Genus theory and attacking CSIDH-like cryptosystems

Jana Sotáková*

QuSoft/University of Amsterdam

Abstract

In this part of the Week 6 of the Isogeny School 2020, we study the schemes based on the group action of a certain class group in an imaginary quadratic field on a set of elliptic curves, such as the Couveignes and Rostovtsev-Stolbunov schemes and CSIDH and CSURF. These notes are based on the paper [4].

Usually, we do not assume more structure than a free and transitive group action on a set: that we have a group action, which is efficiently instantiated on the set of elliptic curves by computing isogenies. However, we will see that finer information about the class group can sometimes give us pretty interesting information and even lead to attacks on some computational assumptions.

There are two kinds of exercises for you to try. The ones marked "Exercise" should be solvable by the techniques introduced in this write-up, the ones marked "Exploration" might require you to look up more details online, code a few examples, discuss with others.

Contents

*Date: August 12, 2021. E-mail: j.s.sotakova@uva.nl.

1 Computational isogeny assumptions

In this section, we first repeat the Couveignes[5] and Rostovtsev-Stolbunov[10] schemes (CRS), of which CSIDH[3] is an improvement and instantiation, as it uses supersingular curves rather than ordinary curves. These protocols are based on an abelian group action of a certain class group in an imaginary quadratic field.

In this section, we focus on the cryptographic assumptions underlying the security of these schemes.

1.1 CSIDH and CRS schemes

In this section we briefly recall the notation for commutative isogeny-based key exchange schemes, which you have already seen in Week 3. These scheme feature two parties, Alice and Bob, who communicate over a public channel and want to agree on a shared secret.

Alice and Bob first agree on an elliptic curve $E/\mathbb{F}_q$ with an endomorphism ring contained in an imaginary quadratic field. Write $\#E(\mathbb{F}_q) = q+1-t$ for some t, called the trace (of Frobenius). Then the endomorphism ring (over $\mathbb{F}_q$) is an order $\mathcal{O} \supset \mathbb{Z}[\sqrt{t^2-4q}]$ with discriminant $\Delta \mid t^2-4q$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{t^2-4q})$. For concreteness, remember that in CSIDH, the choice is $\mathbb{Z}[\sqrt{-p}]$ for $p \equiv 3 \bmod 4$ and $E : y^2 = x^3 + x$ is supersingular. However, the results from this module are most interesting for E supersingular and $p \equiv 1 \bmod 4$ (hence "CSIDH-like schemes"), or E ordinary (Couveignes and Rostovtsev-Stolbunov protocols).

These key exchange schemes rely on a group action of the class group $\mathrm{cl}(\mathcal{O})$ on the set of elliptic curves isogenous to E. By Tate's theorem, two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same number of points. Hence isogenous curve have the same number of points, which is equal to $\#E(\mathbb{F}_q) = q+1-t$ for the same t, called the trace (of Frobenius). We consider the set of curves with the same endomorphism ring and trace, up to isomorphisms:

$$\mathscr{Ell}_q(\mathcal{O}, t) := \{E'/\mathbb{F}_q : \mathrm{End}_{\mathbb{F}_q}(E') \cong \mathcal{O} \text{ and } \#E'(\mathbb{F}_q) = q+1-t\}/\{\mathbb{F}_q\text{-isomorphisms}\}$$

Then the class group $\mathrm{Cl}(\mathcal{O})$ has a free and transitive action on $\mathscr{Ell}_q(\mathcal{O}, t)$ and this action is computed by isogenies. We will denote the classes in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{a}]$ and ideals by the\mathfrak font, so $\mathfrak{a} \in [\mathfrak{a}]$ is a representative of the class in the class group.

Alice chooses an ideal $\mathfrak{a}$ and computes her public key $E_A = [\mathfrak{a}] \star E$, Bob chooses an ideal $\mathfrak{b}$ and computes his public key $E_B = [\mathfrak{b}] \star E$. They exchange E_A and E_B over the public channel and each perform another isogeny corresponding to the secret ideal they hold and both obtain $E_{AB} = [\mathfrak{ab}] \star E$.

1.2 Security assumptions

At the end of the key exchange, Alice and Bob end up with the same elliptic curve $E_{AB} = [\mathfrak{ab}] \star E$. But how much guarantee do we have that only Alice and Bob hold the value E_{AB}? In cryptography, we formalize our security conditions by reductions to problems, which we consider hard - which we do not know how to solve efficiently. We focus on explaining and motivating the security assumptions, not on their formal definitions. All the curves need to lie in the same $\mathscr{Ell}_q(\mathcal{O}, t)$.

