_G : y^2 = x^3 + a_2x^2 + (a_4 - 5t)x + a_6 - 4a_2t - 7w,$$

where

$$t = \sum_{P \in G \setminus \{O_E\}} (3x^2_p + 2a_2xp + a_4),$$

$$u = 2 \sum_{P \in G \setminus \{O_E\}} (x^3_p + a_2x^2p + a_4xp + a_6),$$

$$w = u + \sum_{P \in G \setminus \{O_E\}} x_p(3x^2_p + 2a_2xp + a_4).$$

**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 $((a, 0))$ starting from $E$.

2. What is the complexity of an algorithm for computing an isogeny with kernel a group of order $\ell$, based on this formula?

3. Let $\pi_q : E \to E$ be the Frobenius endomorphism of $E$. Show that if $\pi(G) \subseteq G$, then the isogeny is defined over $\mathbb{F}_q$.

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

**Exercice 3.** [Galbraith’s algorithm] Let $X_{q, \ell}$ be the isogeny graph whose vertices are supersingular curves defined over $\ell$ and whose edges are $\ell$-isogenies, for some prime number $\ell$. 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 $X_i = X_{i-1} \cup \delta_\ell(X_{i-1})$ and $Y_i = Y_{i-1} \cup \delta_\ell(Y_{i-1})$, where $\delta_\ell(X)$ is the set of vertices in the graph which are connected to a vertex in $X$ by an edge of degree $\ell$. 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 $O(\sqrt{q})$. 

1