

PCMI 2021: Supersingular isogeny graphs in cryptography

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

TA: Jana Sotáková

version July 27, 2021

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

- (Elliptic curves) Over \mathbb{F}_p for $p = 431$:
 - Define an elliptic curve E/\mathbb{F}_p with $E : y^2 = x^3 + x$.
 - Compute its j -invariant;
 - Find an elliptic curve E_1/\mathbb{F}_p with j -invariant 234;
 - Is this elliptic curve supersingular?
 - 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? Hint¹
- (Isogenies) Compute the following for $E : y^2 = x^3 + x/\mathbb{F}_{431^2}$
 - Isogeny $\varphi : E \rightarrow E'$ with kernel generated by $(0, 0)$. What is the degree?
 - Compute the dual isogeny $\hat{\varphi} : E' \rightarrow E$;
 - Find all the isogenies of degree 2 from E .
 - Find all the cyclic isogenies of degree 16 from E .
 - Compute a cyclic isogeny of degree 16 as a sequence of 2-isogenies.
- (Modular polynomial) Use the modular polynomial $\Phi_N(X, Y)$ to find isogenous curves:
 - Find all the 2-isogenies curves to $E : y^2 = x^3 + 26x + 279/\mathbb{F}_{431^2}$;
 - Find j -invariants of elliptic curves admitting a 16-isogeny from E . Hint²
 - Find all the self-loops in the ℓ -isogeny graph for $\ell \leq 11$.
- (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 ;
 - Find one supersingular elliptic curve over E_0/\mathbb{F}_{p^2} , represented by the j -invariant;
 - Write a neighbor function that on input an elliptic curve E , finds all the neighbours of E in the SSIG \mathcal{G}_ℓ : (the j -invariants) all the supersingular elliptic curves ℓ -isogenous to E .
 - 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).
- (If you've done Exercise 4), for primes $p \equiv 1 \pmod{12}$, find the adjacency matrix A of the SSIG and find the diameter. SSIGs have very short diameters.
- (CGL Hash function) For a small prime p and any starting supersingular elliptic curve E , find a collision for the CGL hash function on the 2-isogeny SSIG. I.e., find two strings that hash to the same elliptic curve. Hint³

¹Quadratic twists.

²To deal with the large coefficients, reduce the polynomial to \mathbb{F}_{p^2}

³Requires you to decide on the ordering of the edges in the SSIG. Find two isogenies to the same curve.