Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time

AUREL PAGE AND DAMIEN ROBERT

Abstract. In this short note, we present a simplified (but slower) version Clapoti of Clapotis, whose full description will appear later in [PR23]. Let $E/\mathbb{F}_q$ be an elliptic curve with an effective primitive orientation by a quadratic imaginary order $R \subset \operatorname{End}(E)$. Let $\mathfrak{a}$ be an invertible ideal in R. Clapoti is a randomized polynomial time algorithm in $O\left((\log \Delta_R + \log q)^{O(1)}\right)$ operations to compute the class group action $E \mapsto E_\mathfrak{a} \simeq E/E[\mathfrak{a}]$.

1. Introduction

Let $E/\mathbb{F}_q, q = p^e$, be an elliptic curve with an effective primitive orientation by a quadratic imaginary order $R \subset \operatorname{End}(E)$, and $\mathfrak{a}$ be an invertible ideal in R. In this short note, we explain how to compute the class group action by $\mathfrak{a}$ in polynomial time.

Although *specific* instantiations of the full class group action (rather than a restricted action) are known [BKV19; FFK+23; CL23], as explained by Lorenz Panny in `https://yx7.cc/blah/2023-04-14.html` none of them is asymptotically polynomial. By contrast, Clapoti is a polynomial time algorithm that applies to *any* orientation.

We use the now standard trick of going to higher dimension, initially introduced in the SIDH attacks [CD23; MMPPW23; Rob23]. For this, we need to extend the class group action $\mathrm{Cl}(R)$ on E to higher dimension. In [PR23], we build an anti-equivalence of categories between unimodular hermitian torsion free R-modules and N-similitudes on one hand, and principally polarised R-oriented (not necessarily primitively) abelian varieties A isogeneous to E^n and oriented N-isogenies on the other hand (with the restriction that the R-action on differentials ρ_A on A has to be equivalent to ρ_E^n when p is inert in R, owing to the fact that in this case the Frobenius map $\pi_p : E \to E^{(p)}$ is not represented by an ideal). This equivalence of categories is an extension to the oriented setting of an equivalence of categories proved in the non oriented setting in [JKP+18; KNRR21]. The isogeny $\phi_\mathfrak{a} : E \to E_\mathfrak{a}$ of kernel $E[\mathfrak{a}]$ corresponds under this equivalence to the module map $(\mathfrak{a}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{a})) \to (R, \mathcal{N}(\cdot))$, with $\mathcal{N}(\cdot)$ the norm form. This representation does not requires $\mathfrak{a}$ to be invertible, and can therefore also be used to represent going up isogenies (by taking $\mathfrak{a}$ to be the conductor ideal); hence even in dimension 1 it is more general than the class group action.

We then build an N-similitude $(\mathfrak{a}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{a})) \oplus (\overline{\mathfrak{a}}, \mathcal{N}(\cdot)/\mathcal{N}(\mathfrak{a})) \to (R, \mathcal{N}(\cdot)) \oplus (R, \mathcal{N}(\cdot))$ for a “nice” N (e.g. smooth), which we translate back to a N-isogeny $E \times E \to E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}}$. By the converse of Kani's lemma [Kan97], such an isogeny also comes from an isogeny diamond in dimension 1. This allows us to give a simplified (but potentially slower) version Clapoti (CLass group Action in POlynomial TIme) of Clapotis (CLass group Action in POlynomial TIme via Sesquilinear forms), bypassing the equivalence of categories (see Proposition 2.1).

2. The algorithm

Let $E/k, k = \mathbb{F}_q$, be an elliptic curve, and $R \subset \operatorname{End}_k(E)$ be a primitive orientation on E by a quadratic imaginary order of discriminant Δ_R. We will assume that the orientation is effective, meaning that we can evaluate an explicit non trivial endomorphism δ (of polynomial norm) of R on E in polynomial time; such an efficient isogeny representation always exist by [Rob22a]. (By polynomial time, we always mean in term of $\log \Delta_R$ and $\log q$, and by polynomial norm we always mean in term of Δ_R.) All other endomorphisms are of the form $\frac{a+b\delta}{f}$ and can be evaluated in polynomial time too (if they have polynomial norm) by the division algorithm of [Rob22b].

Let $K = \operatorname{Frac} R$, and let $\mathfrak{a}$ be an integral invertible ideal in R (of polynomial norm, which we can always assume by reducing $\mathfrak{a}$ first if necessary). The ideal class group action gives an isogeny $\phi_\mathfrak{a} : E \to E_\mathfrak{a}$ of kernel $E[\mathfrak{a}]$. We

Date: March 29, 2024.
Funded by ANR Ciao (ANR-19-CE48-0008).

say that the N-torsion of E is *accessible* if the primary parts of $E[N]$ lie in small extensions, i.e., extensions of polynomial degree in $O(\log q)$.

