PCMI 2021: Supersingular isogeny graphs in cryptography

Exercises Lecture 1: Elliptic curves, Isogenies, CGL Hash Function

TA: Jana Sotáková **version July 26, 2021**

Use Magma to do the following exercises. If you need help to get started, please ask on the Discord!

1. (Elliptic curves) Over $\mathbb{F}_p$ for $p = 431$:
   (a) Define an elliptic curve $E/\mathbb{F}_p$ with $E : y^2 = x^3 + x$.
   (b) Compute its j-invariant;
   (c) Find an elliptic curve $E_1/\mathbb{F}_p$ with j-invariant 234;
   (d) Is this elliptic curve supersingular?
   (e) Find another elliptic curve E_2 with j-invariant 234. Are E_1 and E_2 isomorphic over $\mathbb{F}_p$? Can you find a non-isomorphic such pair? Hint[1]

2. (Isogenies) Compute the following for $E : y^2 = x^3 + x/\mathbb{F}_{431^2}$
   (a) Isogeny $\varphi : E \to E'$ with kernel generated by $(0, 0)$. What is the degree?
   (b) Compute the dual isogeny $\hat{\varphi} : E' \to E$;
   (c) Find all the isogenies of degree 2 from E.
   (d) Find all the cyclic isogenies of degree 16 from E.
   (e) Compute a cyclic isogeny of degree 16 as a sequence of 2-isogenies.

3. (Modular polynomial) Use the modular polynomial $\Phi_N(X, Y)$ to find isogenous curves:
   (a) Find all the 2-isogenies curves to $E : y^2 = x^3 + 26x + 279/\mathbb{F}_{431^2}$;
   (b) Find j-invariants of elliptic curves admitting a 16-isogeny from E. Hint[2]
   (c) Find all the self-loops in the ℓ-isogeny graph for $\ell \leq 11$.

4. (Supersingular isogeny graphs) Write code to generate the supersingular isogeny graph over $\mathbb{F}_{p^2}$, using the following steps. On input coprime primes p and ℓ;
   (a) Find one supersingular elliptic curve over $E_0/\mathbb{F}_{p^2}$, represented by the j-invariant;
   (b) Write a neighbor function that on input an elliptic curve E, finds all the neighbours of E in the SSIG $\mathcal{G}_\ell$: (the j-invariants) all the supersingular elliptic curves ℓ-isogenous to E.
   (c) Using a breadth-first-search approach, generate the graph by starting from the curve found in Step (b) and the Neighbor function from Step (c).

5. (If you've done Exercise 4), for primes $p \equiv 1 \bmod 12$, find the adjacency matrix A of the SSIG and find the diameter. SSIGs have very short diameters.

6. (CGL Hash function) For a small prime p and any starting supersingular elliptic curve E, find a collision for the CGL hash fuction on the 2-isogeny SSIG. I.e., find two strings that hash to the same elliptic curve. Hint[3]

---

[1] Quadratic twists.
[2] To deal with the large coefficients, reduce the polynomial to $\mathbb{F}_{p^2}$
[3] Requires you to decide on the ordering of the edges in the SSIG. Find two isogenies to the same curve.