Problem Set 5

PAWS 2025

Nathaniel Hurst

1 Consider the following elliptic curves in short Weierstrass form defined over $\mathbb{F}_5$:

$$E_1 : y^2 = x^3 + x + 1 \quad E_2 : y^2 = x^3 + 3x + 1 \quad E_3 : y^2 = x^3 + 1$$

Which of the elliptic curves can be written in Montgomery form over $\mathbb{F}_5$? Find a coordinate transformation if it exists.

E_1 cannot be written in Montgomery form over $\mathbb{F}_5$, for if we write the transformation $x \mapsto ax + b$ and $y \mapsto cy$ we find that the constant term of the new equation is $b^3 + b + 1$, and since in Montgomery form the contstant term is zero, we must also have $b^3 + b + 1 = 0$. However this equation has no roots over $\mathbb{F}_5$. Thus E_1 cannot be written in Montgomery form.

E_2 can be written in Montgomery form. Applying the same trick as in the case of E_1 we solve for the roots of the equation $b^3 + 3b + 1 = 0$, which gives us $b = 1, 2$. Then setting $b = 1$ we solve

$$cy = \frac{a^3}{c}x^3 + \frac{3a^2}{c}x^2 + \frac{4a}{c}x$$

with the goal of the coefficients of x^3 and x being 1 and the coffecient of x^2 not being $2, 3$ (for if so $2^2 = 3^2 = 4$, and in Montgomery form we require $A^2 \neq 4$). Solving gives us $a = 3$ and $c = 2$. Then the coordinate transformation $x \mapsto 3x + 1$ and $y \mapsto 2y$ gives us the Montgomery form for E_2 over $\mathbb{F}_5$,

$$2y^2 = x^3 + x^2 + x$$

E_3 can be written in Montgomery form, and again we apply the same trick as in the case of E_1 and E_2. Setting $x \mapsto ax + b$ and $y \mapsto cy$ we find that the constant term of the new equation for E_3 is $b^3 + 1$, giving us the solution $b = 4$ for $b^3 + 1 = 0$. Then we aim to solve the equation

$$y^2 = \frac{a^3}{c^2}x^3 + \frac{2a^2}{c^2}x^2 + \frac{a}{c^2}x$$

for the coefficient of x^3 and x being 1 and the coefficient and x^2 not being a square root of 4. Solving gives us $a = 4$ and $c = 2$. Then the coordinate transformation $x \mapsto 4x + 4$ and $y \mapsto 2y$ gives us the Montgomery form for E_3 over $\mathbb{F}_5$,

$$y^2 = x^3 + 3x^2 + x$$

2 Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$. Show that the map

$$\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$$

defines an isogeny. This essentially requires showing two properties:

(a) π is well-defined, i.e. if $P = (x, y) \in E$, then $\pi(P) = (x^q, y^q) \in E$ as well.

(b) π is a group homomorphism.

Note that this is an example of an isogeny which is not separable.

(a) Observe that if $(x, y) \in E$ then $y^2 = x^3 + ax + b$, but raising both sides to the q power we see that

$$(y^q)^2 = (y^2)^q = (x^3 + ax + b)^q = (x^3)^q + (ax)^q + b^q = (x^q)^3 + ax^q + b$$

where we used the fact that in the binomial expansion of $(x^3 + ax + b)^q$ all terms with a factor of q go to zero (the curve is defined over $\mathbb{F}_q$) and so $(a + b)^q = a^q + b^q$. We also used the fact that $a, b \in \mathbb{F}_q$ and so $a^q = a$ and $b^q = b$. Thus we have that $(x^q, y^q) \in E$, or π is well-defined.

(b) Since the group law for an elliptic curve defined over $\mathbb{F}_q$ is given by rational functions whose coefficients are elements of $\mathbb{F}_q$ we have that if f is such a rational function, then $f(x^q) = f(x)^q$ (since if $a \in \mathbb{F}_q$ then $a^q = a$, and so $(ax)^q = ax^q$, this is similar to how we used the binomial formula in part (a)). But then if $P, Q \in E$ then $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and $\pi(P + Q) = (f(x_1, y_1, x_2, y_2)^q, g(x_1, y_1, x_2, y_2)^q)$. But then

$$\pi(P) + \pi(Q) = (x_1^q, y_1^q) + (x_2^q, y_2^q) = (f(x_1^q, y_1^q, x_2^q, y_2^q), g(x_1^q, y_1^q, x_2^q, y_2^q)) =$$

$$= (f(x_1, y_1, x_2, y_2)^q, g(x_1, y_1, x_2, y_2)^q) = \pi(P + Q)$$

and so π is a group homomorphism.