Proposition 2.1. *Let $\mathfrak{b}, \mathfrak{c}$ be two explicit integral ideals equivalent to $\mathfrak{a}$ of polynomial norm such that $\mathcal{N}(\mathfrak{b}) + \mathcal{N}(\mathfrak{c}) = N$. Then there is a N-isogeny $F : E \times E \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$, whose kernel can be efficiently computed provided that $\mathcal{N}(\mathfrak{b})$ is coprime to $\mathcal{N}(\mathfrak{c})$ and the N-torsion is accessible.*

Proof. Since $\mathfrak{b}$ is equivalent to $\mathfrak{a}$, there exists $\beta \in K^*$ such that $\mathfrak{b} = \beta\mathfrak{a}$; since $\mathfrak{b}$ is integral and $\mathfrak{a}\overline{\mathfrak{a}} = \mathcal{N}(\mathfrak{a})$, we have $\beta = \overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a})$ for some $\gamma_b \in \mathfrak{a}$ of norm $\mathcal{N}(\gamma_b) = \mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{a})$. Conversely, given $\gamma_b \in \mathfrak{a}$, the ideal $\mathfrak{b} = \overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a}) \cdot \mathfrak{a}$ is an integral ideal equivalent to $\mathfrak{a}$ of norm $\mathcal{N}(\gamma_b)/\,\mathcal{N}(\mathfrak{a})$. Furthermore, since $\overline{\mathfrak{b}}\mathfrak{a} = (\gamma_b)$, the element γ_b can be efficiently computed as the smallest element in the lattice $\overline{\mathfrak{b}}\mathfrak{a}$. Likewise, fix a $\gamma_c \in \mathfrak{a}$ inducing the equivalent ideal $\mathfrak{c}$.

Since $\overline{\mathfrak{a}}$ lies in the class $[\mathfrak{a}]^{-1}$ of the class group, we have that $\overline{\mathfrak{c}}\mathfrak{b}$ is a principal ideal, and in fact $\overline{\mathfrak{c}}\mathfrak{b} = (\gamma_c\overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a}))$. We remark that $\gamma_c\overline{\gamma_b}$ is in $\mathfrak{a}\overline{\mathfrak{a}} = (\mathcal{N}(\mathfrak{a}))$, so $\gamma := \gamma_c\overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a})$ is a well defined endomorphism on E.

Now consider the following isogeny diamond:

$$\begin{tikzcd}
E \arrow[r, "\phi_{\mathfrak{b}}"] \arrow[d, "\phi_{\overline{\mathfrak{c}}}"] & E_{\mathfrak{a}} \arrow[d, "\phi_{\overline{\mathfrak{c}}}"] \\
E_{\overline{\mathfrak{a}}} \arrow[r, "\phi_{\mathfrak{b}}"] & E
\end{tikzcd}$$

which is commutative because $\phi_{\overline{\mathfrak{c}}} \circ \phi_{\mathfrak{b}} = \phi_{\mathfrak{b}} \circ \phi_{\overline{\mathfrak{c}}} = \gamma = \gamma_c\overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a})$. Kani's lemma then gives an N-isogeny $F : E \times E \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}, F = \begin{pmatrix} \phi_{\mathfrak{b}} & \tilde{\phi}_{\overline{\mathfrak{c}}} \\ -\phi_{\overline{\mathfrak{c}}} & \tilde{\phi}_{\mathfrak{b}} \end{pmatrix}$. If $\mathcal{N}(\mathfrak{b})$ is coprime to $\mathcal{N}(\mathfrak{c})$, the kernel of F is given by $\{(\mathcal{N}(\mathfrak{b})P, \gamma P) \mid P \in E[N]\}$. □

Corollary 2.2. *Let $\mathfrak{b}, \mathfrak{c}$ be two integral ideals equivalent to $\mathfrak{a}$ of coprime norms such that $\mathcal{N}(\mathfrak{b}) + \mathcal{N}(\mathfrak{c}) = N$ is smooth and the N-torsion is accessible. Then $E_{\mathfrak{a}}$ can be recovered in polynomial time.*

Proof. By Proposition 2.1, we have an explicit N-isogeny $F : E \times E \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$, which can be computed in polynomial time.