Group Action Inverse Problem (GAIP) The curves E, E_A, E_B are all public information - they are public keys, transmitted over an insecure channel that anyone can eavesdrop on. So, a necessary condition is that upon seeing E and E_A (and the implicit the setup data like $\mathbb{F}_q$, trace t, endomorphism ring), nobody can recover the secret ideal class $\mathfrak{a}$ satisfying $E_A = \mathfrak{a} \star E$. Because if you can recover $\mathfrak{a}$ from E and E_A, you can impersonate Alice and in particular, you can use $\mathfrak{a}$ to compute the shared elliptic curve E_{AB} from Bob's curve E_B.

The Group Action Inverse Problem (GAIP) assumption: On input E, E_A, no adversary running in polynomial time[1] can compute $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ satisfying $E_A = [\mathfrak{a}] \star E$ with better than negligible probability[2].

Naturally, there are pairs of elliptic curves E, E_A for which the GAIP is easy: for instance, if $E_A = E$. Therefore, the correct definition needs to include that the curve E_A is random. Similar issue applies in all the following problems.

The GAIP problem is the analogue of the discrete logarithm problem. It is also called the vectorization problem: think of having two points in an affine space (which has a free and transitive group action by the underlying vector space) and trying to figure out a vector that translates one point to the other.

Computational Diffie-Hellman assumption (CDH) The hardness of the GAIP is certainly necessary but not sufficient for the key exchange to be secure. An adversary does not have to be able to recover the secret keys: perhaps they can compute the shared secret E_{AB} without being able to solve the GAIP problem. But obtaining E_{AB} is enough for the adversary: they can clearly break the whole key exchange, because they now wield the value that only Alice and Bob were supposed to have in the end.

Computational Diffie-Hellman assumption for isogeny group actions (CDH): On input $E, E_A := [\mathfrak{a}] \star E, E_B := [\mathfrak{b}] \star E$, no adversary running in polynomial time can output an elliptic curve E_{AB} such that $E_{AB} = [\mathfrak{ab}] \star E$ with better than negligible probability.

The CDH problem is also called the parallelization problem: again in the affine space analogy, this problem translates to having a segment from E to E_A, and trying to construct a parallel segment of the same length from the point E_B. The CDH is a stronger assumption than GAIP: if an adversary can solve the GAIP problem, then you can modify the adversary to also solve the CDH problem.

It might seem that if the CDH problem is hard then the curve E_{AB} is random. But this is not true in general: just because you cannot compute E_{AB} completely, it does not mean that you cannot for instance guess the first or the last bit of the bit representation of its coefficients. Or guess any other bit of information. Depending on what you use the elliptic curve E_{AB} for, this might be an issue.

Decisional Diffie-Hellman assumption (DDH) Ideally, Alice and Bob would like to use their shared elliptic curve in some further cryptographic primitives, such as symmetric encryption (think AES, or more generally block ciphers). But symmetric encryption needs random bit strings as keys (random elements of $\{0,1\}^n$, typically $n = 128$ or $n = 256$). So you would like the elliptic curve to look as random as possible (we'll discuss below what exactly we mean by this). Similarly, if you would like to construct more advanced cryptographic applications of isogenies (such as the hash proof systems mentioned by Luca de Feo in Week 5), the elliptic curve E_{AB} needs to look sufficiently random.

Exercise 1.1. *Suppose that $E/\mathbb{F}_p$ is supersingular with a Montgomery form $E : y^2 = x^3 + Ax^2 + x$. Explain why A is not a random element of $\mathbb{F}_q$: give a polynomial time algorithm that distinguishes A from a random element in $\mathbb{F}_p$. Adapt your algorithm to show that the j-invariant $j(E)$ of a supersingular elliptic curve is not a random element of $\mathbb{F}_p$.*

The most extreme property we can ask of the shared key E_{AB} is that this elliptic curve looks like any other elliptic curve, that the Diffie-Hellman like protocol does not produce any biases in the elliptic curves, which could be used to link the curve E_{AB} to the elliptic curves E_A and E_B.

The Decisional Diffie-Hellman assumption (DDH): The adversary plays the following game: they are given a tuple of elliptic curves $(E, E_A, E_B, E_C) = (E, [\mathfrak{a}] \star E, [\mathfrak{b}] \star E, [\mathfrak{c}] \star E)$, with $[\mathfrak{c}] = [\mathfrak{ab}]$ with probability $1/2$ and $[\mathfrak{c}] \leftarrow^{\$} \mathrm{Cl}(\mathcal{O})$ (sampled randomly from $\mathrm{Cl}(\mathcal{O})$) with probability $1/2$). The adversary then needs to say whether the tuple they are given is of the first or the second kind, that is, whether $E_C \stackrel{?}{=} E_{AB}$, or equivalently, $[\mathfrak{c}] \stackrel{?}{=} [\mathfrak{ab}]$. Note that the adversary is not given $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ but only the curves E_A, E_B, E_C. The DDH assumption says that no polynomial time adversary can win this game with probability better than $1/2 +$ negligible.