3

Let $(G, \circ)$ be a cyclic group with neutral element id and assume that $\#G = N$ is prime. Show that

$$(\mathbb{Z}/N\mathbb{Z})^* \times G \setminus \{\text{id}\} \to G \setminus \{\text{id}\}$$

$$(n, x) \mapsto \exp_x(n) = x \circ x \circ \ldots \circ x \quad (n \text{ times})$$

is a regular group action.

First observe that for all $g \in G$ we have that $1 \cdot g = g$ (by definition of the group action). Similarly observe that for $r, k \in (\mathbb{Z}/N\mathbb{Z})^*$ we have that $(rk) \cdot g = g \circ g \circ \ldots \circ g \quad (rk \text{ times})$, but this is the same as composing g with itself k times and then composing that result r times, i.e. $(rk) \cdot g = r \cdot (k \cdot g)$. Thus this is a group action.

Now let $a, b \in G$. Observe that since $\text{ord}(a) = N$ (since N is prime and $\text{ord}(a)$ divides N by Lagranges theorem) we have that $n \cdot a$ is a distinct element for each $n \in (\mathbb{Z}/N\mathbb{Z})^*$, and hence there must be only one element $\ell \in (\mathbb{Z}/\mathbb{Z})^*$ such that $b = \ell \cdot a$. Thus the action is also regular.

4

In this exercise we consider a group action based on matrix multiplication. Let $\mathbb{F}_p$ be a finite field (for some large prime p). Consider

$$G = \left\{ \begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix} \mid c_1, c_2 \in \mathbb{F}_p \right\}$$

$$X = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1, x_2 \in \mathbb{F}_p \right\} = \mathbb{F}_p^2$$

and the group action

$$\star : G \times X \to X, \quad (A, x) \mapsto A \cdot x$$

(a) Show that $\star$ defines a commutative group action. Is the group action regular?

(b) Sketch a Diffie–Hellman protocol based on the group action and convince yourself it works correctly.

(c) Show that $\star$ is **not** a cryptographic group action. Find a polynomial-time algorithm to solve GA-DLP for this group action.

(a) First observe that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{id}_G$ is such that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ for all $x_1, x_2 \in \mathbb{F}_p$. Similarly observe that for $\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}, \begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 \end{pmatrix} \in G$ and any $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in X$ we have that

$$\left(\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}\begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 \end{pmatrix}\right)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}\left(\begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right)$$

(matrix multiplication is associative since composition of linear maps is) Thus $\star$ is a group action. It is not regular however, for consider $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \in X$. Then observe that

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

This group action is however commutative, as

$$\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}\begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 \end{pmatrix} = \begin{pmatrix} c_1k_1 + c_2k_2 & c_1k_2 + c_2k_1 \\ c_2k_1 + c_1k_2 & c_2k_2 + c_1k_1 \end{pmatrix} = \begin{pmatrix} k_1c_1 + k_2c_2 & k_1c_2 + k_2c_1 \\ k_2c_1 + k_1c_2 & k_2c_2 + k_1c_1 \end{pmatrix} = \begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 \end{pmatrix}\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}$$

(where we used the fact that elements in $\mathbb{F}_p$ commute).

(b) Alice and Bob pick private matrices $A = \begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 \end{pmatrix}, B = \begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}$ respectively, and agree on a public parameter $P = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Alice's public key is $A \cdot P$ and Bob's public key is $B \cdot P$. Then they each take the others public key and compute the shared key

$$B \cdot (A \cdot P) = (BA) \cdot P = (AB) \cdot P = A \cdot (B \cdot P)$$

(c) Observe that given $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ with

$$\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

we can set up the following system over $\mathbb{F}_p$,

$$c_1x_1 + c_2x_2 = y_2$$

$$c_2x_1 + c_1x_2 = y_2$$

which can be solved in $O(n^3)$ time.

5

Let $\star : G \times X \to X$ be a group action, and assume that the group action is effective. In particular, you may assume the following operations can be performed efficiently.

(i) Evaluating the group action: Given $g \in G, x \in X$, compute $g \star x$.

(ii) Group operation: Given $g_1, g_2 \in G$, compute $g_1 \circ g_2$.

(iii) Equivalence checking: Given $x, x' \in G$, decide if $x = x'$.