We now need to distinguish between $E_{\mathfrak{a}}$ and $E_{\overline{\mathfrak{a}}}$. The first copy of E has an isogeny of degree $\mathcal{N}(\mathfrak{b})$ to $E_{\mathfrak{a}}$ and an isogeny of degree $\mathcal{N}(\mathfrak{c})$ to $E_{\overline{\mathfrak{a}}}$, and this relationship is reversed for the second copy of E. Taking a small ℓ such that these norms are different modulo ℓ, we can use the Weil pairing on the ℓ-torsion to distinguish the two isogenies. □

Remark 2.3. When $\mathcal{N}(\mathfrak{b})$ is not coprime to $\mathcal{N}(\mathfrak{c})$, we still have an isogeny diamond. The description of the kernel of a general isogeny diamond is given in [Kan97, Corollary 2.11], but it is a priori not obvious how we might recover the kernel of F without knowing the action of $\phi_{\mathfrak{b}}, \phi_{\overline{\mathfrak{c}}}$ on $E[N]$ first. However, in Proposition 2.1, F comes from a module map, and in [PR23], we explain how to recover the kernel associated with an arbitrary module map, so in that case we can recover the kernel of F even if the coprimality condition of Proposition 2.1 and Corollary 2.2 is not satisfied.

Let us explain the case of the specific isogeny F to illustrate the usefulness of the module representation. We have $\mathfrak{b} = \frac{\overline{\gamma_b}}{\mathcal{N}(\mathfrak{a})}\mathfrak{a}$, so the multiplication map $\overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a})\colon (\mathfrak{a}, \mathcal{N}(\cdot)/\,\mathcal{N}(\mathfrak{a})) \to (\mathfrak{b}, \mathcal{N}(\cdot)/\,\mathcal{N}(\mathfrak{b}))$ is an isomorphism α_b of unimodular Hermitian modules. The isogeny $\phi_{\mathfrak{b}} : E \to E_{\mathfrak{a}}$ corresponds from the module point of view to the post-composition of α_b with the natural $\mathcal{N}(\mathfrak{b})$-similitude given by the inclusion $(\mathfrak{b}, \mathcal{N}(\cdot)/\,\mathcal{N}(\mathfrak{b})) \to (R, \mathcal{N}(\cdot))$.

Likewise, the isogeny F from Proposition 2.1 corresponds to a N-similitude $\psi\colon (\mathfrak{a}, \mathcal{N}(\cdot)/\,\mathcal{N}(\mathfrak{a})) \oplus (\overline{\mathfrak{a}}, \mathcal{N}(\cdot)/\,\mathcal{N}(\mathfrak{a})) \to (R, \mathcal{N}(\cdot)) \oplus (R, \mathcal{N}(\cdot))$.

The anti-equivalence of categories is exact, so the kernel of F corresponds to the cokernel of ψ. Fix two generators of $\mathfrak{a}$, these generators induce surjective maps $R^2 \twoheadrightarrow \mathfrak{a}$, $R^2 \twoheadrightarrow \overline{\mathfrak{a}}$. Pre-composing ψ with these epimorphisms, we get a module map $\tilde{\psi}\colon R^4 \to R^2$, whose cokernel is exactly the cokernel of ψ. The map $\tilde{\psi}$ is given by a 4×2 matrix of elements of R, hence of endomorphisms on E, and corresponds on the abelian variety side to a morphism $\tilde{\Phi}\colon E^2 \to E^4$. By exactness, the cokernel $\operatorname{coker}\tilde{\psi} = \operatorname{coker}\psi$, which as we have seen corresponds to $\operatorname{Ker} F$, is given by $\operatorname{Ker}\tilde{\Phi}$ which we can explicitly compute since the orientation by R is effective on E.

Remark 2.4. Using $\phi_{\mathfrak{b}}$, we can transfer the effective orientation on E to an effective orientation on $E_{\mathfrak{a}}$ by using the division algorithm of [Rob22b], as explained in [MW23, Lemma 6.11].

It remains to find ideals $\mathfrak{b}, \mathfrak{c}$ satisfying the conditions of Corollary 2.2. First we handle the coprimality condition.

Lemma 2.5. *Given $\mathfrak{a} \subset R$ an invertible ideal, it is possible to find in randomized polynomial time two equivalent integral ideals $\mathfrak{b}, \mathfrak{c}$ whose norms are polynomial in Δ_R and coprime to each other.*

Proof. Let $\mathfrak{h}$ be an integral ideal of polynomial norm, we explain how to find in polynomial time an ideal equivalent to $\mathfrak{a}$ and coprime to $\mathfrak{h}$.

Given an element a in $\mathfrak{a}^{-1}$, then $a\mathfrak{a}$ is integral, and it is coprime to $\mathfrak{h}$ iff for each of the finitely many prime ideals $\mathfrak{h} \subset \mathfrak{p}_i \subset R$ containing $\mathfrak{h}$, $a \notin \mathfrak{p}_i\mathfrak{a}^{-1}$. By the CRT, $\pi \colon \mathfrak{a}^{-1} \to \prod \mathfrak{a}^{-1}/\mathfrak{p}_i\mathfrak{a}^{-1}$ is surjective, and any $a \in \mathfrak{a}^{-1}$ such that $\pi_i(a) \neq 0$ for all i gives an ideal $a\mathfrak{a}$ coprime to $\mathfrak{h}$. If the primes above $\mathfrak{h}$ are known, we can find a suitable $\pi(a)$ in the codomain by linear algebra, and then lift it to $\mathfrak{a}^{-1}$.

Otherwise, we turn to a randomized algorithm. Fix a bound B large enough (but still polynomial) so that the image of π restricted to the ball of radius B is close to uniform, and sample uniformly in $\mathfrak{a}^{-1}$ with bound B (e.g. using [DLRW23, Lemma 4.2.1]) to obtain our required a in random average polynomial time. (As an optimisation: failed random samples, i.e. samples $a \in \mathfrak{a}^{-1}$ such that $a\mathfrak{a}$ is not coprime to $\mathfrak{h}$ give informations on the primes above $\mathfrak{h}$, which we can use to refine the sampling.)

We apply this algorithm to $\mathfrak{h} = \mathcal{N}(\mathfrak{a})$, and take $\mathfrak{b} = \mathfrak{a}$, $\mathfrak{c} = a\mathfrak{a}$. □

Remark 2.6. In Lemma 2.5, we need $\mathfrak{a}$ to be invertible. If $\mathfrak{f} = \bar{\mathfrak{f}}$ is the conductor ideal, all elements in $\mathfrak{f}$ have norm divisible by $\mathcal{N}(\mathfrak{f})^2$, so using Proposition 2.1 with $\mathfrak{a} = \mathfrak{f}$, we can only build N-isogenies with $\mathcal{N}(\mathfrak{f}) \mid N$.

We now need to adjust $\mathfrak{b}, \mathfrak{c}$ so that $\mathcal{N}(\mathfrak{b}) + \mathcal{N}(\mathfrak{c})$ is nice. In this note, we are not looking for an efficient algorithm, just a provably polynomial time one, so we sidestep this problem by going to dimension 8 as in [Rob23].

Proposition 2.7. *Let $\mathfrak{b}, \mathfrak{c}$ two integral ideals equivalent to $\mathfrak{a}$ of norm coprime to each other. Let N be any integer $N \geq \mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c})$. Then, possibly replacing N by $4N$, there exists an N-isogeny $F : E^8 \to E_{\mathfrak{a}}^4 \times E_{\bar{\mathfrak{a}}}^4$.*

Proof. Since $\mathcal{N}(\mathfrak{b})$ is coprime to $\mathcal{N}(\mathfrak{c})$, every integer N is an integral linear combination $N = u\,\mathcal{N}(\mathfrak{b}) + v\,\mathcal{N}(\mathfrak{c})$. If $N \geq \mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c})$, we may find u, v positive by the pigeonhole principle. Let x be an element of the Lipschitz quaternion order whose norm is u and y an element whose norm is v. (By [PT18], x and y can be found by a randomized polynomial time algorithm.) We identify x, y with their 4×4 integral matrix, hence with endomorphisms of E^4 that commute with $\phi_{\mathfrak{b}}$ and $\phi_{\bar{\mathfrak{c}}}$.

Let $z = yx$, by metacommutation we can write $z = x'y'$ where $\mathcal{N}(x') = \mathcal{N}(x)$, $\mathcal{N}(y') = \mathcal{N}(y)$, but x', y' may live in the Hurwitz quaternionic order. The Hurwitz order has an Euclidean division (for both sides), so all ideals are principals and finding a generator can be done efficiently by the Euclidean algorithm. If $u = \mathcal{N}(x), v = \mathcal{N}(y)$ are coprime, we can compute x' as the left gcd of z and $\mathcal{N}(x)$ and set $y' = x'^{-1}z$; the coprimality condition ensures that $\mathcal{N}(x') = \mathcal{N}(x)$,

Since the Liptschitz order is of index 2 inside the maximal Hurwitz order, replacing x', y' by $2x', 2y'$ if necessary (hence also multiplying x, y by 2 and u, v, N by 4), we can assume that x', y' are also given by integral coefficients, i.e. live in the Lipschitz order.

Consider the isogeny diamond:

$$\begin{tikzcd}
E^4 \arrow[r, "\phi_{\mathfrak{b}} x"] \arrow[d, "\phi_{\bar{\mathfrak{c}}} y'"] & E_{\mathfrak{a}}^4 \arrow[d, "y \phi_{\bar{\mathfrak{c}}}"] \\
E_{\bar{\mathfrak{a}}}^4 \arrow[r, "x' \phi_{\mathfrak{b}}"] & E^4
\end{tikzcd}$$

From the diamond in Proposition 2.1 and the construction of x, y, x', y', we do have commutativity, hence Kani's lemma yields a N-isogeny. □

Remark 2.8. If x', y' do not lie in the Liptschitz order, rather than replacing N by $4N$, we can still build an isogeny diamond associated to $y\phi_{\bar{\mathfrak{c}}} \circ \phi_{\mathfrak{b}} x$ since ud_1 is coprime to vd_2; but the bottom left element of the diamond will not be isomorphic to $E_{\bar{\mathfrak{a}}}^4$ anymore. Ensuring that x', y' are in the Lipschitz order (at the cost of eventually replacing N by $4N$) has the nice side effect that we compute $E_{\mathfrak{a}}$ and $E_{\bar{\mathfrak{a}}}$ at the same time in one step.

Theorem 2.9. *The isogeny $\phi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$ can be computed in randomized polynomial time.*

Proof. Use Lemma 2.5 to sample $\mathfrak{b}, \mathfrak{c}$ of coprime norms. Take $N > \mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c})$ coprime to each and such that N is smooth and the N-torsion is accessible (e.g. take N powersmooth).

Replacing N by a divisor of it if necessary, we can assume that the u, v of the proof of Proposition 2.7 are coprime to each other, and so also to N, hence in particular that $u\,\mathcal{N}(\mathfrak{b})$ is coprime to $v\,\mathcal{N}(\mathfrak{c})$.

Assume first that we do not need to change N by $4N$ in Proposition 2.7. With the notations of Propositions 2.1 and 2.7, the composition $y\phi_{\bar{\mathfrak{c}}} \circ x\phi_{\mathfrak{b}} = yx \operatorname{diag}(\gamma)$ in the isogeny diamond is explicit. Thus we can recover the kernel of F as in the proof of Proposition 2.1, evaluate F and recover $E_{\mathfrak{a}}$, $E_{\bar{\mathfrak{a}}}$, and distinguish the two by using pairings as in Corollary 2.2.

Since we know how to evaluate F and $\tilde{F}$, we know how to evaluate $x\phi_{\mathfrak{b}}, y'\phi_{\bar{\mathfrak{c}}}$ and their duals, hence some explicit integer multiple of $\phi_{\mathfrak{b}}, \phi_{\mathfrak{c}}$ and their duals, hence the isogenies $\phi_{\mathfrak{b}}, \phi_{\mathfrak{c}}$ and their duals by the division algorithm of [Rob22b]. The isogeny $\phi_{\mathfrak{a}}$ differ from $\phi_{\mathfrak{b}}$ by the non integral endomorphism $\overline{\gamma_b}/\,\mathcal{N}(\mathfrak{a}) \in K$, so we can also evaluate $\phi_{\mathfrak{a}}$ on suitable torsion points, hence recover $\phi_{\mathfrak{a}}$ by [Rob22a].

Now in the case where we need to change N by $4N$ in Proposition 2.7, in the isogeny diamonds we have isogenies of degrees whose gcd is 4. Assume for simplicity that our original N was odd, then we can still recover the odd part of the kernel $\operatorname{Ker} F$, and we only miss $\operatorname{Ker} F[4]$.

By Remark 2.3, using our module description of F we can still recover its full kernel. In our current simplified description, a solution is to simply try all $O(1)$ possible kernels $\operatorname{Ker} F[4]$ until a splitting isogeny is found. We then verify that the splitting is correct as follows (heuristically there will be only one splitting among all our choices anyway). By the above reasoning, we know how to evaluate $\phi_{\bar{\mathfrak{c}}}$ and $\phi_{\mathfrak{b}}$. The decomposition is correct if and only if the composition $\phi_{\bar{\mathfrak{c}}} \circ \phi_{\mathfrak{b}}$ gives the endomorphism γ defined in the proof of Proposition 2.1.

An alternative is to use Remark 2.8 to keep using N rather than $4N$. The downside is that we give up obtaining $E_{\bar{\mathfrak{a}}}$ at the same time as $E_{\mathfrak{a}}$. □

Remark 2.10 (An heuristic algorithm in dimension 4)**.** Assume that $\mathfrak{b}, \mathfrak{c}$ are of coprime norm.

We can work in dimension 4 in Proposition 2.7 whenever we can find positive u, v such that $N = u\,\mathcal{N}(\mathfrak{b}) + v\,\mathcal{N}(\mathfrak{c})$ and u, v are sums of two squares. In this case we can find $x, y \in \mathbb{Z}[i]$ (the Gaussian integers) of norm $\mathcal{N}(\mathfrak{b})$, $\mathcal{N}(\mathfrak{c})$ (efficiently if these norms are prime) and represent them by 2×2-integral matrices (that commute with each other). Taking N to be coprime to $\mathcal{N}(\mathfrak{b})$ and $\mathcal{N}(\mathfrak{c})$, we can assume as in Theorem 2.9 the degrees $u\,\mathcal{N}(\mathfrak{b})$ and $v\,\mathcal{N}(\mathfrak{c})$ to be coprime, so the kernel of the isogeny F associated with the corresponding diamond is easy to describe via the endomorphism $yx \operatorname{diag}(\gamma)$. (Like in Remark 2.3, we could also relax the coprimality condition by using the module representation.)

Heuristically, we expect u to be a prime congruent to 1 modulo 4 with probability $\Omega(1/\log N)$, and both u, v to satisfy these conditions with probability $\Omega(1/\log^2 N)$. There are at least $\frac{N}{\mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c})}$ possible couples (u, v), so we expect heuristically to find a solution as soon as $N = \Omega(\mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c}) \log^2(\mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c})))$.

If we cannot find suitable u, v for given $N, \mathfrak{b}, \mathfrak{c}$, we can simply tweak N or (if we want to find N as small as possible) rerandomize $\mathfrak{b}, \mathfrak{c}$ until a suitable solution is found.

By Minkowski's bound, we know that there exists two linearly independent elements w_1, w_2 in $\mathfrak{a}$ such that $\|w_1\|\|w_2\| \leq \mathcal{N}(\mathfrak{a})\Delta_R^{1/2}$. Taking $\|w_1\| \leq \|w_2\|$, and using the fact that $\mathcal{N}(x) = \|x\|^2$ and that if $x \in \mathfrak{a}$, $\mathcal{N}(x) \geq \mathcal{N}(\mathfrak{a})$, we find that $\|w_1\| \leq \mathcal{N}(\mathfrak{a})^{1/2}\Delta_R^{1/4}$ and $\|w_2\| \leq \mathcal{N}(\mathfrak{a})^{1/2}\Delta_R^{1/2}$. So the reduced (i.e. the minimal) ideal equivalent to $\mathfrak{a}$ is of norm $\leq \Delta_R^{1/2}$. And there are many equivalent ideals of norm $O(\Delta_R)$, so we can expect to find $\mathfrak{b}, \mathfrak{c}$ of coprime norm such that $\mathcal{N}(\mathfrak{b})\,\mathcal{N}(\mathfrak{c}) = O(\Delta_R^{3/2})$, hence embed the isogeny $E \to E_{\mathfrak{a}}$ into a dimension 4 N-isogeny whenever $N \approx \Delta_R^{3/2} \log^2 \Delta_R$. If the lattice $\mathfrak{a}$ is not too skewed (so that $\|w_2\| \approx \|w_1\|$), we can even expect to find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norm $\approx \Delta_R^{1/2}$, which lowers N to $N \approx \Delta_R \log^2 \Delta_R$.

Remark 2.11. A similar strategy as in Theorem 2.9 applies whenever we can find two isogenies $f, g : E_1 \to E_2$ of coprime degrees N_1, N_2 such that the endomorphism $\gamma = \tilde{g} \circ f$ on E_1 is known. As in Proposition 2.1, we use the isogeny diamond associated with the pushforward square

$$\begin{tikzcd}
E \arrow[r, "f"] \arrow[d, "g'"] & E_2 \arrow[d, "\tilde{g}"] \\
E_2' \arrow[r, "\tilde{f}'"] & E
\end{tikzcd}$$

where $g' : E \to E_2'$ is the isogeny with kernel $f^{-1}(\operatorname{Ker} \tilde{g})$, and $\operatorname{Ker} \tilde{f}' = g'(\operatorname{Ker} \tilde{g} \circ f)$.

Then for any $N > N_1 N_2$, we can embed f, g into an N-isogeny F in dimension 8 as in Proposition 2.7 (or possibly dimension 4 as in Remark 2.10), whose kernel K can be recovered from the action of γ on $E[N]$.

A situation where this might be useful is, as a variant to the KLPT algorithm, to compute the Deuring correspondence from an ideal I to an isogeny $\phi_I : E_1 \to E_2$ between two supersingular curves over $\mathbb{F}_{p^2}$, when we have an effective representation of $\operatorname{End}_{\mathbb{F}_{p^2}}(E_1)$. We sample two ideals J_1, J_2 equivalent to I of coprime reduced norms as in Lemma 2.5 and embed ϕ_I into a N-isogeny F of dimension 8 via the isogeny diamond associated with the decomposition $\overline{J_2} J_1 = \overline{J_1'} J_2'$ for some ideals J_1', J_2' of reduced norm $\mathcal{N}(J_1), \mathcal{N}(J_2)$ respectively. Compared to [Wes22], this gives a proven polynomial time version of an `IdealToIsogeny` algorithm without GRH (at the cost of going to dimension 8 instead of staying in dimension 1).

Heuristically, we can expect to find J_1, J_2 of norm $N_1, N_2 \approx \sqrt{p}$, and compute ϕ_I via a N-isogeny in dimension 8 with $N \approx p$ (resp. of dimension 4 with $N \approx p \log^2 p$).

(As in the R-oriented case, the isogeny F is represented by an explicit module map, so we can compute its full kernel K even in the non coprime degrees case. Thus we can relax the coprimality condition on J_1, J_2 at the expense that N will need to be divisible by the gcd of the reduced norms of J_1, J_2.)

Remark 2.12 (Splitting and pushforward of isogenies)**.** Let $f_1 : E_0 \to E_1$ be a d_1-isogeny, $f_2 : E_1 \to E_2$ a d_2-isogeny, with d_1 coprime to d_2, and let $f = f_2 \circ f_1$. Assume that we know an efficient representation of f, meaning that we can evaluate it on points efficiently. Then the same techniques as in Remark 2.11 allow to find in polynomial time an efficient representation of f_1 and f_2. Indeed Proposition 2.1 works too if γ is an isogeny rather than an endomorphism, we just need to be able to evaluate it on points to recover $\operatorname{Ker} F$.

In fact, it suffices to find a u-isogeny $x : A_u \to E_0^m$ and a v-isogeny $y : E_2^m \to A_v$, in some dimension m, such that we have an efficient representation of x, y (for instance take $m = 4$ and use quaternion matrices). We apply a variant of Proposition 2.1 to recover $\operatorname{diag}(f_1) \circ x$ and $y \circ \operatorname{diag}(f_2)$ and then apply the division algorithm to recover f_1, f_2. Indeed, the division algorithm applies for any isogeny x with an efficient representation: then $\tilde{x}$ has an efficient representation (by the same argument as in [Rob22b, § 5.1]), so we can compose on the right by $\tilde{x}$ to reduce to a division by an integer.

We remark that f also decomposes uniquely as $f = f_1' \circ f_2'$ where f_1' is a d_1-isogeny and f_2' a d_2-isogeny. Furthermore f_2' is the pushforward of f_2 by $\tilde{f}_1$, and $\tilde{f}_1'$ is the pushforward of $\tilde{f}_1$ by f_2. It follows that if we know an efficient representation of $f_1 : E_0 \to E_1$ a d_1-isogeny and of $f_2 : E_0 \to E_2$ a d_2-isogeny with d_1 prime to d_2, then since we can derive an efficient representation of $\tilde{f}_1 : E_1 \to E_0$, hence of $f = f_2 \circ \tilde{f}_1$, we can compute in polynomial time an efficient representation of the pushforwards f_1' of f_1 by f_2 and f_2' of f_2 by f_1.

3. The full algorithm

The algorithm presented in these notes (at least the dimension 8 version) is impractical. The full Clapotis algorithm describes several improvements.

First, there is no real need to go to dimension 8 as in Proposition 2.7; the endomorphism order R in $\operatorname{End}(E)$ is of rank 2 (which we do not even exploit in Proposition 2.7), which is already large enough to devise an algorithm to find suitable ideals $\mathfrak{b}, \mathfrak{c}$ for Corollary 2.2 encoding a N-isogeny (for N large enough). This allows us to work in dimension 2. For instance, for CSIDH-1024 [CLMPR18], taking a random prime $p \equiv 3 \mod 4$ of 1024 bits and a random prime ideal $\mathfrak{a}$ of 512 bits, our algorithm implemented in Pari/GP finds a B-powersmooth isogeny in dimension 2 computing the action of $\mathfrak{a}$ with $B = 2591$.

Still, a 2591-isogeny in dimension 2 is of very large degree 6713281. So for practical specific instantiations of Clapotis, it would be convenient to be able to choose $N = 2^m$ a large power of 2, and a CSIDH-prime p with some accessible 2^t torsion (and extra accessible smooth torsion), and decompose the isogeny F into blocks of

2^t-isogenies a la SQISign [DKLPW20; DLW22]. As a first step for this decomposition, we need a way to describe the intermediate abelian surfaces; this is where we can leverage our equivalence of categories described in Section 1. Indeed, we can describe the intermediate principally polarised abelian surfaces as explicit submodules of rank 2 inside the Hermitian module $(R, \mathcal{N}(\cdot)) \oplus (R, \mathcal{N}(\cdot))$.

4. Acknowledgment

The second author gives special thanks to Antonio Sanso, who spurred this project by asking if we could apply the methods of QFesta [NO23] to CSIDH. We remark also that [CL23, Proposition 10] is essentially Proposition 2.1 applied to $\mathfrak{a} = R$, so this Proposition can be seen as an extension of the ideas of SCALLOP-HD from R to an arbitrary ideal.

References

[BKV19] W. Beullens, T. Kleinjung, and F. Vercauteren. "CSI-FiSh: efficient isogeny based signatures through class group computations". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2019, pp. 227–247 (cit. on p. 1).

[CD23] W. Castryck and T. Decru. "An efficient key recovery attack on SIDH". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 423–447 (cit. on p. 1).

[CLMPR18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. "CSIDH: an efficient post-quantum commutative group action". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2018)*. Springer. 2018, pp. 395–427 (cit. on p. 5).

[CL23] M. Chen and A. Leroux. "SCALLOP-HD: group action from 2-dimensional isogenies". In: *Cryptology ePrint Archive* (2023) (cit. on pp. 1, 6).

[DLRW23] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. "SQISignHD: New Dimensions in Cryptography". Mar. 2023. eprint: 2023/436. (Cit. on p. 3).

[DKLPW20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. "SQISign: compact post-quantum signatures from quaternions and isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2020)*. Springer. 2020, pp. 64–93 (cit. on p. 6).

[DLW22] L. De Feo, A. Leroux, and B. Wesolowski. "New algorithms for the Deuring correspondence: SQISign twice as fast". In: *Cryptology ePrint Archive* (2022) (cit. on p. 6).

[FFK+23] L. D. Feo, T. B. Fouotsa, P. Kutas, A. Leroux, S.-P. Merz, L. Panny, and B. Wesolowski. "SCALLOP: scaling the CSI-FiSh". In: *IACR International Conference on Public-Key Cryptography*. Springer. 2023, pp. 345–375 (cit. on p. 1).

[JKP+18] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, and J. T. Tate. "Abelian varieties isogenous to a power of an elliptic curve". In: *Compositio Mathematica* 154.5 (2018), pp. 934–959 (cit. on p. 1).

[Kan97] E. Kani. "The number of curves of genus two with elliptic differentials." In: *Journal für die reine und angewandte Mathematik* 485 (1997), pp. 93–122 (cit. on pp. 1, 2).

[KNRR21] M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. "Spanning the isogeny class of a power of an elliptic curve". In: *Mathematics of Computation* 91.333 (Sept. 2021), pp. 401–449. DOI: 10.1090/mcom/3672 (cit. on p. 1).

[MMPPW23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. "A direct key recovery attack on SIDH". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 448–471 (cit. on p. 1).

[MW23] A. H. L. Merdy and B. Wesolowski. "The supersingular endomorphism ring problem given one endomorphism". In: *arXiv preprint arXiv:2309.11912* (2023) (cit. on p. 3).

[NO23] K. Nakagawa and H. Onuki. "QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras". In: *Cryptology ePrint Archive* (2023) (cit. on p. 6).

[PR23] A. Page and D. Robert. "Clapotis: Evaluating the isogeny class group action in polynomial time". In preparation. Nov. 2023 (cit. on pp. 1, 2).

[PT18] P. Pollack and E. Treviño. “Finding the Four Squares in Lagrange’s Theorem.” In: *Integers* 18 (2018), A15 (cit. on p. 3).

[Rob22a] D. Robert. “Evaluating isogenies in polylogarithmic time”. Aug. 2022. eprint: 2022/1068, HAL: hal-03943970. (Cit. on pp. 1, 4).

[Rob22b] D. Robert. “Some applications of higher dimensional isogenies to elliptic curves (overview of results)”. Dec. 2022. eprint: 2022/1704, HAL: hal-03943973. (Cit. on pp. 1, 3–5).

[Rob23] D. Robert. “Breaking SIDH in polynomial time”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 472–503 (cit. on pp. 1, 3).

[Wes22] B. Wesolowski. “The supersingular isogeny path and endomorphism ring problems are equivalent”. In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2022, pp. 1100–1111 (cit. on p. 5).

Email address: aurel.page@inria.fr

Email address: damien.robert@inria.fr

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE