CSIDH ON THE SURFACE (CSURF)

ISOGENY-BASED CRYPTOGRAPHY SCHOOL, WEEK 3: 19-23 JULY 2021
(LECTURE NOTES BY WOUTER CASTRYCK)

These notes discuss the paper [2], which is joint work with Thomas Decru.

1. Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$

Throughout this text, we work with supersingular elliptic curves E over a prime field $\mathbb{F}_p$ of characteristic $p > 3$. Such curves satisfy $\#E(\mathbb{F}_p) = p+1$, which in turn implies that the Frobenius endomorphism $\pi : E \to E$ satisfies $\pi^2 = \pi \circ \pi = [-p]$.

Exercise 1. *Prove this last claim.*

Let us write $\mathrm{End}_p(E)$ for the ring of endomorphisms of E that are defined over $\mathbb{F}_p$. The previous observation implies that $\mathbb{Z}[\sqrt{-p}]$ can be viewed as a subring of $\mathrm{End}_p(E)$, through the injection

$$\iota_E : \mathbb{Z}[\sqrt{-p}] \to \mathrm{End}_p(E) : m + n\sqrt{-p} \mapsto [m] + [n] \circ \pi.$$

From [19, §2 and §4] we know that $\mathrm{End}_p(E)$ is an order in an imaginary quadratic field; necessarily, that field is isomorphic to $\mathbb{Q}(\sqrt{-p})$.

We are not left with many options for $\mathrm{End}_p(E)$. Indeed, if $p \equiv 1 \bmod 4$ then we know that $\mathbb{Z}[\sqrt{-p}]$ is the *maximal* order (= ring of integers) of $\mathbb{Q}(\sqrt{-p})$, therefore ι_E must be an isomorphism. On the other hand, if $p \equiv 3 \bmod 4$ then the maximal order is $\mathbb{Z}[(1+\sqrt{-p})/2]$, which is larger than $\mathbb{Z}[\sqrt{-p}]$ but only slightly: the index is 2 so there is no room for another ring in between. We conclude that either $\mathrm{End}_p(E) \cong \mathbb{Z}[\sqrt{-p}]$ or $\mathrm{End}_p(E) \cong \mathbb{Z}[(1+\sqrt{-p})/2]$. In the latter case, there exists a unique endomorphism $\phi \in \mathrm{End}_p(E)$ such that $[2] \circ \phi = [1] + \pi$, and we can extend ι_E to an isomorphism

$$\mathbb{Z}[(1+\sqrt{-p})/2] \to \mathrm{End}_p(E) : m + n(1+\sqrt{-p})/2 \mapsto [m] + [n] \circ \phi,$$

that we still denote by ι_E, by a mild abuse of notation.

The following terminology is key to our discussion and will be motivated in Sections 3 and 4.

Definition 1. Over a finite prime field $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$ and $p > 3$, a supersingular elliptic curve with endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ is said to live on **the floor**, while a supersingular elliptic curve with endomorphism ring $\mathbb{Z}[(1+\sqrt{-p})/2]$ is said to live on **the surface** (also known as **the crater**).

imec-COSIC, Kasteelpark Arenberg 10/2452, 3001 Leuven, wouter.castryck@kuleuven.be

This work is supported by CyberSecurity Research Flanders with reference number VR20192203, and by the Research Council KU Leuven grant C14/18/067 on Cryptanalysis of post-quantum cryptography. I would like to thank Daniel J. Bernstein, Thomas Decru, Luca De Feo, Lorenz Panny and Frederik Vercauteren for some complementary remarks that I incorporated in these notes and that post-date the publication of [2].

Both the floor and the surface are non-empty, i.e., both endomorphism rings occur: you will check this in Exercise 2 below. One can also use Theorem 2 to see this.

The following criterion, which is taken from [10, §2], makes it very easy to decide at which level we are: it suffices to look at the $\mathbb{F}_p$-rational 2-torsion points.

Lemma 1. *Consider a supersingular elliptic curve E over a prime field $\mathbb{F}_p$ with $p > 3$. Then either $\#E[2](\mathbb{F}_p) = 2$ or $\#E[2](\mathbb{F}_p) = 4$, and we are in the latter case if and only if $\mathrm{End}_p(E) \cong \mathbb{Z}[(1+\sqrt{-p})/2]$.*

Proof. There exists at least one $\mathbb{F}_p$-rational point of order two because $\#E(\mathbb{F}_p) = p+1$ is even, and we of course have $\#E[2](\mathbb{F}_p) \leq \#E[2] = 4$, from which the first claim follows. As for the second claim:
$\boxed{\Leftarrow}$ Any $P \in E[2]$ satisfies $P + \pi(P) = 2\phi(P) = \phi(2P) = 0$ and therefore $\pi(P) = -P = P$. Hence $E[2] \subset E(\mathbb{F}_p)$, as wanted.
$\boxed{\Rightarrow}$ Conversely, if $E[2] \subset E(\mathbb{F}_p)$ then any $P \in E[2]$ satisfies $P + \pi(P) = 2P = 0$, hence $\ker[2] \subset \ker(1+\pi)$. The existence of an endomorphism $\phi \in \mathrm{End}_p(E)$ such that $2 \circ [\phi] = 1 + \pi$ now follows from [16, Cor. III.4.11]. □

Exercise 2. *Consider the elliptic curves $E_\pm : y^2 = x^3 \pm x$ over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$ and $p > 3$. Prove that both curves are supersingular. Use Lemma 1 to prove that $\mathrm{End}_p(E_+) \cong \mathbb{Z}[\sqrt{-p}]$ and $\mathrm{End}_p(E_-) \cong \mathbb{Z}[(1+\sqrt{-p})/2]$. In the latter case, can you give an explicit description of the endomorphism ϕ?*

The reason for excluding $p = 3$ throughout these notes is to avoid pathologies of the following kind (as a bonus exercise, you can show that the assumption $p > 3$ can in fact be dropped from the previous exercise):

Exercise 3. *Consider the elliptic curve $E : y^2 = x^3 + 2x + 1$ over $\mathbb{F}_3$. Show that it is supersingular, that $\mathrm{End}_p(E) \cong \mathbb{Z}[(1+\sqrt{-3})/2]$ and that $E[2](\mathbb{F}_p) = \emptyset$.*

2. A quick recap of CSIDH

Let us call to mind the "CM torsor", at the level of generality needed for this lecture:

Theorem 2 (CM torsor)**.** *Consider a prime $p > 3$, and let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ if $p \equiv 1 \bmod 4$ and either $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ or $\mathcal{O} = \mathbb{Z}[(1+\sqrt{-p})/2]$ if $p \equiv 3 \bmod 4$. Write $\mathcal{E\ell\ell}_p(\mathcal{O})$ to denote the set of all $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$. Then the map*

$$\mathrm{cl}(\mathcal{O}) \times \mathcal{E\ell\ell}_p(\mathcal{O}) \to \mathcal{E\ell\ell}_p(\mathcal{O}) : ([\mathfrak{a}], E) \mapsto [\mathfrak{a}]E := E/E[\mathfrak{a}],$$

where

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \iota_E(\alpha),$$

is a well-defined free and transitive group action.

Proof. This is a special case of [19, Thm. 4.5].[1] □

[1] The proof of [19, Thm. 4.5] contains a small error that was pointed out in [14, Proof of Thm. 4.5], but this does not affect our statement.

We also recall that if the norm of $\mathfrak{a}$ is not a multiple of p, then this norm equals the cardinality of $E[\mathfrak{a}]$. In turn, this equals the degree of the corresponding isogeny $E \to E/E[\mathfrak{a}]$.

It is believed that computing $[\mathfrak{a}\mathfrak{b}]E$ from a given triple $E, [\mathfrak{a}]E, [\mathfrak{b}]E$ for secret random $[\mathfrak{a}], [\mathfrak{b}] \in \mathrm{cl}(\mathcal{O})$ is very hard on average, even for quantum computers. Following [8], this problem is called the *parallelization problem.* It immediately gives rise to the Diffie–Hellman style key exchange protocol depicted in Figure 1. In practice, Alice and Bob deviate from this protocol, in that they do *not* sample their ideal classes $[\mathfrak{a}]$ and $[\mathfrak{b}]$ uniformly at random, because both sampling a random ideal class and computing its action are currently infeasible. Instead, they generate them as

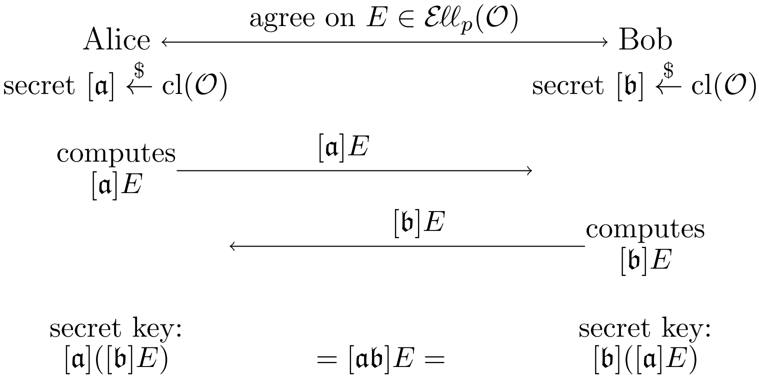
agree on $E \in \mathcal{E}\ell\ell_p(\mathcal{O})$
Alice
Bob
secret $[\mathfrak{a}] \xleftarrow{\$} \mathrm{cl}(\mathcal{O})$
secret $[\mathfrak{b}] \xleftarrow{\$} \mathrm{cl}(\mathcal{O})$
computes $[\mathfrak{a}]E$
$[\mathfrak{a}]E$
$[\mathfrak{b}]E$
computes $[\mathfrak{b}]E$
secret key: $[\mathfrak{a}]([\mathfrak{b}]E)$
$= [\mathfrak{a}\mathfrak{b}]E =$
secret key: $[\mathfrak{b}]([\mathfrak{a}]E)$

FIGURE 1. Diffie–Hellman key exchange using the CM torsor

$$[\mathfrak{l}_1]^{e_1}[\mathfrak{l}_2]^{e_2}\cdots[\mathfrak{l}_r]^{e_r}$$

for certain "easy ideals" $\mathfrak{l}_1, \dots, \mathfrak{l}_r$, where the secret exponent vector $(e_1, \dots, e_r)$ is sampled from a set of size about $\#\,\mathrm{cl}(\mathcal{O}) \approx \sqrt{p}$.[2] The protocol then relies on the heuristic assumption that this way of sampling from $\mathrm{cl}(\mathcal{O})$ is close enough to uniform [4, §7.1]. The more "easy ideals" we have at our disposal, the merrier:

Exercise 4. *Assume that all e_i are sampled uniformly randomly from a fixed, appropriately sized balanced interval, i.e., an interval of the form $[-B, B]$ for some appropriate B. Show that the expected number of actions with the "easy ideal" classes $[\mathfrak{l}_i]^{\pm 1}$ needed for Alice's public key generation is about $r\sqrt[2r]{p}/4$.*

We briefly recall how this works for CSIDH, while referring to [4] and to Tanja's lecture for more details. We work in the orbit of $y^2 = x^3 + x$ over $\mathbb{F}_p$, where

$$p = 4\ell_1\ell_2\cdots\ell_r - 1 \tag{1}$$

for distinct small odd primes $\ell_1, \dots, \ell_r$. Note that $p \equiv 3 \bmod 8$ and $p > 3$ (we assume $r \geq 1$). From Exercise 2 we see that we are working on the floor, i.e., with elliptic curves in $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$. The prime p is constructed such that $\ell_i\mathbb{Z}[\sqrt{-p}] = \mathfrak{l}_i\bar{\mathfrak{l}}_i$ for all $i = 1, \dots, r$, where $\mathfrak{l}_i = (\ell_i, \sqrt{-p} - 1)$ and where $\bar{\mathfrak{l}}_i = (\ell_i, \sqrt{-p} + 1)$ is

[2] We refer to Section 7 for more precise class number estimates

its complex conjugate. The ideal class $[\mathfrak{l}_i]$ has inverse $[\bar{\mathfrak{l}}_i]$ and is not of very small order.[3] It is "easy" to act with, because for each $E \in \mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ the group

$$E[\mathfrak{l}_i] = \{\, P \in E \mid [\ell_i]P = 0 \text{ and } \pi(P) = P \,\} = E[\ell_i](\mathbb{F}_p)$$

is small and defined over $\mathbb{F}_p$ (element-wise), indeed allowing for a fast computation of the isogenous curve $E/E[\mathfrak{l}_i]$. The basic strategy is:

(a) select a random point $Q \in E(\mathbb{F}_p)$,
(b) compute $P = [\frac{p+1}{\ell_i}]Q$ using double-and-add; return to step (a) if $P = 0$,
(c) quotient out the subgroup $E[\mathfrak{l}_i] = \langle P \rangle$ using Vélu's formulae.

The cost of step (b) can be amortized by precomputing a point of order $\ell_{i_1} \cdots \ell_{i_s}$ for some well-chosen set of indices $\{i_1, \ldots, i_s\}$ and pushing it through the corresponding isogenies: in this way one can reduce the number of large scalar multiplications. We refer to [4, Alg. 2] for more details.

We can use balanced exponents as in Exercise 4 because $[\bar{\mathfrak{l}}_i] = [\mathfrak{l}_i]^{-1}$ is equally easy to act with. This may seem a non-trivial claim, because here the kernel

$$\begin{aligned} E[\bar{\mathfrak{l}}_i] &= \{\, P \in E \mid [\ell_i]P = 0 \text{ and } \pi(P) = -P \,\} \\ &= \{\, 0 \,\} \cup \{\, (x, y) \in E[\ell_i] \mid x \in \mathbb{F}_p,\ y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \,\} \end{aligned}$$

contains points that are not defined over $\mathbb{F}_p$. Nevertheless, it remains possible to stick to $\mathbb{F}_p$-arithmetic by using formulae that involve x-coordinates only. Alternatively, one can resort to the rule

$$[\mathfrak{a}]^{-1}E = ([\mathfrak{a}]E^{\text{twist}})^{\text{twist}} \tag{2}$$

from [5, Lem. 5], where $\cdot^{\text{twist}}$ stands for quadratic twisting, which is a very cheap operation.

Example 1. The CSIDH-512 parameter set from [4] takes $r = 74$, with $\ell_1, \ldots, \ell_{73}$ the first 73 odd primes and with $\ell_{74} = 587$, so that $p \approx 2^{511}$. We work with balanced exponents, all sampled from $\{-5, \ldots, 5\}$. This gives rise to an exponent set of size $(2 \cdot 5 + 1)^{74} \approx 2^{256} \approx \sqrt{p}$.

Further optimizations come from the use of Montgomery curves $y^2 = x^3 + Ax^2 + x$, which admit fast Vélu-type formulae, fast formulae for scalar multiplication, and fast key validation; these features will be revisited in Section 6.

3. What about 2-isogenies?

Consider an elliptic curve $E \in \mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ for p a CSIDH prime as in (1). Then we know that

$$E[(2, \sqrt{-p} - 1)] = \{\, P \in E \mid [2]P = 0 \text{ and } \pi(P) = P \,\} = E[2](\mathbb{F}_p)$$

is a subgroup of order 2, thanks to Lemma 1. So it is the kernel of a 2-isogeny emanating from E. Why aren't such isogenies used during key generation? After all, as discussed in Exercise 4, the more "easy isogenies" we have at our disposal, the better, and computing 2-isogenies should be easier than computing isogenies of any other degree.

[3] You will prove a statement of this kind in Exercise 9.

The problem is that $(2, \sqrt{-p} - 1)$ does not represent an element of the class group:

Exercise 5. *Prove that, for* $p \equiv 3 \bmod 4$, *the ideal* $(2, \sqrt{-p} - 1)$ *is not invertible (as a fractional ideal) in* $\mathbb{Z}[\sqrt{-p}]$. *Hint: show that squaring the ideal amounts to multiplying it by* (2), *and conclude.*

It can be argued, see [10], that the subgroup $E[(2, \sqrt{-p} - 1)] = E[2](\mathbb{F}_p)$ takes us to the surface, i.e., the codomain of the corresponding isogeny is an elliptic curve whose endomorphism ring is the maximal order $\mathbb{Z}[(1 + \sqrt{-p})/2]$.

But then, why not working with elliptic curves E on the surface, by considering the orbit of $y^2 = x^3 - x$ instead of $y^2 = x^3 + x$ (see Exercise 2)? Recall that the CM torsor is available at both levels, and in maximal orders *every* non-zero ideal corresponds to an element of the class group, so this should avoid pathologies of the foregoing kind. Unfortunately, we again run into trouble, now for a different reason: while there are 3 outgoing 2-isogenies over $\mathbb{F}_p$ (one for each $\mathbb{F}_p$-rational point of order 2), none of them has a kernel of the form $E[\mathfrak{a}]$ for some ideal $\mathfrak{a} \subset \mathbb{Z}[(1 + \sqrt{-p})/2]$. It turns out that, perhaps not surprisingly, each of these 3 isogenies takes us to the floor. We again refer to [10] for a proof of these claims.

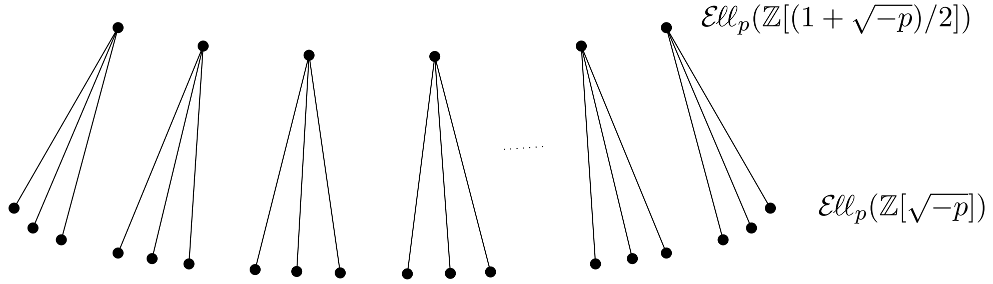
$\mathcal{E}\ell\ell_p(\mathbb{Z}[(1 + \sqrt{-p})/2])$
$\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$

FIGURE 2. Some components of the 2-isogeny graph of supersingular elliptic curves over $\mathbb{F}_p$ if $p \equiv 3 \bmod 8$ and $p > 3$ (as in CSIDH).

The crucial ingredient is that CSIDH primes satisfy $p \equiv 3 \bmod 8$. A summarizing picture can be found in Figure 2.

Here is a short exercise showing the failure of two naive candidates for $\mathfrak{a}$.

Exercise 6. *Show that* $(2, \sqrt{-p} - 1) = (2)$ *as ideals of* $\mathbb{Z}[(1 + \sqrt{-p})/2]$, *and explain why this is just a reinterpretation of* $\boxed{\Leftarrow}$ *in the proof of Lemma 1. Using that* $p \equiv 3 \bmod 8$, *show that the ideal* $(2, (\sqrt{-p} - 1)/2)$ *is the trivial ideal* (1).

Returning to $\mathbb{Z}[\sqrt{-p}]$, we remark that while we don't have horizontal (= endomorphism ring preserving) isogenies of degree 2, we *do* have horizontal isogenies of degree 4:

Exercise 7. *Let* $p \equiv 3 \bmod 8$. *Show that the ideal* $\mathfrak{l}_0 = (4, \sqrt{-p} - 1)$ *is invertible in* $\mathbb{Z}[\sqrt{-p}]$ *and that its class* $[\mathfrak{l}_0]$ *has order* 3. *Show that for* p *a CSIDH prime as in* (1), *the inverse of* $[\mathfrak{l}_0]$ *equals* $[\mathfrak{l}_1] \cdots [\mathfrak{l}_r]$. *Finally, prove that acting with* $[\mathfrak{l}_0]$ *on* $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ *amounts to cyclically permuting the 3 elliptic curves below a fixed curve on the surface.*

Onuki and Takagi [12, §4.2] showed that acting with $[\mathfrak{l}_0]$ is remarkably easy: it amounts to replacing the Montgomery coefficient A by $2(A-6)/(A+2)$. Thus, despite its low order, one can expect a small efficiency gain from including $[\mathfrak{l}_0]$ in the pool of "easy ideals" and letting the corresponding exponent e_0 range in $\{-1,0,1\}$.

Unfortunately, there is another, more compelling end to this story, which kills this optimism:

Exercise 8. *Let $p \equiv 3 \bmod 8$. As we have discussed, the map*

$$m_{\mathcal{E}\ell\ell} : \mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}]) \to \mathcal{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2]) : E \to E/E[2](\mathbb{F}_p)$$

from the floor to the surface is 3-to-1. Prove that the group homomorphism

$$m_{\mathrm{cl}} : \mathrm{cl}(\mathbb{Z}[\sqrt{-p}]) \to \mathrm{cl}(\mathbb{Z}[(1+\sqrt{-p})/2]) : [\mathfrak{a}] \mapsto [\mathfrak{a}\mathbb{Z}[(1+\sqrt{-p})/2]],$$

is also 3-to-1 and that its kernel is generated by the ideal class $[\mathfrak{l}_0]$ from the previous exercise. Finally, show that both maps are compatible with the CM torsor, in that

$$m_{\mathcal{E}\ell\ell}([\mathfrak{a}]E) = m_{\mathrm{cl}}([\mathfrak{a}])m_{\mathcal{E}\ell\ell}(E)$$

for all $E \in \mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ and all $[\mathfrak{a}] \in \mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$.

This reduces the hardness of the parallelization problem in $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ to that in $\mathcal{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2])$, where the acting class group is 3 times smaller. Thus, our small efficiency gain is negatively compensated by a small security loss.

4. Changing the prime p

Wrapping up, if $p \equiv 3 \bmod 8$ then neither $\mathbb{Z}[\sqrt{-p}]$ nor $\mathbb{Z}[(1+\sqrt{-p})/2]$ admits invertible ideals of norm 2. Can we fix this by switching to other p's?

If $p \equiv 7 \bmod 8$ then the floor is equally problematic: the ring $\mathbb{Z}[\sqrt{-p}]$ again has no invertible ideals of norm 2. But on the surface, things look more promising: we have $2\mathbb{Z}[(1+\sqrt{-p})/2] = \mathfrak{l}_0\bar{\mathfrak{l}}_0$ with $\mathfrak{l}_0 = (2, (\sqrt{-p}-1)/2)$ and $\bar{\mathfrak{l}}_0 = (2, (\sqrt{-p}+1)/2)$. The ideal class $[\mathfrak{l}_0]$ has inverse $[\bar{\mathfrak{l}}_0]$ and is not of very small order:

Exercise 9. *Show that the order of $[\mathfrak{l}_0]$ in $\mathrm{cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$ is at least $\lceil \log_2 p \rceil$.*[4]

Thus, we have a good candidate for inclusion in our pool of "easy isogenies". However, it has a slightly different shape than we are used to; we will get back to this in a minute.

It remains true that every curve E on the surface admits 3 outgoing 2-isogenies over $\mathbb{F}_p$, one for each $\mathbb{F}_p$-rational point of order 2. But now, two of their kernels are of the desired form, namely $E[\mathfrak{l}_0]$ and $E[\bar{\mathfrak{l}}_0]$. The third kernel is not of the form $E[\mathfrak{a}]$ for some ideal $\mathfrak{a} \subset \mathbb{Z}[(1+\sqrt{-p})/2]$, and the corresponding isogeny takes us to the floor. Once again, we refer to [10] for a proof. A summarizing picture can be found in Figure 3, where one sees a genuine *volcano graph* [18] showing up: this is where the floor versus surface terminology comes from.

A CSURF prime is then a prime of the form

$$p = 4f\ell_0\ell_1\ell_2\cdots\ell_r - 1 \tag{3}$$

[4] Most likely, the order is way larger than this lower bound.

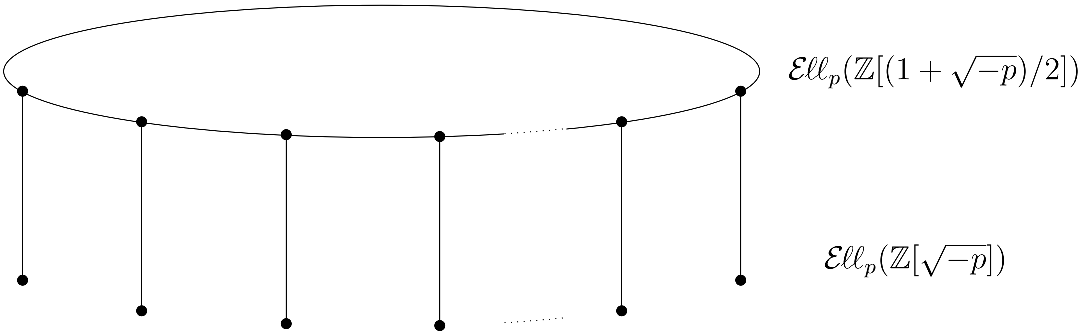
$\mathcal{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2])$
$\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$

FIGURE 3. A component of the 2-isogeny graph of supersingular elliptic curves over $\mathbb{F}_p$ when $p \equiv 7 \bmod 8$ (as in CSURF). The length of the cycle equals the order of $[(2, (\sqrt{-p} - 1)/2)]$.

where $\ell_0 = 2$, where $\ell_1, \ldots, \ell_r$ are distinct small odd primes, and where f is a small cofactor (it can be useful to tolerate this). As said, we work on the surface, i.e., in the orbit of $y^2 = x^3 - x$ over $\mathbb{F}_p$. We again have

$$\ell_i \mathbb{Z}[(1+\sqrt{-p})/2] = \underbrace{(\ell_i, \sqrt{-p} - 1)}_{\mathfrak{l}_i} \underbrace{(\ell_i, \sqrt{-p} + 1)}_{\bar{\mathfrak{l}}_i}$$

for all $i = 1, \ldots, r$, and acting with $[\mathfrak{l}_i]$ or $[\bar{\mathfrak{l}}_i]$ is done as in CSIDH. Thus we can concentrate on how to act with $[\mathfrak{l}_0]$ and $[\bar{\mathfrak{l}}_0]$, which seems to require a different treatment. Indeed,

$$E[\mathfrak{l}_0] = \{\, P \in E \mid [2]P = 0 \text{ and } \phi(P) = P \,\}$$

is not of the form $E[2](\mathbb{F}_p)$, so at first sight, it seems that our basic strategy (a-c) from Section 2 fails: how can we make sure that the order-2 point P from step (b) is a generator of $E[\mathfrak{l}_0]$?

Exercise 10. *Let $p \equiv 3 \bmod 4$ and consider an elliptic curve $E : y^2 = x^3 + ax^2 + bx$ over $\mathbb{F}_p$, where $a, b \in \mathbb{F}_p$ satisfy $b(a^2 - 4b) \neq 0$. Prove that b is a square in $\mathbb{F}_p$ if and only if the four halves of $(0,0)$ have x-coordinates in $\mathbb{F}_p$. Hint: find two expressions for the slope of the tangent line at such a half, and equate.*

Lemma 3. *Assume $p \equiv 7 \bmod 8$ and consider an elliptic curve $E \in \mathcal{E}\ell\ell_p(\mathbb{Z}[(1 + \sqrt{-p})/2])$. Its 3 points of order 2 can be classified as follows:*

- *a point $P_{\rightarrow}$ whose four halves belong to $E(\mathbb{F}_p)$,*
- *a point $P_{\leftarrow}$ whose four halves have x-coordinates in $\mathbb{F}_p$ and y-coordinates outside $\mathbb{F}_p$,*
- *a point $P_{\downarrow}$ whose four halves have x-coordinates outside $\mathbb{F}_p$.*

Furthermore, we have $E[\mathfrak{l}_0] = \langle P_{\rightarrow} \rangle$ and $E[\bar{\mathfrak{l}}_0] = \langle P_{\leftarrow} \rangle$, while quotienting out $\langle P_{\downarrow} \rangle$ takes us to the floor $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$.

Proof. If $E[4](\mathbb{F}_p) = E[4]$ then the curve on the floor which is 2-isogenous to E would have all its 2-torsion defined over $\mathbb{F}_p$ (explain), in contradiction with Lemma 1. Therefore we know that $E[4](\mathbb{F}_p) \subsetneq E[4]$. Together with $E[2](\mathbb{F}_p) =$

$E[2]$ and $\#E(\mathbb{F}_p) = p+1 \equiv 0 \bmod 8$, this implies that $E[4](\mathbb{F}_p) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. In particular, there is a unique point $P_\rightarrow \in E[2]$ whose halves are defined over $\mathbb{F}_p$, namely, the point that corresponds to $(0,2) \in \mathbb{Z}_2 \times \mathbb{Z}_4$.

Using a change of variables if needed, we can assume that $E : y^2 = x^3 + ax^2 + bx$ for certain $a, b \in \mathbb{F}_p$ and that $P_\rightarrow = (0,0)$. From Exercise 10 we know that b is a square. When translating the other points of order 2 to the origin, we get similar equations, of which the coefficients at x become $\delta(\delta \pm a)/2$ with $\delta^2 = a^2 - 4b$. The product of these coefficients equals the non-square $-b\delta^2$, so one of them is a square and the other one is not. The classification then follows from another application of Exercise 10.

Finally, since

$$\phi(P_\rightarrow) = \phi(2Q_\rightarrow) = Q_\rightarrow + \pi(Q_\rightarrow) = 2Q_\rightarrow = P_\rightarrow,$$

where $Q_\rightarrow$ denotes any half of $P_\rightarrow$, we know that $E[\mathfrak{l}_0] = \langle P_\rightarrow \rangle$. A similar calculation (do it) shows that $E[\bar{\mathfrak{l}}_0] = \langle P_\leftarrow \rangle$. By exclusion, we then know that $\langle P_\downarrow \rangle$ must take us to the floor. □

Thus our strategy (a-c) from Section 2 works better than expected. Indeed, the point $P = [(p+1)/2]Q$ from step (b) admits $[(p+1)/4]Q$ as an $\mathbb{F}_p$-rational half, therefore it is guaranteed to generate $E[\mathfrak{l}_0]$.

Example 2. The CSURF-512 parameter set from [2] again takes $r = 74$ and lets

$$p = 4 \cdot 3 \cdot \underbrace{(2 \cdot 3 \cdot \ldots \cdot 389)}_{\substack{\text{75 consecutive primes,} \\ \text{skip 347 and 359}}} - 1$$

which is about 2^{513}. Thanks to the extra prime $\ell_0 = 2$, we can sample the last 12 exponents $e_{63}, \ldots, e_{74}$ from $\{-4, \ldots, 4\}$ rather than $\{-5, \ldots, 5\}$, still covering an exponent set of size $(2 \cdot 5 + 1)^{63}(2 \cdot 4 + 1)^{12} \approx 2^{256} \approx \sqrt{p}$.

We end this section with a comment on the remaining case $p \equiv 1 \bmod 4$. Here, the ideal $(2, \sqrt{-p} - 1) \subset \mathbb{Z}[\sqrt{-p}]$ is invertible of norm 2, but it squares to the principal ideal (2), so its class has order 2. Repeatedly acting with this ideal class makes us jump back and forth between two supersingular elliptic curves over $\mathbb{F}_p$; see Figure 4. Therefore 2-isogenies are not of great help here: when included in the pool of "easy isogenies", it only makes sense to sample the corresponding exponent e_0 from $\{0, 1\}$. To make things worse, the 2-torsion part of the class group does not offer any security, and somehow even compromises it [6, Thm. 10]; see Jana's lecture for more details.

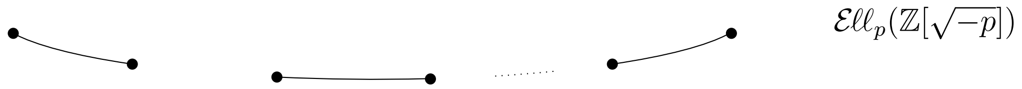

FIGURE 4. Some components of the 2-isogeny graph of supersingular elliptic curves over $\mathbb{F}_p$ when $p \equiv 1 \bmod 4$.

5. Chains of 2-isogenies

Although our basic approach (a-c) successfully produces the generator $P_\rightarrow$ of $E[\mathfrak{l}_0]$, this method is suboptimal. Indeed, an optimistic estimate for the cost of the scalar multiplication in step (b) is $10 \log p$ multiplications in $\mathbb{F}_p$ [7, §13.2], and since there is a 50% chance of hitting $P = 0$, that cost is doubled on average. On the other hand, writing $E : y^2 = f(x)$, we know that $P_\rightarrow = (\alpha, 0)$ for some root α of $f(x)$. The roots of $f(x)$ can be found using the Cantor–Zassenhaus algorithm, after which one can determine which root corresponds to $P_\rightarrow$ by computing halves.

Exercise 11. *Make a rough estimate of the expected cost of this approach, and show that it improves upon our basic strategy (a-c).*

The gain is not spectacular. Moreover, remember from Section 2 that the cost of scalar multiplication can be amortized over various primes ℓ_i by pushing points through isogenies. In view of this, implementing the root-finding approach seems not worth the effort.

This story changes radically when considering *chains* of 2-isogenies, i.e., when computing the action of $[\mathfrak{l}_0]^{e_0}$ for some $e_0 > 1$. Indeed, after the first isogeny, we get the point $P_\leftarrow$ for free, since it is the generator of the kernel of the dual isogeny (remember that $\mathfrak{l}_0\bar{\mathfrak{l}}_0 = (2)$). Thus we are left with a *quadratic* polynomial, rather than a cubic one.

Explicitly, for the first application of $[\mathfrak{l}_0]$ we find the point $P_\rightarrow$ using the basic approach, and we position it at the origin:

$$E : y^2 = x^3 + ax^2 + bx, \qquad P_\rightarrow = (0, 0). \tag{4}$$

The isogenous curve $[\mathfrak{l}_0]E = E/\langle P_\rightarrow \rangle$ is then given by

$$E_1 : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

with $(0, 0)$ generating the dual isogeny [17, Prop. on p. 79], so it concerns the point $P_\leftarrow$ of E_1. For the next application of $[\mathfrak{l}_0]$, we need to find $P_\rightarrow \in E_1$. The roots of $x^2 - 2ax + a^2 - 4b$ are $a \pm 2\beta$ for some square root $\beta \in \mathbb{F}_p^\times$ of b, so we know that

$$\{(a \pm 2\beta, 0)\} = \{P_\rightarrow, P_\downarrow\}.$$

To decide which point is which, in view of Lemma 3, it suffices to check whether or not $(a + 2\beta, 0)$ has a half with x-coordinates in $\mathbb{F}_p$. To that end, let us move $(a + 2\beta, 0)$ to the origin, in order to end up with a new defining equation

$$y^2 = x^3 + (a + 6\beta)x^2 + 4\beta(a + 2\beta)x$$

for E_1. In view of Exercise 10, we need to check whether $4\beta(a + 2\beta)$ is a square or not.

We see that finding $P_\rightarrow$ on E_1 can be done through a square root computation (to determine β), followed by an additional quadratic residuosity check. This is already much better than the basic approach using scalar multiplication. However, interestingly, the quadratic residuosity check can be avoided! The reason is that $a + 2\beta$ is always a square, regardless of our choice of β:

Lemma 4. *Assume $p \equiv 7 \bmod 8$ and consider an elliptic curve $E : y^2 = x^3 + ax^2 + bx$ in $\mathcal{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2])$ such that b is the square of some element $\beta \in \mathbb{F}_p^*$. Then $P_\rightarrow = (0,0)$ if and only if $a \pm 2\beta$ are both squares in $\mathbb{F}_p^*$.*

Proof. An explicit computation shows that the halves of $(0,0)$ are

$$(\beta, \pm\beta\sqrt{a+2\beta}), \quad (-\beta, \pm\beta\sqrt{a-2\beta})$$

(e.g., by your solution to Exercise 10) from which the lemma follows readily. □

Thus, in order for $4\beta(a+2\beta)$ to be a square, it suffices to let β be the **principal square root** of b, i.e., the unique square root which is a square itself:

Exercise 12. *Consider a prime number $p \equiv 3 \bmod 4$ and a square $b \in \mathbb{F}_p^\times$. Prove that b has exactly one square root which is again a square, and show that it can be computed as $b^{(p+1)/4}$.*

Summing up, in the first step one determines $P_\rightarrow$ using the basic approach, after which one rewrites the curve in the form (4). Then one iteratively computes $\beta = b^{(p+1)/4}$ and substitutes $a \leftarrow a + 6\beta$, $b \leftarrow 4\beta(a+2\beta)$. The expected cost of each iteration is $\approx 1.5 \log p$, which is about 13 times smaller than the expected cost of the basic approach.

Example 3. Revisiting the CSURF-512 parameters, computer experiments suggest that sampling e_0 from $\{-137, \dots, 137\}$ is near-optimal. This allows one to sample 28 exponents from $\{-4, \dots, 4\}$ rather than $\{-5, \dots, 5\}$, still covering an exponent set of size $(2 \cdot 137 + 1)(2 \cdot 5 + 1)^{46}(2 \cdot 4 + 1)^{28} \approx 2^{256} \approx \sqrt{p}$. This leads to a modest but noticeable speed-up of 5.68% for key generation, when compared to CSIDH-512. The effect is likely to decrease as p grows, due to the reduced relative weight of 2-isogenies.

We finally remark that the above ideas can be generalized to isogenies of larger degree (although it scales badly), leading to a further speed-up. We refer to Fre's lecture on *radical* isogenies [3] for more details.

6. Choice of curve model

In CSIDH one works with Montgomery curves $y^2 = x^3 + Ax^2 + x$, $A \in \mathbb{F}_p \setminus \{\pm 2\}$, which have been studied intensively over the past decades. They enjoy well-optimized formulae for scalar multiplication [7, §13.2.3] and isogeny computation [13, §4]. Conveniently, the starting curve $y^2 = x^3 + x$ is already in Montgomery form, and:

Proposition 5. *Consider a prime $p > 3$ satisfying $p \equiv 3 \bmod 8$. Let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_p(E) \cong \mathbb{Z}[\sqrt{-p}]$ if and only if there exists an $A \in \mathbb{F}_p \setminus \{\pm 2\}$ such that E is $\mathbb{F}_p$-isomorphic to $y^2 = x^3 + Ax^2 + x$. Moreover, if such an A exists then it is unique.*

Proof. This is [4, Prop. 8]. □

Besides the convenience of having a unique and compact representant for each curve $E \in \mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$, this allows for an easy validation of Alice and Bob's public keys: all one needs to do is check for supersingularity. See [4, §5] for more details.

For a CSURF prime p, the situation is more subtle. Firstly, both the floor $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ and the surface $\mathcal{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2])$ contain Montgomery curves [2, Tbl. 1], so we can no longer hope for an "if and only if" as in Proposition 5. Secondly, on the surface, we do *not* have uniqueness:

Proposition 6. *Consider a prime $p \equiv 7 \bmod 8$. Let $E/\mathbb{F}_p$ be a supersingular elliptic curve with endomorphism ring $\mathbb{Z}[(1+\sqrt{-p})/2]$. There exist precisely two coefficients $A \in \mathbb{F}_p \setminus \{\pm 2\}$ such that E is $\mathbb{F}_p$-isomorphic to $y^2 = x^3 + Ax^2 + x$. For one of these coefficients, the point $(0,0)$ on the corresponding Montgomery curve is the point $P_\rightarrow$. For the other coefficient, it concerns the point $P_\leftarrow$.*

Exercise 13. *Prove Proposition 6. Hint: use Exercise 10 and mimic the relevant parts of the proof of Proposition 5.*

Exercise 14. *Show that if a Montgomery curve $y^2 = x^3 + Ax^2 + x$ satisfies $(0,0) = P_\rightarrow$, then its quadratic twist admits the model $y^2 = x^3 - Ax^2 + x$, which then satisfies $(0,0) = P_\leftarrow$.*

In order to have a unique representant, we suggest to work with Montgomery curves for which $(0,0) = P_\rightarrow$, even though this choice is somewhat arbitrary. This has the following effect on key validation: besides checking supersingularity, one should also verify that $A \pm 2$ are both squares. This indeed guarantees that the curve $y^2 = x^3 + Ax^2 + x$ is located on the surface, because it has 3 rational points of order 2 (the discriminant $A^2 - 4 = (A+2)(A-2)$ is a square), and that $(0,0) = P_\rightarrow$ thanks to Lemma 4.

When computing isogenies of odd degree using the formulae from [13, §4], the property $(0,0) = P_\rightarrow$ is preserved. Thus the action of $[\mathfrak{l}_1]^{e_1} \cdots [\mathfrak{l}_r]^{e_r}$ can be evaluated exactly as in the case of CSIDH. As for the action of $[\mathfrak{l}_0]^{e_0}$: if e_0 is positive then we proceed as in Section 5, where we note that the first instance of $P_\rightarrow$ comes for free (i.e., no large scalar multiplication is needed). If e_0 is negative then we resort to (2): we switch to the quadratic twist, proceed as in Section 5, and twist back.

It remains to fix a starting curve for Alice and Bob. From Exercise 2 we know that $y^2 = x^3 - x \in \mathcal{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2])$, but this equation is not in the desired form: we still need to position the point $P_\rightarrow$ at the origin. For this we substitute $x \leftarrow x + 1$, to obtain the curve

$$y^2 = x^3 + 3x^2 + 2x, \tag{5}$$

which meets the requirements of Lemma 4: indeed, since $p \equiv 7 \bmod 8$ we know that 2 is a square in $\mathbb{F}_p^\times$, and then so are $3 \pm 2\sqrt{2} = (1 \pm \sqrt{2})^2$. We obtain the genuine Montgomery form

$$y^2 = x^3 + (3/\sqrt{2})x^2 + x$$

by means of a suitable rescaling of the variables.[5]

We conclude by remarking that it is also possible to work with the *Montgomery*$^-$ form $y^2 = x^3 + Ax^2 - x$, which is obtained by positioning $P_\downarrow$ at the origin and which is unique:

Proposition 7. *Consider a prime $p \equiv 7 \bmod 8$ and let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_p(E) \cong \mathbb{Z}[(1+\sqrt{-p})/2]$ if and only if there exists an $A \in \mathbb{F}_p$ such that E is $\mathbb{F}_p$-isomorphic to $y^2 = x^3 + Ax^2 - x$. Moreover, if such an A exists then it is unique.*

Proof. See [2, Prop. 4]. □

Because the Montgomery formulae for scalar multiplication and isogenies can be turned into analogous formulae for Montgomery$^-$ curves with just a few sign flips [2, §3.1], and in view of the resimplified key validation enabled by Proposition 7, it is tempting to switch to the Montgomery$^-$ form. This is exactly what we put forward in [2]. However, we overlooked a subtlety that was pointed out to us by Luca De Feo: at a low level [11, p. 261], Montgomery arithmetic exploits the factorization $x(P)^2 - 1 = (x(P)+1)(x(P)-1)$ of the numerator of the formula for $x([2]P)$, which does not carry over nicely to its Montgomery$^-$ counterpart $x(P)^2 + 1$. As a result, scalar multiplication becomes slightly less efficient. This, together with a worsened compatibility with the 2-isogeny chains discussed in Section 5, makes it more reasonable to stick to plain Montgomery curves.

7. A note on the size of the class group

For each positive squarefree integer d we write $h(-d)$, resp. $\Delta(-d)$, for the class number (= size of the class group), resp. the absolute value of the discriminant, of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Recall that $\Delta(-d) = d$ if $d \equiv 3 \bmod 4$, and that $\Delta(-d) = 4d$ if $d \equiv 1 \bmod 4$. Siegel proved that

$$\frac{\log h(-d)}{\log \sqrt{\Delta(-d)}} \to 1$$

as $d \to \infty$, whence the popular estimate

$$h(-d) \approx \sqrt{\Delta(-d)}. \tag{6}$$

One should be careful with this statement: because of the logs, Siegel's result does *not* imply that the ratio $h(-d)/\sqrt{\Delta(-d)}$ is in $O(1)$. The best estimates for this ratio are due to Littlewood, who under the generalized Riemann hypothesis showed that it lies in the range

$$\left[\left(\frac{\pi}{12e^\gamma} + o(1)\right) \frac{1}{\log\log \Delta(-d)} \; , \quad \left(\frac{2e^\gamma}{\pi} + o(1)\right) \log\log \Delta(-d) \right],$$

with γ the Euler-Mascheroni constant; one checks that $e^\gamma/\pi \approx 0.56693$.

[5] In some cases it may be interesting to omit this rescaling and directly work with (5), e.g., as input to the iteration from Section 5.

Interestingly, if d is a CSIDH/CSURF prime p, then it has a strong preference for the upper end of Littlewood's range (which is good!). More concretely, we have the following improved estimates over (6):

Estimate. *For p a CSIDH prime, resp. a CSURF prime, we estimate*

$$h(-p) \approx \frac{e^\gamma}{3\pi}\sqrt{p}\log\log p, \quad \textit{resp.} \quad h(-p) \approx \frac{e^\gamma}{\pi}\sqrt{p}\log\log p.$$

As a small additional bonus worth $\log_2(3) \approx 1.58$ bits, one finds that CSURF primes tend to give rise to class groups that are 3 times as big when compared to CSIDH.[6]

To explain the improved estimate, we content ourselves with a heuristic argument; note that we did not even rigorously define what CSIDH/CSURF primes are, in that we did not quantify what it means for the ℓ_i's to be small. For the estimate, it is important that they are chosen "as small as possible". For instance, in the case of CSIDH, one could let $\ell_1, \ldots, \ell_{r-1}$ be the first $r-1$ odd primes, and then choose ℓ_r minimal such that $p = 4\ell_1 \cdots \ell_r - 1$ is prime.

Our central tool is the analytic class number formula:

Theorem 8. *For all positive squarefree integers $d > 3$ satisfying $d \equiv 3 \bmod 4$ we have*

$$h(-d) = \frac{\sqrt{d}}{\pi} \prod_{\text{primes } \ell} \frac{\ell}{\ell - \chi_{-d}(\ell)} \tag{7}$$

where $\chi_{-d}(\ell)$ is 0 if $\ell \mid d$, it is the Legendre symbol $\left(\frac{-d}{\ell}\right)$ for odd $\ell \nmid d$, and it is equal to $(-1)^{(d^2-1)/8}$ if $\ell = 2 \nmid d$.

Proof. The analytic class number formula for imaginary quadratic fields can be found in many textbooks and states that $h(-d) = w(-d)\sqrt{\Delta(-d)}L(1, \chi_{-d})/2\pi$. Here $w(-d)$ denotes the number of units in the ring of integers of $\mathbb{Q}(\sqrt{-d})$. Since $d \equiv 3 \bmod 4$ and $d > 3$, we simply have $\Delta(-d) = d$ and $w(-d) = 2$. The factor $L(1, \chi_{-d})$ is the evaluation at 1 of the Dirichlet L-function $L(s, \chi_{-d})$ with χ_{-d} the quadratic Dirichlet character for $\mathbb{Q}(\sqrt{-d})$, which on primes takes the stated values. The theorem follows by considering $L(s, \chi_{-d})$ in Euler product form, and by using that the Euler product converges for $s = 1$. The latter claim is a bit harder to find, but see e.g. this mathoverflow discussion. □

Exercise 15. *Show that $\chi_{-d}(\ell) = 1$ if and only if ℓ splits in $\mathbb{Q}(\sqrt{-d})$.*

This immediately hints at why CSIDH/CSURF primes tend to yield large class groups: by design, the small primes ℓ_i all split, so the Euler product in (7) starts off with many factors that are bigger than 1. To quantify this, we estimate that p is roughly equal to the product of all primes ℓ up to some bound B. The Prime Number Theorem in Chebyshev's form states that

$$\sum_{\ell \leq x} \log \ell \ \sim \ x,$$

[6] To avoid confusion: in both cases we are talking about the class number of the maximal order, i.e., this factor 3 is unrelated to the surface-versus-floor phenomena discussed in Exercise 8.

implying that $B \approx \log p$. Let us first focus on the CSURF case, where these small primes all split (except near the upper bound B). Then the Euler product begins with

$$\prod_{\ell \lessapprox \log p} \frac{\ell}{\ell - 1},$$

which is about $e^\gamma \log\log p$ in view of Mertens' third theorem. If p is a CSIDH prime, then a similar estimate applies, but the first Euler factor

$$\frac{2}{2-1} \text{ becomes replaced by } \frac{2}{2+1},$$

i.e., the product scales down by a factor 3. The estimates now follow by simply ignoring the Euler factors at primes ℓ larger than $\log p$: this seems justified, as these factors all lie very close to 1, and moreover they tend to "average out" because $\chi_{-d}(\ell)$ no longer has a preferred value. See [15] for a related discussion.

Example 4. For the CSIDH-512 prime this estimate is about $8.095 \cdot 10^{76}$, whereas the actual order of $\mathrm{cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$, as computed in [1], is about $8.488 \cdot 10^{76}$. The naive estimate (6) is roughly $7.298 \cdot 10^{76}$.

Regardless of these heuristics, we stress that the analytic class number formula is a very useful tool for quickly computing class numbers up to high precision. E.g., for CSIDH-512, computing

$$\frac{\sqrt{p}}{\pi} \prod_{\ell < 10^6} \frac{\ell}{\ell - \chi_{-p}(\ell)}$$

already returns the class number to the above precision $8.488 \cdot 10^{76}$.

Exercise 16. *Use your favorite computer algebra package to compute the (unknown) order of* $\mathrm{cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$*, with p the CSIDH-1024 prime from* [4]*, up to* 3 *digits of decimal precision. Compare with the estimate* $(e^\gamma/3\pi)\sqrt{p}\log\log p$*.*

8. Take-away messages

(i) For a CSIDH prime $p \equiv 3 \bmod 8$, the class number $\#\,\mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$ contains a factor 3 that offers no extra security; see Exercise 8.

(ii) Moving to $\mathrm{cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$ with $p \equiv 7 \bmod 8$ comes with:

- a bonus "easy ideal" of norm 2, whose action can be computed very efficiently, see Section 5
- a class group that regains a factor ≈ 3, which does not suffer from the above security loss; see Section 7,
- a key validation requiring two additional quadratic residuosity checks; see Section 6.

The resulting speed-up is small but noticeable. Overall there seems little reason *not* to work on the surface, but don't expect a dramatic impact.

References

[1] W. Beullens, T. Kleinjung, F. Vercauteren, *CSI-FiSh: Efficient isogeny based signatures through class group computations*, Proceedings of “Asiacrypt 2019” Part I, Lecture Notes in Computer Science **11921**, pp. 227-247 (2019)

[2] W. Castryck, T. Decru, *CSIDH on the surface*, Proceedings of “PQCrypto 2020”, Lecture Notes in Computer Science **12100**, pp. 111-129 (2020)

[3] W. Castryck, T. Decru, F. Vercauteren, *Radical isogenies*, Proceedings of ´´Asiacrypt 2020” Part II, Lecture Notes in Computer Science **12492**, pp. 493-519 (2020)

[4] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, *CSIDH: an efficient post-quantum commutative group action*, Proceedings of “Asiacrypt 2018” Part III, Lecture Notes in Computer Science **11274**, pp. 395-427 (2018)

[5] W. Castryck, L. Panny, F. Vercauteren, *Rational isogenies from irrational endomorphisms*, Proceedings of “Eurocrypt 2020” Part II, Lecture Notes in Computer Science **12106**, pp. 523-548 (2020)

[6] W. Castryck, J. Sotáková, *Breaking the decisional Diffie-Hellman problem for class group actions using genus theory*, Proceedings of “Crypto 2020” Part II, Lecture Notes in Computer Science **12171**, pp. 92-120 (2020)

[7] H. Cohen, G. Frey; R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications, Chapman & Hall/CRC (2006)

[8] J.-M. Couveignes, *Hard homogeneous spaces*, unpublished preprint, available here (1997)

[9] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2nd edition, Pure and Applied Mathematics, Wiley (2013)

[10] C. Delfs, S. Galbraith, *Computing isogenies between super-singular elliptic curves over $\mathbb{F}_p$*, Designs, Codes and Cryptography **78**(2), pp. 425-440 (2016)

[11] P. L. Montgomery, *Speeding the Pollard and elliptic curves methods of factorization*, Mathematics of Computation **48**(177), pp. 243-264 (1987)

[12] H. Onuki and T. Takagi, *On collisions related to an ideal class of order* 3 *in CSIDH*, Proceedings of “IWSEC 2020”, Lecture Notes in Computer Science **12231**, pp. 131-148 (2020)

[13] J. Renes, *Computing isogenies between Montgomery curves using the action of* $(0, 0)$, Proceedings of “PQCrypto 2018”, Lecture Notes in Computer Science **10786**, pp. 229-247 (2018)

[14] R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, Series A **46**(2), pp. 183-208 (1987)

[15] D. Shanks, *Systematic examination of Littlewood's bounds on $L(1, \chi)$*, Proceedings of “Analytic number theory”, Proceedings of Symposia in Pure Mathematics **XXIV**, pp. 267-283 (1973)

[16] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd edition, Graduate Texts in Mathematics **106**, Springer (2009)

[17] J. H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer (1992)

[18] A. V. Sutherland, *Isogeny volcanoes*, Proceedings of “ANTS-X”, MSP Open Book Series **1**, pp. 507-530 (2012)

[19] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales Scientifiques de l'École Normale Supérieure **2**(4), pp. 521-560 (1969)

Solutions to some exercises

Exercise 1. The number of $\mathbb{F}_p$-points on an elliptic curve $E/\mathbb{F}_p$ is given by the formula $p+1-\alpha-\overline{\alpha}$, with $\alpha, \overline{\alpha}$ the eigenvalues of π. These have absolute value $\sqrt{p}$, so if $\#E(\mathbb{F}_p) = p+1$ then they must be equal to $\pm\mathbf{i}\sqrt{p}$. But then the characteristic polynomial of π^2 is given by $(X-\alpha^2)(X-\overline{\alpha}^2) = (X+p)^2$, so $(\pi^2+[p])^2 = 0$, which can only happen if $\pi^2 = [-p]$.

Exercise 2. The key ingredient is that -1 is not a square in $\mathbb{F}_p^\times$. This can be used to answer the first question (prove that $E_\pm$ is supersingular), as follows: define

$$\begin{aligned} S_1 &= \{\, x \in \mathbb{F}_p \,|\, x^3 \pm x \text{ is a non-zero square} \,\}, \\ S_2 &= \{\, x \in \mathbb{F}_p \,|\, x^3 \pm x = 0 \,\}, \\ S_3 &= \{\, x \in \mathbb{F}_p \,|\, x^3 \pm x \text{ is a non-square} \,\} \end{aligned}$$

and note that $\#E_\pm(\mathbb{F}_p) = 2\#S_1 + \#S_2 + 1$ (the $+1$ comes from the point at infinity). Since -1 is a non-square, the sets S_1 and S_3 are in bijection via the map $x \mapsto -x$. Thus we find $\#E_\pm(\mathbb{F}_p) = \#S_1 + \#S_2 + \#S_3 + 1 = p+1$. The second question is immediate from Lemma 1 and the observation that $x^3 + x = x(x^2+1)$ does not factor completely over $\mathbb{F}_p$, while $x^3 - x = x(x-1)(x+1)$ does.

The third question was a bit of an open question; I personally don't know of one uniform formula that covers all p. For the sake of illustration, let me include an explicit description of ϕ for $p = 7$: it maps all affine points $(x,y) \neq (-1,0)$ to

$$\left(\frac{4(x+4)^2}{x+1}, \frac{(x+4)(x+5)}{(x+1)^2} y \right)$$

and it maps $(-1,0), \infty$ to ∞. So in this case the endomorphism is of degree 2 (for general $p \equiv 3 \bmod 4$ we have $4\deg\phi = \deg(1+\pi) = p+1$[7]).

Exercise 9. Let $r \geq 1$ denote the order of $[\mathfrak{l}_0]$ and assume by contradiction that $r < \log_2 p$. We know that $\mathfrak{l}_0^r$ is principal, hence of the form (α) with $\alpha = a + b(1+\sqrt{-p})/2$ for some $a, b \in \mathbb{Z}$. Taking norms yields

$$2^r = \left(a + \frac{b}{2}\right)^2 + p\left(\frac{b}{2}\right)^2,$$

so our assumption implies $b = 0$. But then $2^r = a^2$, so r is even and $\alpha = 2^{r/2}$. We conclude

$$\mathfrak{l}_0^r = (2^{r/2}) = \mathfrak{l}_0^{r/2}\overline{\mathfrak{l}}_0^{r/2},$$

which is impossible, in view of the unique ideal factorization property of $\mathbb{Z}[(1+\sqrt{-p})/2]$.

[7] The fact that this equals $\deg 1 + \deg \pi$ is incidental, i.e., it does *not* rely on some rule saying deg(sum) = sum(degs)! The equality holds because there are $p+1$ points for which $\pi(P) = -P$, which in turn follows from $\#E_-(\mathbb{F}_p) = p+1$ (explain).

Exercise 10. Let (x_0, y_0) be a half of $(0,0)$, and note that $x_0, y_0 \neq 0$. The tangent line at this point has slope

$$\lambda = \frac{3x_0^2 + 2ax_0 + b}{2y_0}.$$

Because $2(x_0, y_0) = (0,0)$, this tangent line should pass through $-(0,0) = (0,0)$. So another expression for λ is simply y_0/x_0. Equating both expressions and clearing denominators yields $2y_0^2 = 3x_0^3 + 2ax_0^2 + bx_0$, and then substituting $x_0^3 + ax_0^2 + bx_0$ for y_0^2 and removing a factor x_0 yields $x_0^2 - b = 0$. The statement is now immediate.

Exercise 14. Since -1 is not a square, the quadratic twist is given by $-y^2 = x^3 + Ax^2 + x$, and then the substitution $x \leftarrow -x$ yields the desired model. If the point $(0,0)$ on $y^2 = x^3 + Ax^2 + x$ equals $P_{\rightarrow}$, then $A \pm 2$ are both squares in view of Lemma 4. But then $-A \pm 2$ are both non-squares, so again from Lemma 4 we see that the point $(0,0)$ on the twisted curve $y^2 = x^3 - Ax^2 + x$ is *not* the point $P_{\rightarrow}$. By Exercise 10 it cannot be the point $P_{\downarrow}$ either, so it must concern the remaining option $P_{\leftarrow}$.