(a) First consider a cyclic group, i.e. assume that $G \cong \mathbb{Z}/N\mathbb{Z}$ for some N. Find an algorithm to solve GA-DLP in time $O\left(\sqrt{N}\right)$ in this setting.

(b) Now assume that G is an arbitrary abelian group, i.e. $G \cong \mathbb{Z}/N_1\mathbb{Z} \times ... \times \mathbb{Z}/N_r\mathbb{Z}$ for some integers $N_1, ..., N_r$ with $N_{i+1} \mid N_i$ for all $i = 1, ..., r-1$. Adapt the algorithm from (a) to solve GA-DLP in this setting.

(Hint: It makes sense to first consider the case $r = 2$. Is there a difference between the cases $N_1 = N_2$ and $N_2 \ll N_1$)

(a) We will adapt the Pollard's Rho algorithm to a group action setting. Let $G \cong \langle a \rangle \cong \mathbb{Z}/N\mathbb{Z}$. We aim to find g given $x, y \in X$ such that $g \cdot x = y$. Then we define the following function which takes a random number and an element of X and outputs an element of X.

$$f(n, a^r \cdot x) = \begin{cases} a^{2r} \cdot x & \text{if } n \equiv 0 \pmod 2 \\ a^{r+1} \cdot x & \text{if } n \equiv 1 \pmod 2 \end{cases}$$

(where it is understood that at each step we keep track of the group element a^k in $a^k \cdot x$ in order to keep applying f based on the current a^k) First we initialize by computing two random numbers n_1, n_2 and setting $x' = f(n_1, x)$ and $y' = f(n_2, y)$. Then at every step we generate two new random numbers n_1, n_2 and compute $x' \leftarrow f(n_1, x')$ and $y' \leftarrow f(n_1, y')$. Then we check if

$$a^k \cdot x = x' = y' = a^p \cdot y$$

in which case we can deduce that

$$a^{k-p} \cdot x = y$$

If our function is sufficiently random we will have a collision in $O\left(\sqrt{N}\right)$ time.

(b) In the case of a general abelian group, say $G \cong \mathbb{Z}/N_1\mathbb{Z} \times ... \times \mathbb{Z}/N_r\mathbb{Z} \cong \langle a_1 \rangle \times ... \times \langle a_r \rangle$ we define a new function as an adaptation of the old one,

$$f(n, (a^{r_1}, ..., a^{r_n}) \cdot x) = \begin{cases} (a^{2r_1}, ..., a^{2r_n}) \cdot x & \text{if } n \equiv 0 \pmod 2 \\ (a^{r_1+1}, ..., a^{r_n+1}) \cdot x & \text{if } n \equiv 1 \pmod 2 \end{cases}$$

in this way we preserve the randomness, essentially applying the f from part (a) to each component individually.

6

Let $\mathbb{F}_q$ be a finite field, $k < n$ integers, and let $X = \mathbb{F}_q^{k \times n}$ be the set of $k \times n$ matrices over $\mathbb{F}_q$. Further we define $G = GL_k(\mathbb{F}_q) \rtimes P_n$, where $GL_k(\mathbb{F}_q)$ are invertible $k \times k$ matrices over $\mathbb{F}_q$ and P_n is the group of $n \times n$ permutation matrices.

We consider the group action

$$\star : G \times X \to X, \quad ((S, P), A) \mapsto S \cdot A \cdot P$$

(a) Let $q = 3, k = 2, n = 4$, and consider the following matrices

$$A_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Find $g = (S, P) \in G$ so that $g \star A_1 = SA_1P = A_2$. Is the solution unique?

(b) In the setting of (a), consider

$$A_3 = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Is there an element $g \in G$ so that $g \star A_1 = A_3$?

(c) Is the group action $\star$ free, transitive, or regular?

(a) Observe that

$$\left(\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

additionally, by a manual search, we find that this solution is unique.

(b) By a manual search we find that no such g exists.

(c) The group action is not free, as $(S, P) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ for any $(S, P) \in G$. This also shows the group action is not transitive or regular, as the orbit of $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ is just itself and there is no unique (S, P) such that $(S, P) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

7

Use Sage to sketch the CSIDH graph with $p = 59 = 4 \cdot 3 \cdot 5 - 1$ (as in Example 4.26).

(a) Verify that the supersingular Montgomery coefficients are $A = 0, 6, 11, 28, 29, 30, 31, 48, 53$.

(b) To draw edges corresponding to 3-isogenies: For each curve E_A, compute a point $P_3 \in E_A[3](\mathbb{F}_p)$, a 3-isogeny φ_3 with $\ker(\varphi_3) = \langle P_3 \rangle$, and the codomain of φ_3 (in Montgomery form).

(c) To draw edges corresponding to 5-isogenies: For each curve E_A, compute a point $P_5 \in E_A[5](\mathbb{F}_p)$, a 5-isogeny φ_5 with $\ker(\varphi_5) = \langle P_5 \rangle$, and the codomain of φ_5 (in Montgomery form).

Code for verifying supersingular coefficients and computing 3/5 isogenies can be found in the file supersingular_p=59.ipynb. Using this we sketch the CSIDH graph with $p = 59$:

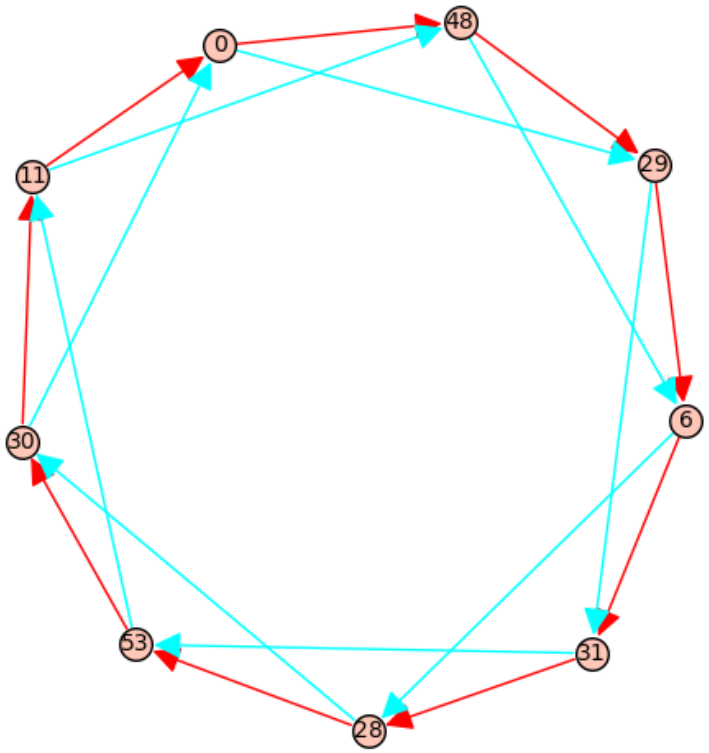


Figure 1: Vertex labels correspond to supersingular coefficients. Red edges are 3-isogenies and blue edges are 5-isogenies.

8

In this exercise, we analyze the setting of CSIDH for $p = 59$ in more detail. Assume that the secret key space is $\{-2, -1, 0, 1, 2\}^2$.

(a) Say Alice's public key is $A = 28$. What was her secret key? In other words, what is $\log_{E_0}(E_{28})$? Is the answer unique?

(b) Say Bob's public key is $B = 11$. What is the shared session key? Is the answer unique?

(c) Is the group action $\star : \{-2, -1, 0, 1, 2\} \times V \to V$ transitive? Is it free?

(d) Now consider the smaller secret key space $\{-1, 0, 1\}^2$. Is the group action $\star : \{-1, 0, 1\} \times V \to V$ transitive? Is it free?

(e) Describe the relations between possible secret keys in $\mathbb{Z}^2$, and represent the equivalence classes of secret keys as $\mathbb{Z}^2/\Lambda$, where Λ is a lattice $\Lambda \subset \mathbb{Z}^2$. Is the group action $\star : \mathbb{Z}^2/\Lambda \times V \to V$ transitive? Is it free?

Here is the CSIDH graph for $p = 59$:

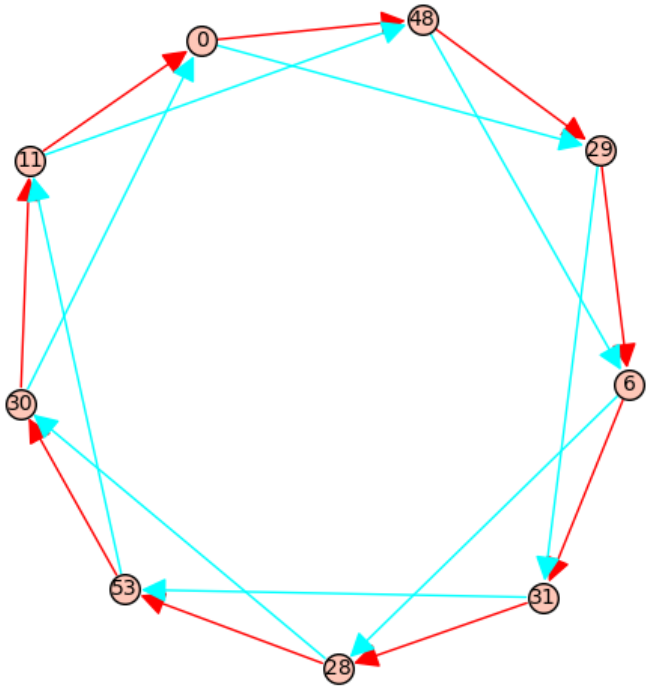


Figure 2: Vertex labels correspond to supersingular coefficients. Red edges are 3-isogenies and Blue edges are 5-isogenies.

(a) Starting at the vertex 0 we see that there are several secret keys which correspond to walking along the CSIDH graph to get the vertex 28. If $(x, y) \in \{-2, -1, 0, 1, 2\}^2$ corresponds to walking x 3-isogeny edges and then y 5-isogeny edges we have that Alice's secret key could be

$$(0, -2), \quad (1, 2), \quad (-2, -1)$$

(b) In all three cases of Alice's secret key, we have that the shared session key will be E_{31}.

(c) The group action is transitive, since every vertex can be reached by starting at the vertex E_0 and applying some $(x, y) \in \{-2, -1, 0, 1, 2\}^2$. It is not however free, for observe that starting at E_0 and applying the element $(2, -1)$ yeilds the vertex E_0 again.

(d) The group action is not transitive, there is no way to reach the vertex E_{28} from the vertex E_0 with this smaller keyspace. It is however free as if an element (x, y) fixes an vertex and is not $(0, 0)$ then this would correspond to having both a 3 and 5 isogeny between two vertices, which does not happen.

(e) The lattice $\Lambda \subseteq \mathbb{Z}^2$ represents the set of points $(x, y) \in \mathbb{Z}^2$ such that for any vertex v in the CSIDH graph we have $(x, y) \cdot v = v$. Λ is a subgroup, for it is closed under addition and inversion, and contains $(0, 0)$. Then when we consider the quotient group $\mathbb{Z}^2/\Lambda$ and the group action $\mathbb{Z}^2/\Lambda \times V \to V$ given by $(x, y)\Lambda \cdot v = (x, y) \cdot v$ (this is well defined for if $(x_1, y_1)\Lambda = (x_2, y_2)\Lambda$ then $(x_1, y_1) - (x_2, y_2) \in \Lambda$, or $[(x_1, y_1) - (x_2, y_2)] \cdot v = v$, and so $(x_1, y_1) \cdot v = (x_2, y_2) \cdot v$) we have that necessarily it is transitive (since we already deduced that the group action only using $\{-2, -1, 0, 1, 2\}^2$ is transitive, and $\{-2, -1, 0, 1, 2\}^2 \subseteq \mathbb{Z}^2$). Similarly it is also free, since if $(x, y)\Lambda \cdot v = v$ for all vertices v then $(x, y) \in \Lambda$, or $(x, y)\Lambda = \Lambda$.

9

We consider a CSIDH graph for some prime $p = 4 \cdot \ell_1 ... \ell_n - 1$.

(a) Let A be the label of a vertex in the CSIDH graph. Show that there exists a vertex with label $-A$ as well.

(b) Consider $E_0 : y^2 = x^3 + x$. Let $P_1 = (x_1, y_1) \in E(\mathbb{F}_p)$ and denote $\text{ord}(P_1) = N$ for some $N \mid p + 1$. Show that $P_{1'} = (x_1, iy_1) \in E(\mathbb{F}_{p^2})$, and moreover $\text{ord}(P_{1'}) = N$ as well.

(c) Now consider the isogeny $\varphi : E_0 \to E$ with kernel $\langle P_1 \rangle$. Using Vélu's formulas, one finds that $E : y^2 = x^3 + ax + b$ for some a, b. Further consider the isogeny $\psi : E \to E'$ with kernel $\langle P_{1'} \rangle$. Show that $E' : y^2 = x^3 + ax - b$.

(a) We will show that $\#E_A(\mathbb{F}_p) = \#E_{-A}(\mathbb{F}_p)$, and thus E_A is supersingular if and only if E_{-A} is. Let $(x, y) \in E_A(\mathbb{F}_p)$ i.e. $By^2 = x^3 + Ax^2 + x$ for some $B \in \mathbb{F}_p$. Then define E_{-A} by the equation $-By^2 = x^3 - Ax^2 + x$. Then $(-x, y) \in E_{-A}(\mathbb{F}_p)$ since

$$By^2 = x^3 + Ax^2 + x \implies -By^2 = (-x)^3 - Ax^2 - x$$

Thus $\#E_A(\mathbb{F}_p) \leq \#E_{-A}(\mathbb{F}_p)$. Then similarly if $(x, y) \in E_{-A}(\mathbb{F}_p)$ then $-By^2 = x^3 - Ax^2 + x$, and applying the same trick as before we see that $(-x, y) \in E_A(\mathbb{F}_p)$. Thus $\#E_{-A}(\mathbb{F}_p) \leq \#E_A(\mathbb{F}_p)$, and so we can conclude that $\#E_{-A}(\mathbb{F}_p) = \#E_A(\mathbb{F}_p)$, and so there exists a vertex with label $-A$.

(b) and (c) Ommited, to be revisited.

10

Let ℓ be a prime such that $(\ell, p) = 1$. One can define the **supersingular ℓ-isogeny graph** whose vertices are supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphisms), and whose edges are ℓ-isogenies between supersingular elliptic curves.

As seen in Remark 4.25.v, we can assume the graph is undirected since each isogeny $\varphi : E \to E'$ can be associated to the dual one $\hat{\varphi} : E' \to E$. Also, we consider two ℓ-isogenies equivalent if they have the same kernel. One way to phrase a fundamental problem in isogeny-based cryptography is: "Given two supersingular elliptic curves, find a path between them in the supersingular ℓ-isogeny graph."

(a) In the lecture, **supersingular** was defined only for elliptic curves over $\mathbb{F}_{p^2}$. Over $\mathbb{F}_{p^2}$ an elliptic curve E is supersingular if and only if $\#E(\mathbb{F}_p) - p^2 - 1 \equiv 0 \pmod{p}$. List all supersingular curves over $\mathbb{F}_{59^2}$.

(b) To label the vertices we need a unique identifier. Before we used the Montgomery coefficient, but now we need a more general one: the j-invariant. For an elliptic curve in short Weierstrass form $y^2 = x^3 + ax + b$, the j-invariant is given by

$$j = 1728\frac{4a^3}{4a^3 + 27b^2}$$

(i) Compute the j-invariants for the two elliptic curves $E : y^2 = x^3 + x$ and $E' : y^2 = x^3 + 1$. (We have seen previously that E is supersingular if and only if $p \equiv 3 \pmod 4$ and E' is supersingular if and only if $p \equiv 2 \pmod 3$.) (ii) Compute the j-invariants corresponding to vertices in CSIDH for $p = 59$.

(c) Show that there are $\ell + 1$ edges starting at any given vertex.

(Hint: each edge corresponds to a subgroup of $E[\ell]$ of order ℓ)}

(d) Generate the 3-isogeny graph for $p = 59$, using the following code:

sage: E = EllipticCurve(GF(59^2), j=1728) sage: G = E.isogeny_ell_graph(3, directed=False, label_by_j=True) sage: G.show()

(i) Check that the graph has the properties you expect (i.e. has all the correct j-invariants and has 4 outgoing edges from each vertex), except at $j = 0, 1728$. One can use $p \equiv 1 \pmod{12}$ to avoid this issue at $j = 0, 1728$.

(ii) Do the same for $\ell = 5$.

(iii) Compare these graphs to the CSIDH graph for $p = 59$.

(iv) Do the same for $p = 419$ and compare to the CSIDH graph.

(v) Do the same for $p \equiv 1 \pmod{12}$ and see if the graph changes.