[1] In the size of the input, that is, polynomial in $\log q$.

[2] This last part means that a guessing adversary (which can run in polynomial time) can sometimes guess correctly, but the probability of guessing correctly is *negligible* - think on the order of inverse exponential $2^{-\log q} = O(1/q)$.

One way to read the DDH assumption is that even after seeing the transcript of the Diffie-Hellman exchange, that is, knowing E, E_A, E_B, your only way of distinguishing the shared key E_{AB} from a random curve E_C is not much better than guessing. The DDH assumption is a stronger assumption that CDH: an adversary that can compute the curve E_{AB} can be used to distinguish E_{AB} from a random curve E_C.

Exercise 1.2. *DDH for multiplicative groups. Let p be a prime. Show that the DDH problem is not hard for the group $(\mathbb{Z}/p\mathbb{Z})^\times$, that is, if g is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $a, b, c \in \mathbb{Z}$ random, then we can distinguish the tuple (g, g^a, g^b, g^{ab}) from the tuple (g, g^a, g^b, g^c) with better probability than $1/2 +$ negligible. Calculate the probability of your attack succeeding.*

Exercise 1.3. *Figure out a countermeasure to your attack to the exercise above.*

1.3 Summary

We reviewed the group action-based isogeny schemes and defined the GAIP, CDH and DDH assumptions.

Exploration 1.4. *Formulate the Computational and Decisional Diffie-Hellman problems for SIDH. Determine whether thus defined DDH problem is equivalent to the computational problem.*

2 The Tate pairing

Let $E/\mathbb{F}_q$ be an elliptic curve. A pairing is a bilinear map $E \times E \to \mathbb{F}_q$. Pairings can be very strong tools in any cryptographic protocol using elliptic curves - both in a destructive and a constructive way. The main destructive property is that one can use pairings to transfer the discrete logarithm problem for points on a elliptic curve $E/\mathbb{F}_q$ to a finite field $\mathbb{F}_{q^k}$, which can be much much easier - especially if k is small, which is the case for supersingular elliptic curves. On the other hand, the bilinearity of pairings allows you to play various new tricks, such as a Diffie-Hellman protocol for 3 parties and other cool constructions from pairing-based cryptography. Arguably the most famous pairing for elliptic curves is the Weil pairing, which you can read more about in Week 5's notes. We will focus on the Tate pairing.

For us, the most relevant property of pairings is that they often work well with isogenies. However, the main drawback is that to obtain information on (the degrees of) isogenies using pairings, you need to know the images of the points you are pairing, and this is in general a hard problem to do. In fact, the SiGamal scheme from Week 3 is based on the very problem of not being able to distinguish the image of a point of order 2^r under a secret isogeny of odd degree from a random point of order 2^r on the target curve[3]!

2.1 Definition of the Tate pairing

Let $E/\mathbb{F}_q$ be an elliptic curve and let m be an odd prime. Assume that $\mu_m \subset \mathbb{F}_q$. The (reduced) Tate pairing is a non-degenerate bilinear pairing

$$\begin{aligned} T_m : \qquad E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) &\longrightarrow \mu_m \subset \mathbb{F}_q^* \ , \\ (P, Q) &\longmapsto T_m(P, Q) \ ; \end{aligned}$$

bilinear means that it is linear in both components and non-degeneracy means that for any $P \in E(\mathbb{F}_q)[m]$ there exists a point $Q \in E(\mathbb{F}_q)$ such that the pairing $T_m(P, Q) \neq 1$.

The Tate pairing is compatible with isogenies: Consider an isogeny $\varphi : E \to E'$, then

$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg(\varphi)}.$$

[3]This is the Points-Commutative Supersingular Isogeny Decisional Diffie-Hellman assumption, see Def 4 in Week 3 notes.

So, Tate pairing can reveal the degree of the isogeny. This is great news: if we can find two points P, Q and their images $\varphi(P), \varphi(Q)$, then by taking discrete logarithms for m-th roots of unity we can recover $\deg(\varphi) \bmod m$. But the isogeny φ we would like to study is the secret isogeny $E \to [\mathfrak{a}]\star E$, so we immediately run into problems:

1. We do not known the (secret) isogeny φ, and in general are unable to compute the images $\varphi(P), \varphi(Q)$ for points $P, Q \in E(\mathbb{F}_q)$;
2. Even if we could compute the image of the points P, Q, the Tate pairing $T_m(P, Q)$ could still be trivial ($T_m(P, Q) = 1$), so taking the discrete logarithm does not actually give any information;
3. There are infinitely many isogenies $E \to [\mathfrak{a}] \star E$: one for every ideal $\mathfrak{a}$ in the class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$. If this approach would work, we would be able to determine the value $\deg(\varphi) = \mathrm{N}(\mathfrak{a}) \bmod m$ for all ideals $\mathfrak{a} \in [\mathfrak{a}]$.

We discuss Problem 1 in Section 2.3 and there we also argue that we need to relax our expectations, with Problem 2 in Section 2.2 and

We will first deal with this question in the simplest case that $E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/A\mathbb{Z}$ with $\gcd(m, A) = 1$, that is, $m | \#E(\mathbb{F}_q)$ but $m^2 \nmid \#E(\mathbb{F}_q)$. Another way how to express this condition: if we define

$$E(\mathbb{F}_q)[m^\infty] = \cup_{i \geq 1} E(\mathbb{F}_q)[m^i]$$

as the subgroup of $E(\mathbb{F}_q)$ consisting precisely of points whose order is a power of m, then our condition means that $E(\mathbb{F}_q)[m^\infty] = \langle P \rangle$ is cyclic and generated by a point of order m.

Later, we will discuss what needs to change for more general settings.

2.2 Non-degeneracy of the Tate pairing

We can use the Tate pairing T_m to pair any point of order m with an arbitrary point in $E(\mathbb{F}_q)$. Moreover, unlike for the Weil pairing, the Tate self-pairing can be non-trivial! That is, it can happen that the self-pairings $T_m(P, P) \neq 1$. It will be our strategy for the rest of the write-up to find points P for which the self-pairing is non-trivial.

Let P be any point of order m. We know that $E(\mathbb{F}_q) \cong E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)[A]$ with $\gcd(m, A) = 1$. So multiplication by m is the zero map on the first summand and a bijection for the second summand, and therefore

$$E(\mathbb{F}_q)/mE(\mathbb{F}_q) \cong E(\mathbb{F}_q)[m] \cong \langle P \rangle.$$

But we know that the Tate pairing T_m is a non-degenerate pairing. Therefore, $T_m(P, P) \neq 1$.

Exercise 2.1. *Suppose that $E(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/m^n\mathbb{Z}$ is cyclic and generated by a point Q of order m^n. Let $P = m^{n-1}Q$ be a point of order m. By examining $E(\mathbb{F}_q)/mE(\mathbb{F}_q)$, show that $T_m(P, Q) \neq 1$.*

Exploration 2.2. *Suppose that $E(\mathbb{F}_q)[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Let $P \in E[m]$ be a point of order m. Can its self-pairing be non-trivial, that is, $T_m(P, P) \neq 1$? Can you find a point Q such that $T_m(P, Q) \neq 1$?*

2.3 Computing the image under an unknown isogeny

In the previous section, we have seen that if $E(\mathbb{F}_q)[m^\infty] = \langle P \rangle$ is cyclic, then the pairing $T_m(P, P)$ is non-trivial. How can we find the image of P under an unknown isogeny φ?

We need the following two ingredients. Let $\varphi : E \to E'$ be an isogeny defined over $\mathbb{F}_q$, then:

- Points of order m map to points of order m, that is,

  $$\varphi(E(\mathbb{F}_q)[m]) \subset E'(\mathbb{F}_q)[m].$$

  and there is equality if $\gcd(\deg(\varphi), m) = 1$;

- (Tate's theorem) isogenous curves over $\mathbb{F}_q$ have the same number of points[4].

The second point implies in our setting that $E'(\mathbb{F}_q)[m^\infty] = \langle P' \rangle$ for some $P' \in E'(\mathbb{F}_q)$ of order m because m is the highest power dividing $\#E(\mathbb{F}_q)$, which is equal to $\#E'(\mathbb{F}_q)$ by Tate's theorem.

Suppose now[5] that $\deg \varphi$ is coprime to m. Then there exists some $k \in (\mathbb{Z}/m\mathbb{Z})^*$ such that

$$\varphi(P) = kP'.$$

Bear in mind that k is unknown, but P, P' we can choose arbitrarily. If we return to the Tate pairings:

$$T_m(P,P)^{\deg(\varphi)} = T_m(\varphi(P), \varphi(P)) = T_m(kP', kP') = T_m(P', P')^{k^2}$$

(the first equality is the isogeny property of the Tate pairing, the second substitution, the last equality is the bilinearity). If we compare the discrete logarithms, we see that by computing

$$\log_{T_m(P,P)}(T_m(P', P')) \equiv \deg(\varphi) \cdot k^{-2} \bmod m,$$

so we can at least determine $\deg(\varphi) \bmod m$ up to squares mod m.

To simplify the notation, if $E' = [\mathfrak{a}] \star E$ and the isogeny $\varphi := \varphi_{\mathfrak{a}}$ corresponds to ideal $\mathfrak{a}$, then we define

$$\chi_m(E, E') = \begin{cases} 1, & \text{if } \log_{T_m(P,P)}(T_m(P', P')) \text{ is a square mod } m \text{ or } T_m(P,P) = 1; \\ -1 & \text{else.} \end{cases} \tag{1}$$

Note that we do not refer to the ideal $\mathfrak{a}$ in the notation $\chi_m(E, E')$. Indeed, because none of the choices in the computation of $\chi_m(E, E')$ depend on the (unknown) isogeny φ, this value needs to be the same for all ideals $\mathfrak{a}$ in the ideal class $[\mathfrak{a}]$.

Exercise 2.3. *Use Exercise 2.1 to extend the results of this section: show that if $E(\mathbb{F}_q)[m^\infty] = \langle Q \rangle$ and $E'(\mathbb{F}_q)[m^\infty] = \langle Q' \rangle$ for points Q and Q' of order m^n, then the one can use the pairings $T_m(m^{n-1}Q, Q)$ and $T_m(m^{n-1}Q', Q')$ to compute $\chi_m(E, E')$.*

2.4 Summary

We have seen that the Tate pairing T_m is compatible with isogenies, and that there may exists points $P \in E(\mathbb{F}_q)[m]$ such that $T_m(P,P) \neq 1$. Moreover, if $\varphi : E \to E'$ is an isogeny and we can find or guess the image $\varphi(P)$, then we can recover $\deg(\varphi) \bmod m$ from

$$T_m(\varphi(P), \varphi(P)) = T_m(P,P)^{\deg(\varphi)}.$$

If we only know $\varphi(P) = kP'$ for some unknown k, then we can recover $\deg(\varphi) \bmod m$ up to squares $\bmod m$.

3 Class group and characters

Until now, we have assumed that the group action given by the class group $\mathrm{Cl}(\mathcal{O})$ is essentially a black-box group action that can be instantiated efficiently using isogenies. Our discussion in Section 2 implied that if we can find an m-torsion point for which the Tate pairing $T_m(P,P)$ is non-trivial, we can use this to obtain information about $\deg \varphi_{\mathfrak{a}}$ (in particular, the value up to squares) for any ideal $\mathfrak{a}$ in the ideal class $[\mathfrak{a}]$. This is too good to be true to expect in full generality. In this section we take a closer look at the class group $\mathrm{cl}(\mathcal{O})$ to find out more.

[4] The full Tate's theorem says that curves over $\mathbb{F}_q$ are isogenous if and only if the have the same number of points

[5] And we will, again, see later why we can assume this for isogenies coming from the group action.

3.1 Quadratic characters

Let m be an integer. Note that being a square mod$m$ is a multiplicative property. Similarly, composing isogenies multiplies the degree. So, the construction from Section 2 gives us a quadratic character on the class group:

$$\chi_m(E, \mathfrak{a} \star E) \cdot \chi_m(E, \mathfrak{b} \star E) = \chi_m(E, \mathfrak{ab} \star E),$$

and $\chi_m(E, E')^2 = 1$ for all E, E'. Moreover, it's easily seen that because of this multiplicativity and because the group action of $\mathrm{cl}(\mathcal{O})$ on $\mathscr{E}\ell\ell$ is transitive, we can define the map on the class group:

$$\begin{aligned}
\chi_m : \mathrm{cl}(\mathcal{O}) &\to \{\pm 1\}; \\
\chi_m([\mathfrak{a}]) &= \chi(E, [\mathfrak{a}] \star E) \quad \text{for any } E \in \mathscr{E}\ell\ell \\
&= \left(\frac{\deg(\varphi_{\mathfrak{a}})}{m}\right) \quad \text{for the isogeny } \varphi_{\mathfrak{a}} : E \to [\mathfrak{a}] \star E \\
&= \left(\frac{\mathrm{N}\mathfrak{a}}{m}\right) \quad \text{for any } \mathfrak{a} \in [\mathfrak{a}] \text{ with } \gcd(\mathrm{N}\mathfrak{a}, m) = 1,
\end{aligned}$$

where $\left(\frac{\cdot}{m}\right)$ is the Legendre symbol of m. The last equality follows from the fact that the degree of an isogeny corresponding to an ideal $\mathfrak{a}$ is $\mathrm{N}\mathfrak{a}$.

Exercise 3.1. *Suppose that there exists m an odd prime such that the character $\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$ is non-trivial and can be computed in polynomial time, as in Section 2. Break the DDH assumption for the class group action of $\mathrm{Cl}(\mathcal{O})$ on $\mathscr{E}\ell\ell_q(\mathcal{O}, t)$.*

For the computational complexity, please see Section 5 of [**?**].

3.2 Genus theory

So, the Tate pairing T_m can be used to produce a quadratic character on $\mathrm{Cl}(\mathcal{O})$, which we would like to be non-trivial. Fortunately, all the non-trivial quadratic characters on the class group we already known to Gauss.

Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field. Write $\Delta = -2^a \cdot b$ with $b = \prod_{i=1}^{r} m_i^{e_i}$ for distinct odd primes m_i.

Theorem 3.2 (Genus theory, see I.3 and II.7 of [6])**.** *All quadratic characters of $\mathrm{Cl}(\mathcal{O})$ are given by (products of):*

- *for every odd prime m_i:*
$$\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} \qquad [\mathfrak{a}] \mapsto \left(\frac{\mathrm{N}(\mathfrak{a})}{m}\right)$$
where $\mathfrak{a}$ is any representative of $[\mathfrak{a}]$ satisfying $\gcd(m, \mathrm{N}(\mathfrak{a})) = 1$.
- *Define*
$$\delta : \mathfrak{a} \mapsto (-1)^{(\mathrm{N}(\mathfrak{a})-1)/2} \qquad \varepsilon : \mathfrak{a} \mapsto (-1)^{(\mathrm{N}(\mathfrak{a})^2-1)/8}$$
if $\Delta = -4n$, extend the set of characters by
  1. *δ if $n \equiv 1, 4, 5 \pmod 8$,*
  2. *ε if $n \equiv 6 \pmod 8$,*
  3. *$\delta\varepsilon$ if $n \equiv 2 \pmod 8$.*

There is one relation between these characters:

$$\chi_{m_1}^{e_1} \cdot \cdots \cdot \chi_r^{e_r} \cdot \delta^{\frac{b+1}{2} \bmod 2} \cdot \varepsilon^{a \bmod 2} \equiv 1 \quad \text{on } \mathrm{Cl}(\mathcal{O}).$$

Because of the beauty of number theory, the relation between the characters is secretly the following statement about ideals, which might be a lot easier to believe: for simplicity, if $\mathcal{O} = \mathbb{Z}[\sqrt{-\Delta}]$ with Δ square-free, then the ideals $\mathfrak{p}_m$ above the primes $m \mid \Delta$ are ramified and of order 2 in the class group, and their product (again with an appropriate adjustment at the prime 2) is the principal ideal $(\sqrt{\Delta})$.

Exercise 3.3. *Find all the quadratic characters and relations between them for the class groups of the following imaginary quadratic orders:*

1. $\mathbb{Z}[\sqrt{-105}]$;
2. $\mathbb{Z}[\sqrt{-p}]$ *for* $p \equiv 1 \bmod 4$;
3. $\mathbb{Z}[\sqrt{-p}]$ *for* $p \equiv 3 \bmod 4$;
4. $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ *for* $p \equiv 3 \bmod 4$.

Exercise 3.4. *Describe all discriminants* Δ *for which there exist non-trivial characters on* $\mathrm{Cl}(\mathcal{O})$.

Once you solve the exercises above, you will see that there are no non-trivial characters for the class groups used in CSIDH or CSURF [2]. If we instantiate the CRS/CSIDH class group action with supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 1 \bmod 4$, then the character δ is always non-trivial.

Exploration 3.5. *Quadratic characters are maps from* $\mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$*, and so have to factor through the quotient map*

$$\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O})/\mathrm{Cl}(\mathcal{O})^2 \to \{\pm\}.$$

So, if there are non-trivial characters, it means that the class number is even. But we cannot fully determine the structure of $\mathrm{Cl}(\mathcal{O})[2^\infty]$ *just from quadratic characters. Use Sage or LMFDB to find examples with interesting* $\mathrm{Cl}(\mathcal{O})[2^\infty]$.

However, for a given $\mathcal{O}$*, already Gauss knew how to compute square-roots in class groups. You can use the algorithms of [1] to try to compute square roots of ideals of order* 2 *in the class group.*

4 Noncyclic torsion

Let $E/\mathbb{F}_q$ be an elliptic curve and let m be an odd prime. In Section 2, we assumed that $E(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/m\mathbb{Z}$ (or at least that the m^∞-torsion is cyclic in Exercise 2.1). In this section, we discuss how to remove this condition, leading to the beautiful theory of isogeny volcanoes.

4.1 All ℓ-isogenies

Tate's theorem says that two curves $E, E'/\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if they have the same number of points. Say $\#E(\mathbb{F}_q) = q + 1 - t$. Then $\mathrm{End}(E) = \mathcal{O} \supset \mathbb{Z}[\pi]$ for π a root of the polynomial $x^2 - tx + q$ (corresponding to the Frobenius endomorphism). Note that $\mathbb{Z}[\pi]$ has discriminant $\Delta_\pi = t^2 - 4q$. Similarly, $\mathrm{End}(E') = \mathcal{O}' \supset \mathbb{Z}[\pi]$. In this section we study the relationship between the orders $\mathcal{O}$ and $\mathcal{O}'$ if the elliptic curves are isogenous by an isogeny of degree a power of ℓ.

The isogenies between elliptic curves in the CRS or CSIDH-like schemes always preserve the endomorphism ring: they induce group actions of $\mathrm{Cl}(\mathcal{O})$ on $\mathscr{E}\ell\ell_q(\mathcal{O}, t)$, the set of elliptic curves $E/\mathbb{F}_q$ with fixed endomorhism ring $\mathcal{O}$ and trace t, up to isomorphism. Take ℓ a split prime in $\mathcal{O}$, that is, $\ell\mathcal{O} = \mathfrak{l}\bar{\mathfrak{l}}$ as ideals. Then the two ideals $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ give two ℓ-isogenies for any elliptic curve $E \in \mathscr{E}\ell\ell_q(\mathcal{O}, t)$. Those isogenies do not change the endomorphism ring.

However, any isogeny is given by its kernel and the kernel of an ℓ-isogeny is a subgroup of size ℓ. By looking at the subgroups of size ℓ in

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z},$$

we see that there are up to $\ell + 1$ isogenies of degree ℓ defined over $\mathbb{F}_q$. But only at most two can preserve the endomorphism ring. The following theorem gives us the rest of the possibilities.

Theorem 4.1 ([7]). *If E and E' are ℓ-isogenous by $\varphi : E \to E'$, then*

1. *either $\mathcal{O} = \mathcal{O}'$, in which case φ is called horizontal;*
2. *or $[\mathcal{O} : \mathcal{O}'] = \ell$, in which case φ is called descending;*
3. *or $[\mathcal{O}' : \mathcal{O}] = \ell$, in which case φ is called ascending.*

Group action-based isogeny schemes only use horizontal isogenies, with the exception of CSURF (see Wouter's Week 3 and the discussion of 2-isogenies).

4.2 Isogeny volcanoes

Define the *component of E* (in the ℓ-isogeny graph) as the graph $G = (V, E)$ with

- vertices V given by $\mathbb{F}_q$-isomorphism classes of curves which are ℓ^k-isogenous to E over $\mathbb{F}_q$,
- edges given by ℓ-isogenies, up to $\mathbb{F}_q$ equivalence and dual isogenies (as before).

This component of E captures all the curves over $\mathbb{F}_q$ that can be reached from E by taking ℓ-isogenies.

Theorem 4.2 (Kohel's theorem). *For any $E/\mathbb{F}_q$, the component of E is an **isogeny volcano**: There is a partition of the vertices into disjoint sets $V = V_0 \cup V_1 \cup \dots V_h$ such that*

- *the subgraph on V_h is a cycle*
- *the subgraph of V_i for $i \neq h$ has no edges,*
- *isogenies from surface to floor are descending,*
- *isogenies from floor to surface are ascending,*
- *if $i < h$, every $E_i \in V_i$ has exactly one neighbour $E_{i+1} \in V_{i+1}$,*
- *every $E_i \in V_i$ for $i \neq 0$ has $\ell + 1$ neighbours.*

The integer h is called the *height*, the set V_h is called the *surface*, the set V_0 is called the *floor*. Note that some authors flip the labelling so that V_0 is the surface and talk about the depth of the volcano instead.

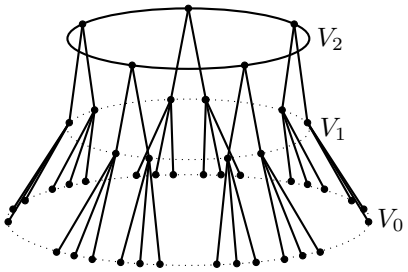

Figure 4.1: *Example of a volcano of height 2.*

All curves in V_i have the same endomorphism ring $\mathcal{O}_i$ and the curves on the floor satisfy

$$(\mathcal{O}_0)_\ell = \mathbb{Z}[\pi]_\ell,$$

that is, localizing at ℓ, the endomorphism ring $\mathcal{O}_0$ is as small as possible (the endomorphism ring always contains $\mathbb{Z}[\pi]$).

Assume that ℓ is odd and the elliptic curves on the floor V_0 have $\mathrm{End}(E) = \mathbb{Z}[\pi]$ with discriminant $t^2 - 4q$. Suppose that $\mathrm{val}_\ell(t^2 - 4q) = 2h$. Since the isogenies going towards the surface are ascending, we obtain a sequence of orders of successive index ℓ:

$$\mathcal{O}_0 = \mathbb{Z}[\pi] \subset \mathcal{O}_1 \cdots \subset \mathcal{O}_h.$$

Therefore, to have a volcano of large height, we need a large power of ℓ to divide $t^2 - 4q$.

Exercise 4.3. *What are the possible heights of volcanoes of ℓ-isogenies for supersingular elliptic curves over $\mathbb{F}_p$? How large can the surface be? Note that the answer depends on $p \bmod 8$.*

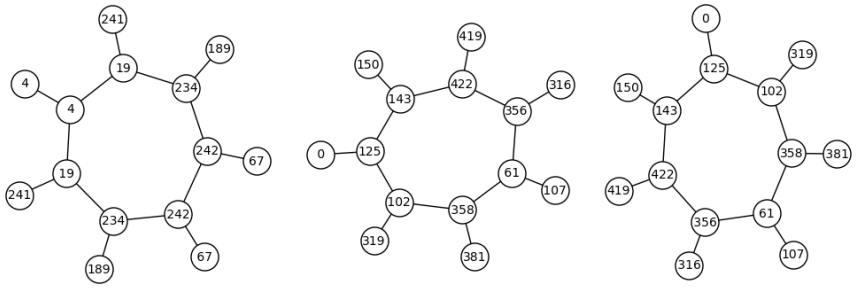

Figure 4.2: *2-isogeny volcanoes over $\mathbb{F}_{431}$, the elliptic curves are labelled with the j-invariants and so there are always two curves with the same label.*

4.3 From volcanoes to torsion

In this section, we keep the previous notation of m an odd prime. We tie in together the behaviour of m^∞-torsion with the levels of the isogeny volcanoes.

Theorem 4.4 ([8])**.** *Let $\mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O}$ be an order in an imaginary quadratic field and let π be the Frobenius endomorphism. Then*

$$E(\mathbb{F}_q) \cong \frac{\mathcal{O}}{\pi - 1}$$

as $\mathrm{End}_{\mathbb{F}_q}(E)$-modules, so in particular as abelian groups.

Exercise 4.5. *Compute all the possible group structures for a supersingular elliptic curve over $\mathbb{F}_p$.*

Exercise 4.6. *Show that if two elliptic curves have isomorphic endomorphism rings, then they lie on the same level of their volcanoes.*

Corollary 4.7 ([9])**.** *Let m be an odd prime, $E/\mathbb{F}_q$ an elliptic curve with endomorphism ring $\mathcal{O}$. Let $v = \mathrm{val}_m(q + 1 - t)$ and let h be the heigth of the isogeny volcano of E. Then*

- *$E(\mathbb{F}_q)[m^\infty] = \mathbb{Z}/m^v$ if and only if $\mathcal{O}_m = \mathbb{Z}[\pi]_m$ if and only if E is on the floor;*
- *$E(\mathbb{F}_q)[m^\infty] = \mathbb{Z}/m^{v-1} \times \mathbb{Z}/m$ if and only if E is on level 1;*
- *with each ascending isogeny, the m^∞-torsion becomes more balanced.*

Suppose we have two elliptic curves $E, E' \in \mathscr{Ell}_q(\mathcal{O}, t)$, with $E' = [\mathfrak{a}] \star E$ for some $\mathfrak{a} \subset \mathcal{O}$ an ideal. Then they have isomorphic endomorphism rings, and hence, by Exercise 4.6, are on the same level. By walking to the floor from both elliptic curves (which can be done efficiently), we find two elliptic curves E_0, E_0' with the same endomorphism ring $\mathcal{O}_0$ and hence connected by an ideal $\mathfrak{b} \subset \mathcal{O}_0$, that is, $E_0' = [\mathfrak{b}] \star E_0$. But curves on the floor have cyclic m^∞ torsion, so we can apply the methods from Section 2! That is, compute $\chi_m([\mathfrak{b}])$ directly from the elliptic curves E_0, E_0'. One can show that $[\mathfrak{b}\mathcal{O}] = [\mathfrak{a}]$ and hence can also obtain the value of $\chi_m([\mathfrak{a}])$.

References

[1] Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2-class groups. *Journal de Théorie des Nombres de Bordeaux*, 8(2):283–313, 1996.

[2] Wouter Castryck and Thomas Decru. CSIDH on the surface. In *PQCrypto*, volume 12100 of *Lecture Notes in Computer Science*, pages 111–129. Springer, 2020. https://ia.cr/2019/1404.

[3] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *ASIACRYPT (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018. https://ia.cr/2018/383.

[4] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. Springer-Verlag, 2020.

[5] Jean-Marc Couveignes. Hard homogeneous spaces, 1997. IACR Cryptology ePrint Archive 2006/291, https://ia.cr/2006/291.

[6] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Pure and Applied Mathematics. Wiley, second edition, 2013.

[7] David R. Kohel. Endomorphism rings of elliptic curves over finite fields. 1996. PhD thesis.

[8] Hendrik W. Lenstra. Complex multiplication structure of elliptic curves. *J. Number Theory*, 56:227–241, 1996.

[9] Josep Miret, Daniel Sadornil, Juan Tena-Ayuso, Rosana Tomàs, and Magda Valls. Volcanoes of ℓ-isogenies of elliptic curves over finite fields: The case $\ell = 3$. *Publicacions Matemàtiques*, 51:165–180, 2007.

[10] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.