(a) Using SageMath we find that the supersingular curves over $\mathbb{F}_{59^2}$ are curves of the form $y^2 = x^3 + Ax^2 + x$ for A in

$$\{0, 51i + 56, 7i + 26, 47i + 6, 45i + 31, 28, 44i + 37, 56i, 14i + 17, 3i + 56, 53, 8i + 48,$$

$$11, 27i + 16, 29, 8i + 3, 52i + 33, 12i + 53, 14i + 28, 31, 15i + 22, 3i, 45i + 42,$$

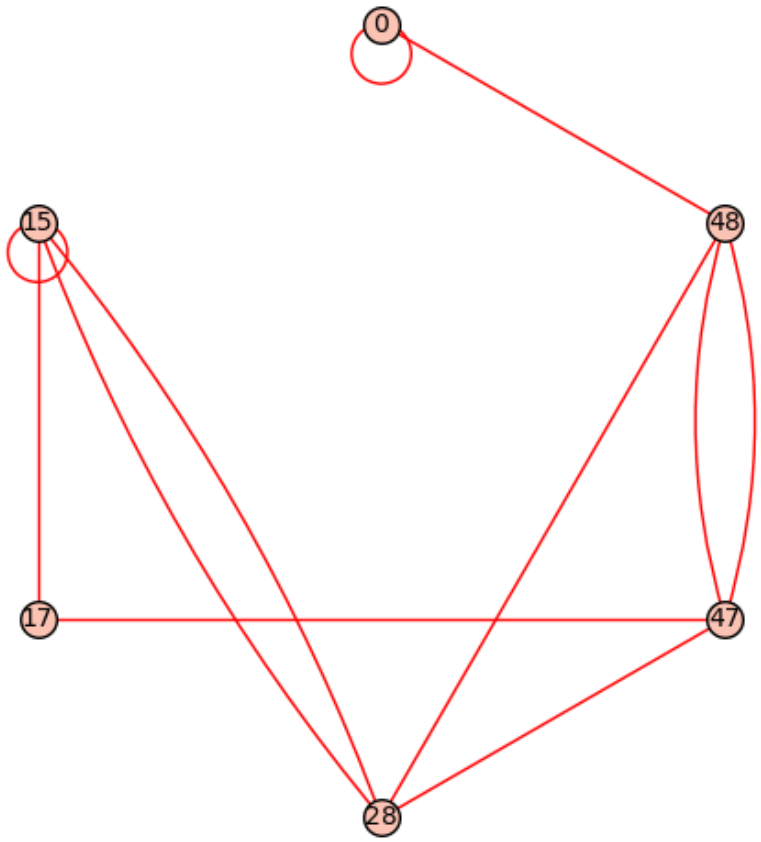
$$56i + 3, 6, 51i + 11, 48, 32i + 43, 30\}$$

(b) (i) For E we have $a = 1$ and $b = 0$ and so the j invariant is 1738. Similarly since for E' we have $a = 0$ and $b = 1$ we have that the j invariant is 0.

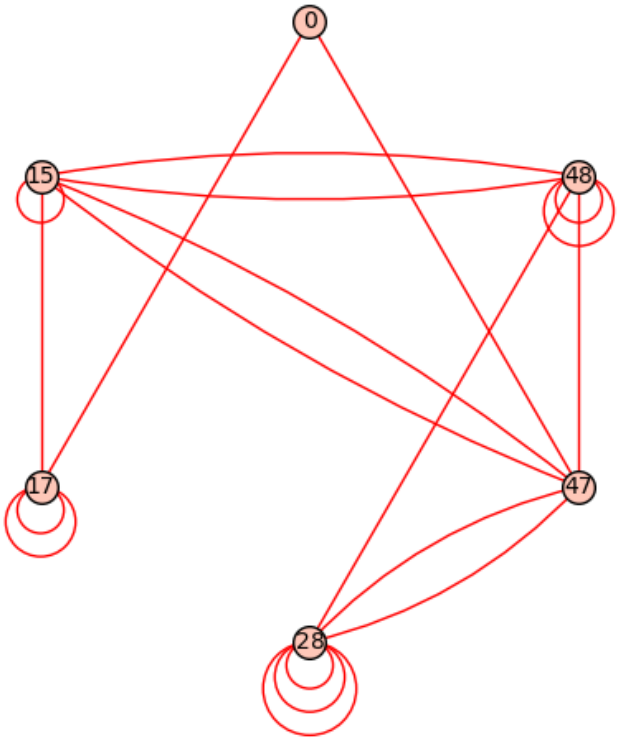
(ii) Using SageMath to convert the Montgomery form supersingular curves to Weierstrass form and computing their j invariants we have that the j invariants corresonding to vertices in CSIDH for $p = 59$ are: $17, 48, 0, 28, 47$.

(c) Ommited, to be revisited.

(d) (i) Here is the 3-isogeny graph for $p = 59$:

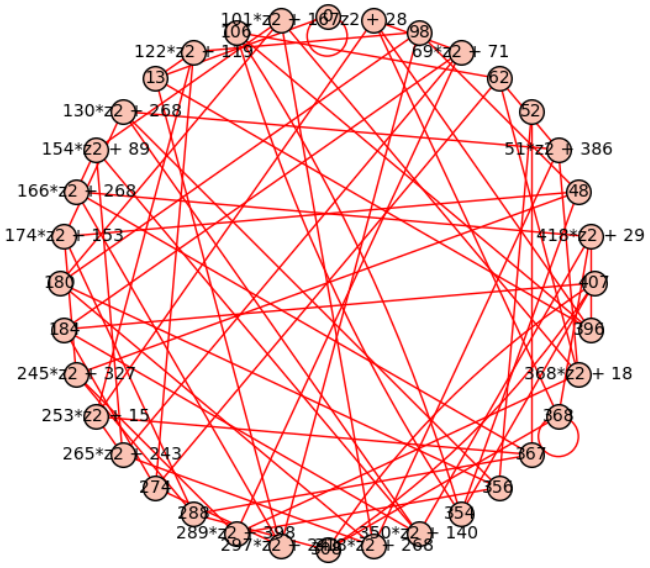


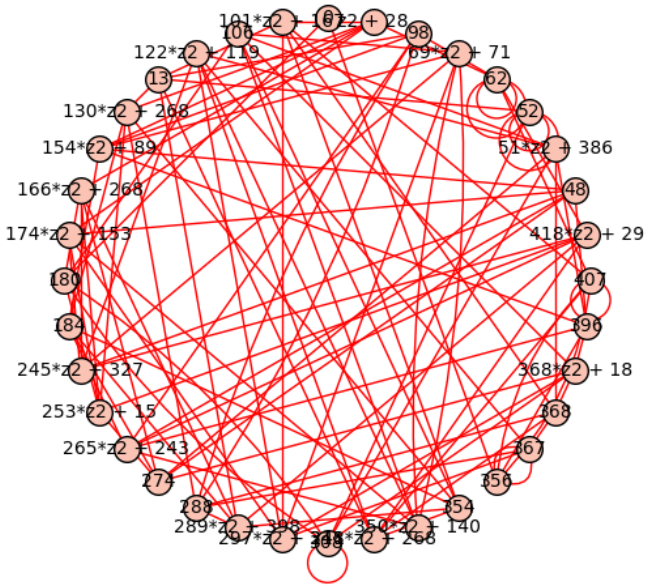
(ii) Here is the 5-isogeny graph for $p = 59$:

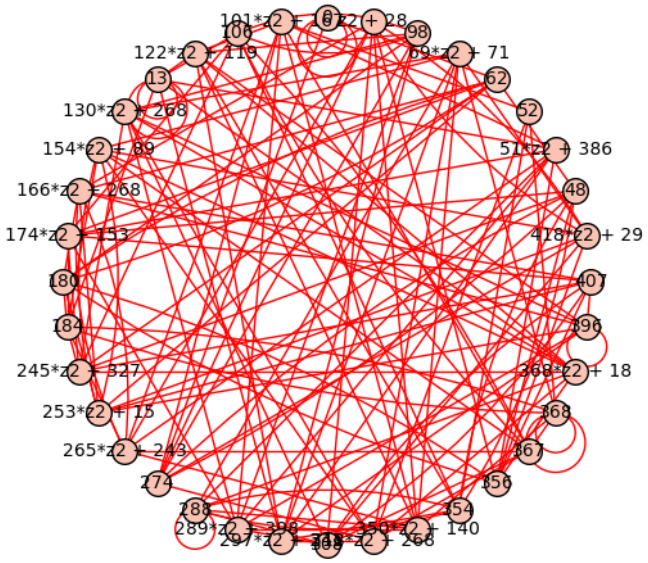


(iii) Comparing to the CSIDH graph for $p = 59$ we see that (for many of the edges, there are some unaccounted for) the 3 and 5 isogeny graphs looks like the same graph but we have merged vertices with the same j invariant, creating a non-simple graph. (just my non-rigorous observation)

(iv) Here are the $3, 5, 7$-isogeny graphs for $p = 429$ (not very pretty!)







(v) Using the code in the file CSIDH-graph.sage we see that (testing only a few such $p \equiv 1 \pmod{12}$) that quite a few of these graphs contain only one vertex. We cannot generalize this however, as certain counterexamples exist, such as the 5-isogeny graph for $p = 109$:

