# An Effective Lower Bound on the Number of Orientable Supersingular Elliptic Curves

Antonin Leroux

[1] DGA
[2] LIX, CNRS, Ecole Polytechnique, Institut Polytechnique de Paris
[3] INRIA
antonin.leroux@polytechnique.org

**Abstract.** In this article, we prove a generic lower bound on the number of $\mathfrak{O}$-*orientable* supersingular curves over $\mathbb{F}_{p^2}$, i.e curves that admit an embedding of the quadratic order $\mathfrak{O}$ inside their endomorphism ring. Prior to this work, the only known effective lower-bound is restricted to small discriminants. Our main result targets the case of fundamental discriminants and we derive a generic bound using the expansion properties of the supersingular isogeny graphs.
Our work is motivated by isogeny-based cryptography and the increasing number of protocols based on $\mathfrak{O}$-oriented curves. In particular, our lower bound provides a complexity estimate for the brute-force attack against the new $\mathfrak{O}$-uber isogeny problem introduced by De Feo, Delpech de Saint Guilhem, Fouotsa, Kutas, Leroux, Petit, Silva and Wesolowski in their recent article on the SETA encryption scheme.

## 1 Introduction

The link between quadratic imaginary orders and elliptic curves have always been of great importance to elliptic-curve cryptography, and isogeny-based cryptography is no exception. This connection dates back to the very beginning of the field with the CRS scheme, discovered independently by Couveignes [Cou06] and Rostovtsev and Stolbunov [RS06]. Their original idea is based on isogenies between ordinary curves, i.e elliptic curves whose endomorphism ring is isomorphic to a quadratic imaginary order. However, for both security and efficiency reasons, ordinary curves were soon replaced by supersingular curves, i.e curves whose endomorphisms ring is isomorphic to a maximal order inside a quaternion algebra. With the CGL hash function [CLG09] and the SIDH key exchange [JDF11] leading the charge, it seemed like the quadratic orders were destined to slowly disappear from the picture. However, they claimed back a share of the spotlight with CSIDH [CLM+18], a revival of CRS in the setting of supersingular curves with the quadratic order obtained by restricting to endomorphisms defined over $\mathbb{F}_p$. In fact, quadratic orders were never really gone as quaternion orders actually contain an infinity of them. Isogeny experts only needed time to understand their place in the rapidly evolving picture of isogeny-based cryptography. In parallel of numerous schemes built upon CSIDH and its variants ([BKV19,ADFMP20]

among others), several papers appeared trying to study the link between isogenies of supersingular curves and quadratic imaginary orders outside of the CSIDH framework. We can mention the OSIDH protocol by Colò and Kohel [CK19] for quadratic orders of smooth discriminant which introduced the terminology of orientations that we use in this paper and the work of Love and Boneh [LB20] on quadratic orders of small discriminant. More recently, Chenu and Smith [CS21] studied the case where the discriminant is a small integer times $p$. De quehen et al. have highlighted in [QKL+21] the possibility to use the embedding of a specific quadratic order as a backdoor to break unbalanced variants of SIDH. The SETA encryption scheme [DFFdSG+21] is built on the same principle. The set of SETA public keys is simply the set of $\mathfrak{O}$-orientable curves for some quadratic order $\mathfrak{O}$ and secret keys are concrete $\mathfrak{O}$-orientations. Additionally, the authors from SETA have introduced the "uber-isogeny assumption" as an attempt to provide a common framework for various security assumptions in isogeny-based cryptography. The formulation of the $\mathfrak{O}$-Uber Isogeny Problem ($\mathfrak{O}$-UIP) is explicitly parametrized by a quadratic imaginary order $\mathfrak{O}$ and it was shown in [DFFdSG+21] how different variants of the $\mathfrak{O}$-UIP were related to the security of several isogeny-based protocols (including SIDH).

Given the rich history that we have summarized above, it is important to study in more details the link between quadratic orders and isogenies of supersingular curves. In this work, we study the number of $\mathfrak{O}$-orientable supersingular elliptic curves over $\mathbb{F}_{p^2}$ for a given quadratic order $\mathfrak{O}$, we write $\mathcal{E}_{\mathfrak{O}}(p)$ for this set. The complexity of the brute force algorithm to solve the $\mathfrak{O}$-UIP is linear in $\#\mathcal{E}_{\mathfrak{O}}(p)$. Aiming at the cryptographic applications, we look for an effective bound in the cases where $d$ is polynomial in $p$ and both have cryptographic size.

*Related works.* The number of orientable supersingular curve is related to the number of optimal embeddings of quadratic orders inside maximal orders of the quaternion algebra ramified at $p$ and $\infty$ and is also linked with representation number of integers by ternary quadratic forms. Both quantity have been studied in the literature but not with the same goal. As far as we know, prior to our work, an effective bound is only known for a restricted range of discriminants and is due to Kaneko [Kan89]. In [Voi21, Chapter 30], several formulas are given involving these numbers (such as the Eichler class number formula) but it does seem easy to derive an effective bound from that. There are also asymptotic results on representation number of ternary quadratic forms (see for instance [IK21, Chapter 20]) but they rather target the case where $d$ grows to infinity while $p$ is fixed. Our work also shares some similarities with the trend of work started by Gross and Zagier [ZG85] on singular moduli and later enriched by Dorman and Lauter and Viray [Dor87,LV15]. Their results cannot be directly applied to our case because they target simultaneous embeddings of quadratic orders of distinct discriminants while we are going to focus on simultaneous embeddings of quadratic orders with the same discriminant. Nonetheless, some of the techniques developed in these works have inspired part of our analysis.

*Contributions.* Our main result is Proposition 11, a lower bound on $\#\mathcal{E}_{\mathfrak{O}}(p)$ when $\mathfrak{O}$ is a maximal quadratic order. The proof is based on the study of $K_{\mathfrak{O}}(p)$, the number of quaternion orders obtained from pairs of distinct $\mathfrak{O}$-orientations. With Proposition 14, we cover the case of non-maximal orders and a lower bound on $\#\mathcal{E}_{\mathfrak{O}}(p)$ can be derived for any quadratic order by combining Propositions 11 and 14.

The statement of Proposition 11 involves a function $\tau$ that has already appeared in [EHL+20] to analyze the complexity of an algorithm computing the endomorphism ring of a supersingular curve. We study this function to make the bound of Proposition 11 more effective and prove a conjecture formulated in [EHL+20] on the asymptotic behavior of $\tau$.

Asymptotically, our bound becomes trivial when the discriminant grows while the characteristic $p$ stays fixed. However, in the case where the discriminant is polynomial in $p$, our bound proves to be quite tight as we illustrate by using it to verify that the parameters proposed in [DFFdSG+21] for the SETA encryption scheme reach the claimed level of security.

The remainder of this paper is organized as follows: Section 2 introduces the necessary notations and mathematical notions. Section 3 is where we present our main result. We start by treating the case of fundamental discriminants in Section 3.2 before stating the generic result in Section 3.3. In Section 4, we prove the conjecture from [EHL+20] on the asymptotic behavior of the $\tau$ function. Finally, in Section 5, we apply our results to a concrete example corresponding to the parameters of SETA.

## 2 Mathematical background

*Notations.* Throughout this document, we place ourselves in $B_{p,\infty}$, the definite quaternion algebra ramified at $p$ and $\infty$ for some prime $p > 3$. We consider supersingular elliptic curves over $\mathbb{F}_{p^2}$ and write $N_p$ for the number of isomorphism classes of such curves over the algebraic closure of $\mathbb{F}_p$.

We fix an imaginary quadratic field $\mathfrak{K}$ of discriminant $-d$ and ring of integers $\mathfrak{O}_{\mathfrak{K}}$. For any $\mathfrak{O} \subset \mathfrak{O}_{\mathfrak{K}}$, we write $f(\mathfrak{O})$ the conductor of $\mathfrak{O}$, i.e the only integer such that $\mathfrak{O} = \mathbb{Z} + f(\mathfrak{O})\mathfrak{O}_{\mathfrak{K}}$, when it is clear from the context we will simply write $f$. The class group of $\mathfrak{O}$ is $\mathrm{Cl}(\mathfrak{O})$ and the class number is $h(\mathfrak{O})$. As a convention, we use $\mathcal{O}_*$ for quaternion orders in $B_{p,\infty}$ and $\mathfrak{O}_*$ for quadratic imaginary orders.

We write $\mathbb{P}$ for the set of all primes. For any $d \in \mathbb{N}$, we define $\mathbb{P}_d = \{\ell,\ \ell \in \mathbb{P} \text{ and } \ell | d\}$.

### 2.1 Quaternion orders

For $a, b \in \mathbb{Z}^\star$ we denote by $H(a,b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$ the quaternion algebra over $\mathbb{Q}$ with basis $1, i, j, k$ such that $i^2 = a$, $j^2 = b$ and $k = ij = -ji$. The unique quaternion algebra (up to isomorphism) ramified exactly at $p$ and $\infty$, is always isomorphic to $H(-q, -p)$ where $q$ is a small integer relatively to $p$ ($q = O(\log(p)^2)$. For instance, when $p = 3 \mod 4$, we can always take $q = 1$.

Every quaternion algebra has a canonical involution that sends an element $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ to its conjugate $\overline{\alpha} = a_1 - a_2 i - a_3 j - a_4 k$. We define the *reduced trace* and the *reduced norm* by $tr(\alpha) = \alpha + \overline{\alpha}$ and $n(\alpha) = \alpha\overline{\alpha}$.

Quaternion orders of $B_{p,\infty}$ are lattices of rank 4 inside $B_{p,\infty}$ that are also rings. It can be shown that quaternion orders are integral, i.e that norm and trace of all the elements are in $\mathbb{Z}$. Given a basis $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of $\mathcal{O}$, the *reduced discriminant* (or simply discriminant) of $\mathcal{O}$ is $\mathrm{disc}(\mathcal{O}) = \sqrt{\det(\alpha_i \alpha_j)_{i,j \in [1,4]}}$. For any $\mathcal{O} \subset B_{p,\infty}$, we have $p | \mathrm{disc}(\mathcal{O})$. The discriminant of a suborder $\mathcal{O}' \subset \mathcal{O}$ satisfies $\mathrm{disc}(\mathcal{O}) | \mathrm{disc}(\mathcal{O}')$.

*Maximal* orders are the orders that admit no suborder and, in particular, their discriminant is equal to $p$. *Eichler* orders are equal to intersection of two maximal orders (not necessarily distinct). Every quaternion order admit the unique decomposition $\mathbb{Z} + f(\mathcal{O})\mathrm{Gor}(\mathcal{O})$ where $f(\mathcal{O}) \in \mathbb{N}$ is the *Brandt Invariant* and $\mathrm{Gor}(\mathcal{O})$ is the *Gorenstein closure*. We can define Gorenstein orders as orders whose Brandt Invariant is 1. As the name suggests, $\mathrm{Gor}(\mathcal{O})$ is always Gorenstein. An order is *Bass* when all its superorders are Gorenstein. Equivalently, Bass orders of $B_{p,\infty}$ are the orders containing a maximal order of a quadratic imaginary order (this was originally the definition of *basic* orders but the two notions were proven equivalent by Chari, Smertnig and Voight in [CSV21]).

We have a chain of proper implication between all those notions

$$\text{maximal} \Rightarrow \text{Eichler} \Rightarrow \text{Bass} \Rightarrow \text{Gorenstein}.$$

We refer the reader to the book of John Voight for more backgrounds on quaternion algebras and quaternion orders [Voi21].

In this article, we will make use of *embedding numbers* of Bass orders, i.e the number of distinct maximal orders containing a given order. This problem was studied by Eichler and Brzezinski [BE92,Brz83] and was more recently used in [EHL+20] to estimate the complexity of an algorithm to compute the endomorphism ring of a supersingular curve. For the rest of this section, we fix a Bass order $\mathcal{O}$ of discriminant $D$. Following [BE92], we denote by $e(\mathcal{O})$ the *embedding number of* $\mathcal{O}$. It turns out that $e(\mathcal{O})$ can be computed efficiently using the local-to-global principle with the formula $e(\mathcal{O}) = \prod_{\ell \in \mathbb{P}} e_\ell(\mathcal{O})$ where $e_\ell(\mathcal{O})$ is the analog of $e(\mathcal{O})$ over the $\ell$-adics: $e_\ell(\mathcal{O})$ is the number of maximal orders in $B_{p,\infty} \otimes \mathbb{Q}_\ell$ containing $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$. An easy preliminary observation is that, $e_\ell(\mathcal{O}) = 1$ when $\ell$ is coprime with $D$. Thus, we can rewrite the above formula as $e(\mathcal{O}) = \prod_{\ell \in \mathbb{P}_d} e_\ell(\mathcal{O})$. The value of $e_\ell(\mathcal{O})$ is in fact closely related to the Eichler symbol $(\mathcal{O}/\ell)$, a notion introduced by Eichler in [Eic36]. Let us write $k$ for the residue field of $\mathbb{Q}_\ell$ and $J$ for the Jacobson radical of $\mathcal{O}_\ell$. Then, we define the Eichler symbol as follows:

$$\left(\frac{\mathcal{O}}{\ell}\right) = \begin{cases} 1 & \text{if } \mathcal{O}_\ell / J \cong k \times k, \\ 0 & \text{if } \mathcal{O}_\ell / J \cong k, \\ -1 & \text{if } \mathcal{O}_\ell / J \text{ is a quadratic extension of k.} \end{cases} \tag{1}$$

The Eichler symbol is a very useful tool to understand the structure of an order $\mathcal{O}$ by the local-global principle. For instance, the order $\mathcal{O}_\ell$ is Eichler if and only if

$(\mathcal{O}/\ell) = 1$. The Eichler symbol can be seen as a generalization of the Kronecker symbol, as becomes explicit with the reinterpretation presented in Proposition 1 (see [Voi21]). For any quaternion element $\alpha$, we write $\Delta(\alpha) = \mathrm{disc}(\mathbb{Z}[\alpha]) = \mathrm{tr}(\alpha)^2 - 4n(\alpha)$.

**Proposition 1.** *$\left(\frac{\mathcal{O}}{\ell}\right) = \epsilon$ if and only if $\left(\frac{\Delta(\alpha)}{\ell}\right)$ takes all the values $0, \varepsilon$ when $\alpha$ ranges over all the elements of $\mathcal{O}$.*

Then, it was shown by Eichler in [Eic36] (see [Brz83] for an account in english of this result) how the value of the Eichler symbol was linked to $e_\ell(\mathcal{O})$. We write $v_\ell(n)$ for the $\ell$-adic valuation of a integer $n$.

**Proposition 2.** *Let $\mathcal{O}$ be a Bass order in $B_{p,\infty}$ of discriminant $D$ and $\ell \in \mathbb{P}_D$:*

$$e_\ell(\mathcal{O}) = \begin{cases} v_\ell(D) + 1 & \text{if } (\mathcal{O}/\ell) = 1, \\ 2 & \text{if } (\mathcal{O}/\ell) = 0 \text{ and } \ell \neq p, \\ 1 & \text{if } (\mathcal{O}/\ell) = -1 \text{ or } (\mathcal{O}/\ell) = 0 \text{ and } \ell = p. \end{cases}$$

*Remark 1.* Note that $e_p(\mathcal{O})$ is always equal to 1. This follows from Proposition 2 and the fact that $(\mathcal{O}/p)$ cannot be 1.

### 2.2 Quadratic orders and oriented supersingular elliptic curves

In this section, we recall basic definition and properties about orientations of elliptic curves. This notion was first introduced by Colo and Kohel in [CK19]. Note that our definition below is in fact what is defined as a *primitive* orientation in [CK19]. This also matches the notion of *optimal embeddings* of Love and Boneh [LB20].

**Definition 1.** *Let $\mathfrak{K}$, be a quadratic imaginary field. For any elliptic curve $E$, a $\mathfrak{K}$-orientation is a ring homomorphism $\iota : \mathfrak{K} \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$. A $\mathfrak{K}$-orientation induces an $\mathfrak{O}$-orientation if $\iota(\mathfrak{O}) = \mathrm{End}(E) \cap \iota(\mathfrak{K})$. In that case, the pair $(E, \iota)$ is called a $\mathfrak{O}$-oriented curve and $E$ is an $\mathfrak{O}$-orientable curve.*

When $E/\mathbb{F}_{p^2}$ is supersingular, Deuring showed that $\mathrm{End}(E)$ is a maximal order of $B_{p,\infty}$ [Deu41] and so we have $\mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$. We denote by $\mathcal{S}_{\mathfrak{O}}(p)$ the set of $\mathfrak{O}$-oriented supersingular curves over $\mathbb{F}_{p^2}$ up to isomorphism and Galois conjugacy. Note that this does not exactly match the definition used in [Onu21,Wes21] where orientations are not considered up to Galois conjugacy. We took this convention because we can state precise results when working up to Galois conjugacy (the Frobenius, which is the only non-trivial element in the Galois group of $\mathbb{F}_{p^2}$, creates somewhat artificial duplicates of a given orientation). The following proposition was shown by Onuki [Onu21, Proposition 3.2] and gives a concrete criterion to determine when $\mathcal{S}_{\mathfrak{O}}(p)$ is not empty.

**Proposition 3.** *The set $\mathcal{S}_{\mathfrak{O}}(p)$ is not empty if and only if $p$ does not split in $\mathfrak{K}$ and does not divide the conductor of $\mathfrak{O}$.*

A consequence of [Onu21, Proposition 3.3, Theorem 3.4] is that $\#\mathcal{S}_{\mathfrak{O}}(p) = h(\mathfrak{O})$ when the criterion in Proposition 3 is met. In that case, the class group $\mathrm{Cl}(\mathfrak{O})$ acts on $\mathfrak{O}$-orientations through an operation that we write $\mathfrak{a} \star (E, \iota) = (E^{\mathfrak{a}}, \iota^{\mathfrak{a}})$.

We define $\mathcal{E}_{\mathfrak{O}}(p)$ as the set of $\mathfrak{O}$-orientable curves (under isomorphism and Galois conjugacy) for which there exists a $\mathfrak{O}$-orientation. By definition, we have the obvious inequality $\#\mathcal{E}_{\mathfrak{O}}(p) \leq \min(\#\mathcal{S}_{\mathfrak{O}}(p), N_p)$.

The recent article [DFFdSG+21] introduced a new isogeny-based problem: the $\mathfrak{O}$-Uber Isogeny Problem ($\mathfrak{O}$-UIP). We describe below as Problem 1, the $\mathfrak{O}$-UBER variant introduced by Wesolowski in [Wes21]. We assume for Problem 1 that $\mathfrak{O}$ and $p$ satisfy the constraint in Proposition 3.

*Problem 1.* ($\mathfrak{O}$-UBER) Given $(E, \iota) \in \mathcal{S}_{\mathfrak{O}}(p)$ and $F \in \mathcal{E}_{\mathfrak{O}}(p)$, find $\mathfrak{a} \in \mathrm{Cl}(\mathfrak{O})$, such that $F = E^{\mathfrak{a}}$.

The brute force method to solve Problem 1 consists in trying all ideal classes until a solution is found. The expected complexity of this algorithm is linear in $\#\mathcal{E}_{\mathfrak{O}}(p)$ (and not $h(\mathfrak{O})$ since we look for any class connecting $E$ and $F$ and not a specific class).

## 3 The number of $\mathfrak{O}$-orientable supersingular curves.

In this section, we pursue the main goal of this article: finding a generic lower bound on the size of $\mathcal{E}_{\mathfrak{O}}(p)$. Henceforth, we assume that the Legendre symbol $(\mathrm{disc}(\mathfrak{O})/p) \neq 1$ and the conductor $f(\mathfrak{O})$ is coprime with $p$ so we know by Proposition 3 that $\#\mathcal{E}_{\mathfrak{O}}(p) > 0$. We start with Section 3.1, where we introduce useful results from the literature and show a first lower bound when $\mathrm{disc}(\mathfrak{O}) \leq p$. In Section 3.2, we prove our main lower bound in the case where $f(\mathfrak{O}) = 1$. We extend this result to the generic case using the expansion property of the isogeny graphs in Section 3.3.

### 3.1 A first result for small discriminants

The main result of this Section is Proposition 5 that was first proven by Kaneko in [Kan89]. This proposition allows us to derive interesting results on $\mathcal{E}_{\mathfrak{O}}(p)$ with Corollaries 1 and 2 (Corollary 1 being the only effective lower bound on $\#\mathcal{E}_{\mathfrak{O}}(p)$ prior to this work). Proposition 5 is obtained by studying the quaternion order generated by two integral elements in $B_{p,\infty}$. The study of these objects will prove of prime importance for our results as well.

*The quaternion order generated by two non-commuting elements.* Let us take $\alpha_1, \alpha_2$, two integral elements in $B_{p,\infty}$. We want to look at the order $\mathcal{O}_{1,2} = \langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$. When $\alpha_1$ and $\alpha_2$ are not commuting, $\mathcal{O}_{1,2}$ is a quaternion order, i.e has rank 4 as a $\mathbb{Z}$-module. In Proposition 4, we give the classical formula to compute $\mathrm{disc}(\mathcal{O}_{1,2})$. Proposition 5 is a consequence of this formula.

**Proposition 4.** *Let $\mathfrak{O}_i$ be quadratic orders equal to $\mathbb{Z}[\alpha_i]$ for $i = 1, 2$ such that $\alpha_1, \alpha_2$ are not commuting. Let $D_i = \mathrm{disc}(\mathfrak{O}_i)$, $t_i = \mathrm{tr}(\alpha_i)$ for $i \in \{1, 2\}$ and $s = \mathrm{tr}(\alpha_1\alpha_2)$, then $\mathrm{disc}(\mathcal{O}_{1,2}) = (D_1D_2 - (t_1t_2 - 2s)^2)/4$.*

**Proposition 5.** *Let $\mathfrak{O}_i$ be quadratic orders equal to $\mathbb{Z}[\alpha_i]$ for $i = 1, 2$ such that $\alpha_1, \alpha_2$ are not commuting. If $\mathfrak{O}_1, \mathfrak{O}_2$ have respective discriminant $-f_i^2 d$ (where $d$ is a fundamental discriminant) and are contained inside the same quaternion maximal order $\mathcal{O} \subset B_{p,\infty}$, we have that $p \leq f_i f_j d$.*

*Proof.* We can write $\mathfrak{O}_i = \mathbb{Z}[\alpha_i]$ for two integral elements $\alpha_1, \alpha_2$. We can consider the quaternion order $\mathcal{O}_{1,2}$ generated by these two elements because $\alpha_1, \alpha_2$ do not commute. When $D_i = -f_i^2 d$, we can rewrite the formula from Proposition 4 as $(D_1D_2 - (t_1t_2 - 2s)^2)/4 = (f_1f_2d - t_1t_2 + 2s)(f_1f_2d + t_1t_2 - 2s)/4$. Wlog we can assume that $t_1t_2 - 2s > 0$ (as we can replace $\alpha_1$ by $-\alpha_1$ if needed). The discriminant of a quaternion order is always divisible by $p$. Since $p$ is prime, we have that $p$ divides either $(f_1f_2d - t_1t_2 + 2s)/2$ or $(f_1f_2d + t_1t_2 - 2s)/2$. Since $0 < t_1t_2 - 2s < f_1f_2d$, both factors are smaller than $f_1f_2d$ and so we have that $p$ is always smaller than $f_1f_2d$.

*Remark 2.* During the proof for Proposition 5 we showed that $t_1t_2 - 2s = \pm f_1f_2d \mod p$. This fact will be useful for what follows in Section 3.2.

Proposition 5 allows us to show interesting properties, including a lower bound on the size of $\mathcal{E}_{\mathfrak{O}}(p)$ (Corollary 1) and a bound on the minimal distance between two $\mathfrak{O}$-oriented curves (Corollary 2).

**Corollary 1.** *When $\mathrm{disc}(\mathfrak{O}) < p$, $\#\mathcal{E}_{\mathfrak{O}}(p) = \#\mathcal{S}_{\mathfrak{O}}(p) = h(\mathfrak{O})$.*

*Proof.* If we assume that $\#\mathcal{E}_{\mathfrak{O}}(p) < \#\mathcal{S}_{\mathfrak{O}}(p)$, then there must be a curve $E$ with two distinct $\mathfrak{O}$-orientations $\iota_1, \iota_2$. Under the Deuring correspondence, this implies that there are two distinct quadratic orders $\mathfrak{O}_1, \mathfrak{O}_2$ isomorphic to $\mathfrak{O}$ contained inside the maximal order $\mathcal{O} \cong \mathrm{End}(E)$. By Proposition 5, $p$ must be smaller than $d$ which contradicts our assumption.

**Corollary 2.** *Let $\ell$ be a prime different from $p$. If $\ell$ is inert in $\mathfrak{O}$ of discriminant $d$, then the smallest chain of $\ell$-isogenies between two curves of $\mathcal{E}_{\mathfrak{O}}(p)$ has degree larger than $p/d$.*

*Proof.* (sketch) Let us write $E_1, E_2$ these two curves and $\mathcal{O}_1, \mathcal{O}_2$, their respective endomorphism rings and let us take $\varphi : E_1 \to E_2$ the smallest chain of $\ell$-isogenies connecting them. Let us write $\theta_i \in \mathcal{O}_i$ such that $\mathfrak{O} \cong \mathbb{Z}[\theta_i]$. Since $\ell$ is inert in $\mathfrak{O}$, we can show that $\alpha_1 = \theta_1$ and $\alpha_2 = \hat{\varphi} \circ \theta_2 \circ \varphi$ are two elements in $\mathcal{O}_1$ that are not commuting (otherwise, at least one of the isogeny composing $\varphi$ would be commuting with $\theta$ which is impossible since $\ell \neq p$ and is inert in $\mathfrak{K}$). Since $\mathrm{disc}(\mathbb{Z}[\alpha_1]) = -d$ and $\mathrm{disc}(\mathbb{Z}[\alpha_2]) = -\deg\varphi^2 d$, we obtain the desired bound by applying Proposition 5.

### 3.2 The case of $\mathfrak{O}_{\mathfrak{K}}$.

In this section, we focus on the case where $\mathfrak{O} = \mathfrak{O}_{\mathfrak{K}}$ for a quadratic imaginary field $\mathfrak{K}$ of discriminant $-d$. Our main result is Proposition 11.

To improve the reader understanding, we divide the proof of Proposition 11 into several Lemmas and Propositions. Next, we give a brief outline and some insights on the generic principle. Our starting point is the observation (already used to prove Corollary 1) that if $\#\mathcal{E}_{\mathfrak{O}}(p) < h(\mathfrak{O})$, then there are some curves admitting several $\mathfrak{O}$-orientations. Similarly to Proposition 5, our result is obtained through the analysis of the quaternion orders obtained by combining together the different pairs of orientations. More concretely, we bound the number of these quaternion orders in two very different ways. The first one is a lower bound depending on $\#\mathcal{E}_{\mathfrak{O}}(p)$ and $h(\mathfrak{O})$ (Proposition 7) while the second one is an upper-bound (Proposition 10) that involves an explicit quantity that can be computed from $d$ and $p$. The combination of these two bounds yields Proposition 11.

Here are some notations that we will use throughout this section. For any given $E \in \mathcal{E}_{\mathfrak{O}}(p)$, we write $N_E \geq 1$ for the number of distinct $\mathfrak{O}$-orientations of $E$. We write $\iota_1, \ldots, \iota_{N_E}$ for these $N_E$ orientations, they induce the existence of endomorphisms $\alpha_1, \ldots, \alpha_{N_E} \in \mathrm{End}(E)$ such that $(\iota_i(\mathfrak{O}))_{1 \leq i \leq N_E} = (\mathbb{Z}[\alpha_i])_{1 \leq i \leq N_E}$. Since $\mathfrak{O}$ is the maximal order of $\mathfrak{K}$, we can assume that $\alpha_i$ is either $\sqrt{-q}$ or $(1 + \sqrt{-q})/2$ where $q$ is the squarefree integer such that $\mathfrak{K} = \mathbb{Q}(\sqrt{-q})$. Let $I^2_{\neq}(N_E)$ be the set of pairs of distinct unordered elements inside $\{1, \ldots, N_E\}$. We define an equivalence relation $\sim_E$ on $I^2_{\neq}(N_E)$ as

$$(i, j) \sim_E (l, m) \text{ iff } \langle 1, \alpha_i, \alpha_j, \alpha_i\alpha_j \rangle = \langle 1, \alpha_l, \alpha_m, \alpha_l\alpha_m \rangle.$$

The set of equivalence classes under $\sim_E$ is denoted by $\mathcal{K}_E$. Intuitively, $\mathcal{K}_E$ is the set of distinct quaternion orders obtained by combining two embeddings of $\mathfrak{O}$ inside $\mathrm{End}(E)$. We write $K_E = \#\mathcal{K}_E$.

By the results presented in Section 2.2, we have $h(\mathfrak{O}) = \#\mathcal{S}_{\mathfrak{O}}(p) = \sum_{E \in \mathcal{E}_{\mathfrak{O}}(p)} N_E$. The quantity we propose to study is $K_{\mathfrak{O}}(p) = \sum_{E \in \mathcal{E}_{\mathfrak{O}}(p)} K_E$.

*The link between $\#\mathcal{E}_{\mathfrak{O}}(p)$ and $K_{\mathfrak{O}}(p)$.* The number $K_E$ is obviously related to $N_E$ for every curve $E \in \mathcal{E}_{\mathfrak{O}}(p)$. Intuitively, we would like to say that every pair $\alpha_i, \alpha_j$ generates a different quaternion order $\mathcal{O}_{i,j}$ with $1 \leq i < j \leq N_E$ (thus proving that $K_E = N_E(N_E - 1)/2$). However, even if this seems to be the case with good probability, it is not true in full generality. The correct statement is given in Proposition 6. Fortunately, Proposition 6 still allows us to derive Corollary 3 that lower-bounds $K_E$ by $CN_E(N_E - 1)$ for some constant factor $C$, which is enough for our purpose.

**Proposition 6.** *Let $\mathbb{Z}[\alpha_1], \mathbb{Z}[\alpha_2], \mathbb{Z}[\alpha_3]$ be three distinct embeddings of the quadratic order of discriminant $-d$ (with $d > 10$) inside a maximal quaternion order $\mathcal{O}$. If $d \neq 3 \mod 4$ or $d \neq 0, 1 \mod p$, then $\alpha_3 \notin \mathcal{O}_{1,2} = \langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$. When $d = 0 \mod p$, either $\alpha_3 \notin \mathcal{O}_{1,2}$ or the trace of $\alpha_1\alpha_2$ is equal to $4n(\alpha_1)$ and $\alpha_3$ is one of $\pm(\mathrm{tr}(\alpha_1)/2 + \alpha_1 - \alpha_2)$. When $d = 3 \mod 4$ and $d = 1$*

mod $p$, *either* $\alpha_3 \notin \mathcal{O}_{1,2}$ *or the trace of* $\alpha_1\alpha_2$ *is* $(d-1)/2$ *and* $\alpha_3$ *is one of* $\pm((3-d)/4+\alpha_1\alpha_2), \pm((d-3)/4+\alpha_1+\alpha_2-\alpha_1\alpha_2)$.

*Proof.* Since all orders are isomorphic, we can assume that all $\alpha_i$ have same trace and norm. Let us write $t = \mathrm{tr}(\alpha_i), n = n(\alpha_i)$ for any $i = 1, 2, 3$. If we assume that $\alpha_3 \in \mathcal{O}_{1,2}$, then there exists $v, x, y, z \in \mathbb{Z}$ such that $\alpha_3 = v + x\alpha_1 + y\alpha_2 + z\alpha_1\alpha_2$. The trace of $\alpha_3$ implies the equation $t = 2v + t(x+y) + z\mathrm{tr}(\alpha_1\alpha_2)$. Thus, we rewrite $\alpha_3 = t/2 + x(\alpha_1 - t/2) + y(\alpha_2 - t/2) + z(\alpha_1\alpha_2 - \mathrm{tr}(\alpha_1\alpha_2)/2)$. There are two different cases. If $d = 0 \mod 4$ then $d = 4q$ for some square-free $q = 1 \mod 4$ and so we can assume wlog that $t = 0$ and $\alpha_i = \omega_i$ with $\omega_i^2 = -q$. Else $d = q$ for some square-free $q = 3 \mod 4$ and we can take $t = 1$, $\alpha_i = (1+\omega_i)/2$ with $\omega_i^2 = -q$. Let us write $s = \mathrm{tr}(\omega_1\omega_2)$.
If $d = 0 \mod 4$, then we obtain the norm equation $q = n(\alpha_3) = q(x^2+y^2) + sxy + z^2(q^2 - s^2/4)$. When $d = q = 3 \mod 4$, we have $\alpha_3 = (1+\omega_3)/2 = 1/2 + x\omega_1/2 + y\omega_2/2 + z/4(1+\omega_1+\omega_2+\omega_1\omega_2-(1+1/2s))$. Thus we obtain $\omega_3 = (x+z/2)\omega_1 + (y+z/2)\omega_2 + z/2(\omega_1\omega_2 - s/2)$. Writing $x_2 = x + z/2$, $y_2 = y + z/2$, $z_2 = z/2$, and taking the norm we obtain the equation $q = n(\omega_3) = q(x_2^2+y_2^2) + sx_2y_2 + z_2^2(q^2 - s^2/4)$. Thus, we need to find the solutions $x, y, z$ in $\mathbb{Z}[1/2]$ and $x - y \in \mathbb{Z}, y - z \in \mathbb{Z}$ to the quadratic equation $q = q(x^2+y^2) + sxy + z^2(q^2 - s^2/4)$ different from the obvious solutions $(1,0,0)$ and $(0,1,0)$. We will use heavily the fact that $|s| < 2q$ (which comes from $\mathrm{disc}(\mathbb{Z})[\omega_1\omega_2] = s^2 - 4q^2 < 0$). Wlog we can assume that $s \geq 0$. First, is it clear that we cannot have $x = y = 0$. Indeed, we would have $q = z^2(q^2 - s^2/4)$ which is clearly impossible.
Let us rewrite our equation as $q = q(x^2+y^2) + sxy + z^2(q - s/2)(q + s_2)$. With the bound $(q - s/2)(q + s/2) \geq q/2$ we get that we must have $z \in \{0, \pm 1/2, \pm 1\}$. This implies that $s = 0 \mod 2$ (otherwise $q(x^2+y^2) + sxy + z^2(q - s/2)(q + s_2)$ would not be an integer). With that additional information, we can actually show that $q^2 - s^2/4 \geq q$. Thus, in fact we must have $z \in \{0, \pm 1/2\}$. We also have $q \geq q(x^2+y^2) + sxy$.
Let us assume that $xy \geq 0$, then we get $q \geq q(x^2+y^2) + sxy$. Thus, we must have $x^2 + y^2 \leq 1$. Since we exclude $(x, y) \in \{(0,0), (0,1), (1,0)\}$, the only possibility respecting all our constraints is $(x, y, z) = (1/2, 1/2, \pm 1/2)$. Thus, we obtain $q = q/2 + s/4 + q^2/4 - s^2/16$ which leads to the equation $q^2 - 2q + s(1 - s/4)$. The discriminant of $X^2 - 2X + s(1 - s/4)$ is equal to $4 - 4s + s^2 = (s-2)^2$. The two possible solutions are $s/2$ and $(4-s)/2$. The first one is impossible by the bound $s < 2q$. Since $s \geq 0$ we obtain $(4-s)/2 < 2$ and this is incompatible with the bound $d > 10$.
So we must have $xy < 0$ and wlog we can assume that $x > 0$ and $y < 0$. Then, we have $q \leq q(x^2+y^2) - s|xy|$, but the bound $s < 2q$ leads to the inequality $q(x^2+y^2) - s|xy| > q(x^2+y^2) - 2q|xy| = q(x+y)^2$. Since $x - y \in \mathbb{Z}$, the only possibility is $x = -y$. Thus, we must have $q = x^2(2q - s) + z^2(q^2 - s^2/4) = (q - s/2)(2x^2 + z^2(q + s/2))$. We now use the fact that $z \in \{0, \pm 1/2\}$ If $z = 0$, we get $q = x^2(2q - s)$ where $x \in \mathbb{Z}$ and so the only solution is $x = 1$ and $s = q$ since $q$ is square-free. However, looking at the discriminant of $\langle 1, \omega_1, \omega_2, \omega_1\omega_2 \rangle$ with Proposition 4, we get that $p$ must divide $q$ as it divides the discriminant of any maximal order in $B_{p,\infty}$. In that case, we have the solution $(x, y, z) = \pm(1, -1, 0)$.

Otherwise, wlog we can assume that $z = 1/2$ and $x = x'/2$ with $x' = 1 \mod 2$ and we obtain $q = (q - s/2)x'^2/2 + 1/4(q - s/2)(q + s/2)$ ( we recall that $s/2 = s' \in \mathbb{Z}$). It is clear that we must have $q \pm s' = 0 \mod 2$ so let us write $q \pm s' = 2q_{\pm}$. Thus, our equation becomes $q = q_- + q_+ = q_- x'^2 + q_+ q_-$ which implies that $q_+ = 0 \mod q_-$. Thus we must have $q_+ = kq_-$ for some $k \in \mathbb{Z}$ and are equation becomes $q = (k+1)q_- = q_-(x'^2 + kq_-)$ which can only be satisfied if $x' = 1$ and $q_- = 1$. In that case, the only possible solution (up to signs) is $(x, y, z) = (1/2, 1/2, 1/2)$ when $s = 2q - 4$.
In summary, we have showed that our equations have the non-trivial solutions $\pm(1, -1, 0)$ when $d = 0 \mod p$ and $s = q$ or $\pm(1/2, 1/2, \pm 1/2)$ when $d = 3 \mod 4$ and $s = 2q - 4$ and none otherwise. In the first situation, selecting the value $v$ to verify the trace equation we get that $\alpha_3 = \pm\mathrm{tr}(\alpha_1) + \alpha_1 - \alpha_2$. It is easily verified that $\mathrm{tr}(\alpha_1\alpha_2) = 4n(\alpha_1\alpha_2)$ when $s = q$. Otherwise, $\alpha_3 = v + x\alpha_1 + y\alpha_2 + z\alpha_1\alpha_2$ can only have a solution when $d = q = 3 \mod 4$ and $\mathrm{tr}(\alpha_1\alpha_2) = 1/2 + 1/4(\mathrm{tr}(\omega_1\omega_2)) = (d-1)/2$. By computing the discriminant of $\mathbb{Z}\langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2\rangle$ with Proposition 4 when $\mathrm{tr}(\alpha_1) = \mathrm{tr}(\alpha_2) = 1$ and $\mathrm{tr}(\alpha_1\alpha_2) = (q-1)/2$, we see that $\Delta = d - 1$ and so $p$ divides $d - 1$. This proves that $d = 1 \mod p$ is also a necessary condition for our equation to be satisfied. The possibilities for $\alpha_3$ can easily be found by taking $(x + z/2, y + z/2, z/2) = \pm(1/2, 1/2, \pm 1/2)$ and $v$ be such that $\mathrm{tr}(\alpha_3) = 1$.

**Corollary 3.** $K_E \geq \frac{N_E(N_E-1)}{12}$.

*Proof.* From $\alpha_l \notin \mathcal{O}_{i,j}$ or $\alpha_m \notin \mathcal{O}_{i,j} \Rightarrow (i,j) \not\sim_E (l,m)$ for any $i, j, m, l$, we see from Proposition 6 that the cardinal of any equivalence class in $I^2_{\neq}(N_E)$ must be smaller than 6 (choosing two among the three or four indices $i'$ such that $\alpha_{i'} \in \mathcal{O}_{i,j}$). This bound combined with $\#I^2_{\neq}(N_E) = N(N-1)/2$ gives the result directly.

The bound obtained in Corollary 3 is the key ingredient to the inequality between $\#\mathcal{E}_{\mathfrak{O}}(p)$, $h(\mathfrak{O})$ and $K_{\mathfrak{O}}(p)$ in Proposition 7.

**Proposition 7.** $K_{\mathfrak{O}}(p) \geq \frac{1}{12}\left(\frac{h(\mathfrak{O})^2}{\#\mathcal{E}_{\mathfrak{O}}(p)} - h(\mathfrak{O})\right)$

*Proof.* We have $h(\mathfrak{O}) = \#\mathcal{S}_{\mathfrak{O}}(p) = \sum_{E \in \mathcal{E}_{\mathfrak{O}}(p)} N_E$. Using Corollary 2 we get $\sum_{E \in \mathcal{E}_{\mathfrak{O}}(p)} K_E \geq (1/12) \sum_{E \in \mathcal{E}_{\mathfrak{O}}(p)} (N_E^2 - N_E)$. Then, we can use the classical inequality $\sum_{i=1}^n x_i^2 \geq (1/n)(\sum_{i=1}^n x_i)^2$ to get the result.

*A generic upper-bound of $K_{\mathfrak{O}}(p)$.* If $(i,j)$ is a representative of a class $k \in \mathcal{K}_E$, we define $t_k$ as the value of $\mathrm{tr}(\alpha_i\alpha_j)$ and $\mathcal{O}_k$ as the quaternion order equal to the image of $\langle 1, \alpha_i, \alpha_j, \alpha_i\alpha_j\rangle$ under the isomorphism between $B_{p,\infty}$ and $\mathrm{End}(E) \otimes \mathbb{Q}$ (by definition of $\mathcal{K}_E$, $t_k$ and $\mathcal{O}_k$ are independent of a choice of $i, j$). The idea is to look at the embedding number of the different orders $\mathcal{O}_k$ for $k \in \mathcal{K}_E$ and $E \in \mathcal{E}_{\mathfrak{O}}(p)$ in order to rewrite $\sum_{E \in \mathcal{E}_{\mathfrak{O}}(p)} K_E$. With the notation from Section 2.1, we write this number $e(\mathcal{O}_k)$ for a given class $k$ and we compute it in Proposition 8. Before proving this result, we need to understand a bit better the structure of the orders $\mathcal{O}_k$, this is the purpose of Lemma 1 below.

**Lemma 1.** *Let $E$ be a curve in $\mathcal{E}_{\mathfrak{O}}(p)$ and $k \in \mathcal{K}_E$. The order $\mathcal{O}_k$ is a Bass order.*

*Proof.* One of the several equivalent definitions of Bass orders inside $B_{p,\infty}$ is that they contain a maximal order inside a commutative subalgebra of $B_{p,\infty}$. Since $\mathfrak{O}$ is the maximal order of $\mathfrak{K}$ and so the property follows from the definition of $\mathcal{O}_k$.

With the knowledge that the $\mathcal{O}_k$ are Bass orders, we can use Proposition 1 and Proposition 2 to compute $e(\mathcal{O}_k)$.

**Proposition 8.** *Let $D_k = \mathrm{disc}(\mathcal{O}_k)/p$. The embedding number of $\mathcal{O}_k$ is*

$$e(\mathcal{O}_k) = \prod_{\ell \in \mathbb{P}_{D_k} \wedge (d/\ell)=1} (v_\ell(D_k)+1) \prod_{\ell \in \mathbb{P}_{D_k} \wedge (d/\ell)=0 \wedge \ell \neq p} 2.$$

*Proof.* If we show that when $\ell$ is a prime dividing $D_k$, $(\mathcal{O}/\ell) = (d/\ell)$, then the result follows from Proposition 2 and Lemma 1. First note, than when $\ell = p$, the local embedding number $e_\ell(\mathcal{O})$ is always equal to 1 (it is a consequence of Propositions 1 and 2 and the fact that $(d/p) \neq 1$). Then, it suffices to do it for the cases where $\ell \neq p$ is either split or ramified in $\mathfrak{K}$. The two results $(d/\ell) = 1 \Rightarrow (\mathcal{O}/\ell) = 1$ and $(\mathcal{O}/\ell) = 0 \Rightarrow (d/\ell) = 0$ are easily implied by Proposition 1. To conclude, it suffices to show $(\mathcal{O}/\ell) = 0 \Leftarrow (d/\ell) = 0$ as $(\mathcal{O}/\ell) = 1 \Rightarrow (d/\ell) \in \{0, 1\}$. Thus, we conclude our proof by showing that $(\mathcal{O}/\ell) = 0 \Leftarrow (d/\ell) = 0$. For that, we will show that $\ell$ divides the discriminant of every $\alpha \in \mathcal{O}_k$. We recall that there exists $\alpha_i, \alpha_j$ with $\mathfrak{O} \cong \mathbb{Z}[\alpha_i] \cong \mathbb{Z}[\alpha_j]$ and $\mathcal{O}_k = \langle 1, \alpha_i, \alpha_j, \alpha_i\alpha_j \rangle$. By assumption, the property is satisfied for $\alpha_i, \alpha_j$. We recall the value of $D_k = (d^2 - (\varepsilon - 2t_k)^2)/4p$ where $\varepsilon = \mathrm{tr}(\alpha_i)\mathrm{tr}(\alpha_j)$. It is easy to see from $\ell | D_k$ that $\ell$ must divide $2t_k - \varepsilon$ which implies that $\ell | \Delta(\alpha_i\alpha_j)$. Then, using $\ell | d$ and $\ell | (2t_k - \varepsilon)$, we can conclude that $\ell | \Delta(x + y\alpha_i + z\alpha_j + w\alpha_1\alpha_2)$ for any $x, y, z, w \in \mathbb{Z}^4$.

The value of $\mathrm{disc}(\mathcal{O}_k)$ is $(d^2 - (\mathrm{tr}(\alpha_i)\mathrm{tr}(\alpha_j) - 2t_k)^2)/4$ by Proposition 4. It can be shown that $\mathrm{tr}(\alpha_i)\mathrm{tr}(\alpha_j)$ is a constant that is either $0, 1$ depending only on the value of $d \mod 4$. Henceforth, we write this constant $\varepsilon_d$. Inspired by the formulation of Proposition 8, we define the functions

$$D : (t, d, p) \mapsto \frac{(d^2 - (\varepsilon_d - 2t)^2)}{4p}$$

and

$$e : (t, d, p) \mapsto \prod_{\ell \in \mathbb{P}_{D(t,d,p)} \wedge (d/\ell)=1} (v_\ell(D(t, d, p)) + 1) \prod_{\ell \in \mathbb{P}_{D(t,d,p)} \wedge (d/\ell)=0} 2.$$

Let us define $T_{\mathfrak{O}}(p) = \{t_k | t_k \in \mathcal{K}_E \text{ for } E \in \mathcal{E}_{\mathfrak{O}}(p)\}$. For each $t \in T_{\mathfrak{O}}(p)$, the values $D(t, d, p)$ and $e(t, d, p)$ are well-defined, when $p$ is prime and $d$ is a fundamental discriminant coprime with $p$.

**Proposition 9.** *Let $\mathfrak{O}$ be the maximal quadratic order of discriminant $-d$.*

$$\sum_{t \in T_{\mathfrak{O}}(p)} e(t,d,p) = K_{\mathfrak{O}}(p).$$

*Proof.* Let us take an element $t \in T_{\mathfrak{O}}(p)$. We are going to show that there are exactly $e(t,d,p)$ distinct pairs $(E,k)$ where $k \in \mathcal{K}_E$ and $t_k = t$. By definition of $T_{\mathfrak{O}}(p)$, there exists a curve $E \in \mathcal{E}_{\mathfrak{O}}(p)$ and a class $k \in K_E$ with $t_k = t$. By definition of the embedding number, there exist $e(t,d,p)$ distinct maximal orders containing $\mathcal{O}_k$. Each of these maximal orders $\mathcal{O}'$ corresponds to some isomorphism class up to Galois conjugacy of supersingular curve $E'$ under the Deuring Correspondence. By definition there also exists a class $k' \in \mathcal{K}_{E'}$ such that $\mathcal{O}_{k'} \cong \mathcal{O}_k$. We will show that every such class is distinct. Up to composition with the relevant isomorphisms, we can assume that all such orders $\mathcal{O}_{k'}$ are actually equal (and not simply isomorphic). Let us take $\mathcal{O}^1 \neq \mathcal{O}^2$, maximal orders with $\mathcal{O}_k \subset \mathcal{O}^i$ for $i = 1, 2$ and assume that these two embeddings of $\mathcal{O}_k$ lead to the same class $k'$ and curve $E'$. We must have $\mathcal{O}^1 \cong \mathcal{O}^2 \cong \mathrm{End}(E)'$, so let us write $\sigma_i : \mathcal{O}^i \to \mathrm{End}(E)$ the isomorphisms. By definition of our equivalence relation, we must have $\sigma_1(\mathcal{O}_k) = \sigma_2(\mathcal{O}_k)$, which means that $\mathcal{O}_k$ is stable under the isomorphism $\sigma_1^{-1} \circ \sigma_2 : \mathcal{O}^2 \to \mathcal{O}^1$. When $\mathcal{O}_k$ is a full quaternion order of rank 4 this is not possible unless $\sigma_1^{-1} \circ \sigma_2$ is the identity, which is impossible since $\mathcal{O}^1 \neq \mathcal{O}^2$. Thus, there cannot be collisions and there are exactly $e(t,d,p)$ distinct classes $k$ with $t_k = t$.

Then, since, for every class $k$, there exists $t \in T_{\mathfrak{O}}(p)$ with $t = t_k$ and $e(\mathcal{O}_k) = e(t,d,p)$, we get the equality $\sum_{t \in T_{\mathfrak{O}}(p)} e(t,d,p) = K_{\mathfrak{O}}(p)$.

With Proposition 9, we have all the necessary ingredients to prove our generic upper-bound of $K_{\mathfrak{O}}(p)$. We introduce in Definition 2, a final notation to simplify the formulation of Proposition 10.

**Definition 2.** *The function $\tau : \mathbb{N} \to \mathbb{N}$ is defined as $N \mapsto \prod_{\ell \in \mathbb{P}_N} (v_\ell(N) + 1)$.*

**Proposition 10.** $K_{\mathfrak{O}}(p) \leq \left\lceil \frac{d+1}{4p} \right\rceil \max_{0 \leq N \leq d^2/(4p)} \tau(N)$.

*Proof.* It is clear from the definition of the functions $\tau, D, e$ that $\tau(D(d,t,p)) \geq e(d,t,p)$. Since $0 \leq D(t,d,p) \leq (d^2)/4p$ we get that

$$\sum_{t \in T_{\mathfrak{O}}(p)} e(t,d,p) \leq \#T_{\mathfrak{O}}(p) \max_{0 \leq N \leq d^2/(4p)} \tau(N).$$

Next, we prove that $\#T_{\mathfrak{O}} \leq \lceil (d+1)/4p \rceil$. If $t \in T_{\mathfrak{O}}$, we must have that $D(d,t,p) = \mathrm{disc}(\mathcal{O}_k)/p \in \mathbb{N}^\star$ for some class $k$. Note that the two values $t_k, -t_k$ lead to the same order $\mathcal{O}_k$ so we can assume $t_k \geq 0$. The condition on the discriminant yields $d^2 - (\varepsilon_d - 2t)^2 = 0 \mod 4p$ and $d^2 > (\varepsilon_d - 2t)^2$. When $t > 0$, we have $2t - \varepsilon_d > 0$ and so get the bound $(-d + \varepsilon_d)/2 > t$. There are two possible values of $t \mod 4p$ and combining that with the $0 < t < (-d + \varepsilon_d)/2$ we obtain at most $\lfloor (d+1)/(4p) \rfloor$ possible values. Adding $t = 0$, we obtain the desired bound. The proof is concluded by Proposition 9.

We obtain a generic lower bound on $\#\mathcal{E}_{\mathfrak{O}}(p)$ in Proposition 11. It is a combination of Proposition 7 and Proposition 10.

**Proposition 11.** *$\#\mathcal{E}_{\mathfrak{O}}(p) \geq \lambda h(\mathfrak{O})$ or $\#\mathcal{E}_{\mathfrak{O}}(p) > \frac{(1-\lambda)h(\mathfrak{O})^2}{3(4p+d+1)} \frac{p}{\max\limits_{0\leq N\leq d^2/4p} \tau(N)}$ for any $\lambda \in [0,1]$*

*Proof.* Note that when $\#\mathcal{E}_{\mathfrak{O}}(p) < \lambda h(\mathfrak{O})$ for some $\lambda \leq 1$, we must have $K_{\mathfrak{O}}(p) > 0$ because there is at least one curve with two distinct orientations. Thus, Proposition 7 proves that

$$\#\mathcal{E}_{\mathfrak{O}}(p) \geq \frac{h(\mathfrak{O})^2 - h(\mathfrak{O})\#\mathcal{E}_{\mathfrak{O}}(p)}{12K_{\mathfrak{O}}(p)}.$$

For any $\lambda \in [0,1]$, if $\#\mathcal{E}_{\mathfrak{O}}(p) < \lambda h(\mathfrak{O})$, we have that

$$\#\mathcal{E}_{\mathfrak{O}}(p) > (1-\lambda)\frac{h(\mathfrak{O})^2}{12K_{\mathfrak{O}}(p)}.$$

The proof is concluded by Proposition 10 and $\lceil (d+1)/4p \rceil \leq 1 + (d+1)/4p$.

*Remark 3.* Of course, $\#\mathcal{E}_{\mathfrak{O}}(p)$ cannot be bigger than $N_p \approx p/12$. One way of seeing that the bound we obtained in Proposition 11 is not incoherent is to see that under the approximation $h(\mathfrak{O}) \sim \sqrt{\mathrm{disc}(\mathfrak{O})}$ (see Section 5 for a more precise esimate), it is clear that $\frac{h(\mathfrak{O})^2}{3(4p+d+1)} \frac{p}{\max\limits_{0\leq N\leq d^2/4p} \tau(N)}$ is smaller than $N_p$.

*Remark 4.* Our bound becomes less and less accurate when the size of $d$ grows in comparison to $p$. Asymptotically, we have

$$\lim_{d\to\infty} \frac{h(\mathfrak{O})^2}{3(4p+d+1)} \frac{p}{\max\limits_{0\leq N\leq d^2/4p} \tau(N)} = 0$$

which is very far from the expected $\mathcal{E}_{\mathfrak{O}}(p) = N_p$ when $d \to \infty$. However, when the value of $d$ is polynomial in $p$, our analysis of the $\tau$ function in Section 4 shows that our bound will never be trivial even as $p$ grows to infinity (see Proposition 17). This is typically the case needed for isogeny-based cryptography as illustrated by our numerical application in Section 5 for a prime $p \approx 2^{400}$ and a discriminant $d$ satisfying $p < d < p^2$.

*Remark 5.* When $p$ divides $d$, it might be possible to get better bounds. For instance, when $d/p$ is a prime smaller than $p/4$, a lower bound was proven in [EHL+20, Theorem 3.9], using the fact that a curve in $\mathcal{E}_{\mathfrak{O}}(p)$ must be $d/p$-isogenous to its galois conjugate $E^p$. Another possibility, is to exploit the fact that when $d = 0 \mod p$, the element $\omega_1\omega_2/p$ is integral (see the proof of Proposition 6 for the definition of $\omega_1, \omega_2$) and so we may be able to consider superorders of the $\mathcal{O}_k$ (which might give a better bound since the discriminants are smaller). While this idea seems promising, it does not appear trivial to obtain the analog of Proposition 6 and this is why we left the study of this special case open for future work.

### 3.3 The case of non-maximal orders

In this section, we provide an upper-bound on $\#\mathcal{E}_{\mathfrak{O}}(p)$ when $\mathfrak{O}$ is not maximal. Most of the ideas exposed below are not fundamentally new, but we expose them here for completeness since we are not aware of any concrete statement in the literature.

For the rest of this section, let us take $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_0$ where $f > 1$ is coprime with $p$ and $\mathfrak{O}_0$ is a maximal quadratic order. The fundamental property underlying our result in Proposition 14 is summarized in Proposition 12. This is a consequence of [LB20, Lemma 5.4, Corollary 5.5] showed by Love and Boneh (they talk about optimal embeddings inside maximal orders rather than orientations of elliptic curves in their papers but the two notions are the same under the Deuring Correspondence) and the standard characterization of *horizontal, ascending and descending* isogenies (see [CK19] for instance).

**Proposition 12.** *Let $\mathfrak{O}$ be a quadratic order of conductor $f$ and discriminant $d$ such that $\mathcal{E}_{\mathfrak{O}}(p)$ is not empty. Let $\ell \neq p$ be a prime number. For every curve $E \in \mathcal{E}_{\mathfrak{O}}(p)$, among the $\ell + 1$ curves $\ell$-isogenous to $E$, there are $\ell - (d/\ell)$ curves contained in $\mathcal{E}_{\mathbb{Z}+\ell\mathfrak{O}}$. If $\ell$ is coprime with $f$, the $1 + (d/\ell)$ remaining curves are in $\mathcal{E}_{\mathfrak{O}}(p)$ and if not, then the final curve is contained in $\mathcal{E}_{\mathfrak{O}'}(p)$ where $\mathfrak{O}'$ is the quadratic order of discriminant $d/\ell^2$ such that $\mathfrak{O} = \mathbb{Z} + \ell\mathfrak{O}'$.*

Note that by $\ell$-isogenous we mean connected by a *cyclic* $\ell$-isogeny. From Proposition 12, we see that we can tie the generic case to the fundamental discriminant one using the expanding properties of the isogeny graphs. For simplicity, we assume henceforth that $f = \ell^e$ for some prime $\ell$ and $e \in \mathbb{N}$ and $\mathfrak{O}_0$ is any maximal quadratic order. By Proposition 12, each coprime factor of the conductor can be treated independently . The exact bound in Proposition 14 depends on whether $\ell$ is split, ramified or inert in $\mathfrak{K}$ but the three cases can be treated in a similar manner. As a warm-up, we start with Proposition 13, to give a lower bound on the number of curves that are $f$-isogenous to a curve in an arbitrary set $\mathcal{E}_0$.

For any prime $\ell$ coprime with $p$, the graph of cyclic $\ell$-isogenies is Ramanujan with degree of regularity equal to $\ell + 1$. For $\ell^e$-isogenies, we obtain an almost-Ramanujan graph with with degree of regularity equal to $\lambda_1(\ell^e) = \ell^e(1+1/\ell)$. We write $A(\ell^e)$ for the adjacency matrix of this graph. The matrices $A(\ell^r)$ for $r \in \mathbb{N}$ are related to the Brandt matrices $B(\ell^r)$ for $r \in \mathbb{N}$ under the relation $A(\ell^r) = B(\ell^r) - B(\ell^{r-2})$ and $B(\ell) = A(\ell)$ and $B(1) = A(1) = I$. The Brandt matrices $B(m)$ correspond to the action of the Hecke operator $T_m$ on the space of modular form of weight 2 on $\Gamma_0(N)$ when $m$ and $N$ are coprime. The graph associated to the $B(\ell^r)$ are $\sum_{i=0}^{r} \ell^i$-regular. The matrices $A(\ell^r)$ and $B(\ell^r)$ are real symmetric positive and have $N_p$ ordered real eigenvalues. The biggest eigenvalue is always equal to the degree of regularity $k$ of the associated graph and the corresponding eigenspace is generated by the vector $(1/\sqrt{N_p})_{1 \leq i \leq N_p}$ of norm 1. The expansion of the graph can be measured by the size of the second eigenvalue. The graph is said to *Ramanujan* when this value is smaller than $2\sqrt{k-1}$. A consequence of the Riemann hypothesis for function fields, proven by Deligne (see [Kat76]

for instance)is that the second eigen vector of $B(\ell^r)$ is smaller than $(r+1)\sqrt{\ell^r}$. When $r=1$, this proves that the graph of $\ell$-isogenies is Ramanujan. For $r>1$, the bound is not good enough to prove the same thing. This is why the other graphs are to be almost-Ramanujan. We will use $A(\ell^r) = B(\ell^r) - B(\ell^{r-2})$ to deduce results on the expansion of the graph of $\ell^e$ isogenies.

**Proposition 13.** *Let $e \in \mathbb{N}$ and $\ell \in \mathbb{P}$ different from $p$ and $\mathcal{E}_0$ be a set of isomorphism classes of supersingular elliptic curve. Let us write $C_0 = \#\mathcal{E}_0$ and $\mathcal{E}_{\ell^e}$ for the set of isomorphism classes of curve $\ell^e$-isogenous to a curve of $\mathcal{E}_0$. We have the bound*

$$\#\mathcal{E}_{\ell^e} \geq \frac{N_P}{1+(N_P/C_0-1)\frac{(e+1)^2\ell^e+(e-1)^2\ell^{e-2})}{\lambda_1(\ell^e)^2}}$$

*Proof.* Assume that we have an ordering $E_1, \dots, E_{N_p}$ of all supersingular elliptic curves (up to isomorphism). Let us write $X = (x_i)_{1\leq i\leq N_p} \in \mathbb{R}^{N_p}$, the vector such that $x_i = 1$ if $E_i \in \mathcal{E}_0$ and 0 otherwise. If we write $Y = A(\ell^e)X$, then $\#\mathcal{E}_{\ell^e}$ is equal to the number of non-zero coefficient of $Y$. A very classical bound tells us that

$$\#\mathcal{E}_{\ell^e} \geq \frac{\|Y\|_1^2}{\|Y\|_2^2}.$$

We see easily that $\|Y\|_1 = \lambda_1(\ell^e)C_0$. To upper-bound $\|Y\|_2^2$, we are going to use the Ramanujan property. Let us write $f_1, \dots, f_{N_p}$ the orthonormal basis of eigenvectors of $A(\ell^e)$. We already explained that $f_1 = (1/\sqrt{N_p})_{1\leq i\leq N_p}$. We can write $X = z_1 f_1 + X'$ where $X'$ is orthogonal to $f_1$. The coefficient $z_1$ is equal to $\langle X, f_1\rangle = C_0/\sqrt{N_p}$. We have $\|A(\ell^e)X\|_2^2 = \lambda_1(\ell^e)^2 z_1^2 + \|A(\ell^e)X'\|^2$. We have the equality $A(\ell^e) = B(\ell^e) - B(\ell^{e-2})$. The vector $X'$ lies in a space of dimension $N_p - 1$ where all the eigenvalues of $B(\ell^r)$ have absolute value smaller than $(r+1)\sqrt{\ell^r}$ for every $r \geq 1$. We have $\|A(\ell^e)X'\|_2^2 \leq \|B(\ell^e)X'\|_2^2 + \|B(\ell^{e-2})X'\|_2^2$ by the triangular inequality. Thus, $\|A(\ell^e)X\|_2^2 \leq \lambda_1(f)^2 z_1^2 + ((e+1)^2\ell^e + (e-1)^2\ell^{e-2})\|X'\|_2^2$. We can easily compute that $\|X'\|_2^2 = \|X\|_2^2 - z_1^2$. Thus we obtain $\|Y\|_2^2 \leq \lambda_1(\ell^e)^2 C_0^2/N_p + ((e+1)^2\ell^e + (e-1)^2\ell^{e-2})(C_0 - C_0^2/N_p)$. Thus, we obtain

$$\#\mathcal{E}_{\ell^e} \geq \frac{\lambda_1(\ell^e)^2 C_0^2}{\frac{\lambda_1(\ell^e)^2 C_0^2}{N_p} + ((e+1)^2\ell^e + (e-1)^2\ell^{e-2})(C_0 - C_0^2/N_p)}$$

$$\#\mathcal{E}_{\ell^e} \geq \frac{N_P}{1+(N_P/C_0-1)\frac{(e+1)^2\ell^e+(e-1)^2\ell^{e-2}}{\lambda_1(\ell^e)^2}}.$$

**Proposition 14.** *Let $\mathfrak{O} = \mathbb{Z} + \ell^e\mathfrak{O}_0$ for some $\ell \in \mathbb{N}$ coprime with $p$ and a maximal quadratic order $\mathfrak{O}_0$. Let us write $C_0 = \#\mathcal{E}_{\mathfrak{O}_0}$.*
*If $\ell$ is inert in $\mathfrak{K}$:*

$$\#\mathcal{E}_{\mathfrak{O}}(p) \geq \frac{N_P}{1+(N_P/C_0-1)\frac{(e+1)^2\ell^e+(e-1)^2\ell^{e-2}}{(\ell^e+\ell^{e-1})^2}},$$

*else if $\ell$ is ramified:*

$$\#\mathcal{E}_{\mathfrak{O}}(p) \geq \frac{N_P}{1+(N_P/C_0-1)\frac{((e+1)^2\ell^e+e^2\ell^{e-1})}{\ell^{2e}}},$$

*else, $\ell$ is split and:*

$$\#\mathcal{E}_{\mathfrak{O}}(p) \geq \frac{N_P}{1+(N_P/C_0-1)\frac{\sum_{j=0}^{e}(2^{\lfloor (1+j)/2\rfloor}-2^{\lfloor (1+j-2)/2\rfloor})^2(e-j+1)^2\ell^{e-j+1}}{(\ell^e-\ell^{e-1})^2}}.$$

*Proof.* The case $\ell$ inert is a simple combination of Proposition 12 and Proposition 13 since the set $\mathcal{E}_{\mathbb{Z}+\ell\mathfrak{O}}(p)$ is exactly the set of curves $\ell$-isogenous to curves in $\mathcal{E}_{\mathfrak{O}}(p)$. When $\ell$ is ramified or split, the situation is slightly more complicated. In fact, in both cases, the result is obtained by rewriting the reasoning used in the proof of Proposition 13. Indeed, we are going to show that $\#\mathcal{E}_{\mathbb{Z}+\ell^e\mathfrak{O}_0}$ is equal to the number of non-zero coefficient of a vector $Y$ computed as $MX$ where $X$ is defined as in the proof of Proposition 13 and $M$ is a liner combination of the $A(\ell^i)$ for $i \in [0,e]$. For Proposition 13 (and $\ell$ inert) we can simply take $M = A(\ell^e)$. When $\ell$ is not inert, we need to remove some of the $\ell^e$ isogenies and this is why we have a more complicated expression for $M$.
For what remains, let us assume that the labelling of the $N_P$-isomorphism classes of supersingular curves is such that $E_1, \dots, E_{C_0}$ are the $C_0$ curves contained in $E \in \mathcal{E}_{\mathfrak{O}_0}(p)$. $X_i$ is the vector of $\mathbb{N}^{N_p}$ such that $(X_i)_j = 1$ if $j = i$ and 0 otherwise and $X = \sum_{i=1}^{C_0} X_i$.
When $\ell$ is ramified, Proposition 12 implies that there exists a permutation $\sigma$ of $[1, C_0]$ such that $E_i$ and $E_{\sigma(i)}$ are $\ell$-isogenous and $\sigma^2$ is the identity. To get the curves of $\mathcal{E}_{\mathfrak{O}}(p)$, we need to exclude all the $\ell^e$-isogenies that can be written as $\phi \circ \varphi_i$ where $\varphi_i$ is the $\ell$-isogeny between $E_i$ and $E_{\sigma(i)}$. $A(\ell^e)X_i$ gives all the curves that are $\ell^e$-isogenous to $E_i$. To remove the ones that are obtained through the wrong isogenies we can subtract by $A(\ell^{e-1})X_{\sigma(i)}$ but with that we have also subtracted the curves that are $\ell^{e-2}$-isogenous to $E_i$. So we need to compensate by adding $A(\ell^{e-2})X_i$ and iterating this reasoning, we end up with the $\sum_{j=0}^{e}(-1)^j A(\ell^{e-j})X_{\sigma^j(i)}$. Thus, we get $M = \sum_{j=0}^{e}(-1)^j A(\ell^{e-j})$ after summing this formula for all $i \in [1, C_0]$. The lower bound on the number of zeroes of $Y = MX$ is given by $\|Y\|_1^2/\|Y\|_2^2$. A simple counting gives that $\|Y\|_1^2 = (\sum_{j=0}^{e}(-1)^j\lambda_1(\ell^{e_i}))^2 = \ell^{2e}$. To lower bound $\|Y\|_2^2$, we see that $M$ has the same eigenvector $f_1$ (see the notations of the proof of Proposition 13) for the eigenvalue $\ell^{2e}$. Thus, we can decompose $X = z_1 f_1 + X'$ with $z_1 = C_0/\sqrt{N_p}$. Once again we replay each $A(\ell^r)$ by $B(\ell^r) - B(\ell^{r-2})$ and $B(\ell) = A(\ell)$ and $B(1) = A(1)$. Interestingly, a lot of terms cancel out in $M$ and we end with $B(\ell^e) - B(\ell^{e-1})$. As in the proof of Proposition 13, we conclude with the bound on the eigenvalues of the $B(\ell^r)$ and the triangular inequality. This is how we get $\|MX'\|_2^2 \leq ((e+1)^2\ell^e + e^2\ell^{e-1})\|X'\|_2^2$. The proof is concluded in a similar way to Proposition 13.
When $\ell$ is split, we have by Proposition 12 that there exists two permutations $\sigma_l, \sigma_r$ such that $E_i$ is $\ell$-isogenous to $E_{\sigma_l(i)}$ and $E_{\sigma_r(i)}$ and $\sigma_l \circ \sigma_r = \sigma_r \circ \sigma_l$ is the

identity. A similar reasoning proves that we can take

$$M = \sum_{j=0}^{e} (-1)^j 2^{\lfloor (1+j)/2 \rfloor} A(\ell^{e-j}).$$

Once again, we use our relation between $A$ and $B$ matrices to get a sum on the $B(\ell^{e-j})$. We have $\ell^e(1-1/\ell) = \sum_{j=0}^{e}(-1)^j 2^{\lfloor (1+j)/2 \rfloor}\lambda_1(\ell^{e-j})$ and the final result follows from the same ideas as before.

## 4 Analysis of the $\tau$ function and proof of a conjecture on the size of $\tau(N)$

In this section we analyze the $\tau$ function introduced in Definition 2 and its maximum over a large interval in order to get an efficient way to use the bound in Proposition 11 concretely. Interestingly enough, the study of this function was already part of [EHL+20]. It was shown in this paper that when $v_\ell(N) \leq 1$ for all primes $\ell$, we have $\tau(N) = O(N^\epsilon)$ for any $\epsilon > 0$. It was conjectured by Eisentrager et al. [EHL+20, Conjecture 5.6] that the same was true for any $N$ but not proven. We prove this conjecture below.

We start our analysis by considering a restricted version of the problem where the number of primes $\ell$ with $v_\ell(N) \neq 0$ is fixed.

*A reformulation of the problem with a fixed number of factors.* With Proposition 15, we try to answer the following question: Given an integer $k$, a bound $C$ and an increasing sequence $L_1, L_2, \ldots, L_k$, what it the maximum of $\prod_{i=1}^k x_i$ when $\sum_{i=1}^k (x_i - 1)L_i \leq C$ and $x_i \geq 0$ for all $x_i$? We write $\Sigma_k = \sum_{i=1}^k L_i$ and $\Pi_k = \prod_{i=1}^k L_i$.

**Proposition 15.** *Let us take $C \geq 0$, a sequence $(L_i)_{i\in\mathbb{N}}$ of positive numbers and $k \in \mathbb{N}^*$. If $\sum_{i=1}^k x_i L_i \leq C$ then $\prod_{i=1}^k x_i \leq C^k/k^k\Pi_k$.*

*Proof.* The bound is obviously true for $k = 1$. Now we show that the bound for a given $k$ implies it for $k+1$. We have $\sum_{i=1}^{k+1} x_i L_i \leq C$ which implies $\sum_{i=1}^k x_i L_i \leq (C - x_{k+1}L_{k+1})$. Since $x_{k+1}L_{k+1} \leq C$, we can apply the bound for $k$ to obtain $\prod_{i=1}^k \leq (C - x_{k+1}L_{k+1})^k/k^k\Pi_k$ and so we have $\prod_{i=1}^{k+1} \leq (C - x_{k+1}L_{k+1})^k x_{k+1}/k^k\Pi_k$. In the interval $[0, C/L_{k+1}]$, it is easy to see that the polynomial $P_{k+1}(x_{k+1})(C - x_{k+1}L_{k+1})^k x_{k+1}$ has exactly one maximum which is obtained at the unique root of $P'_{k+1}(x_{k+1}) = (C - x_{k+1}L_{k+1})^{k-1}(C - (k+1)L_{k+1}x_{k+1})$. The root is at $x_{k+1} = C/(k+1)L_{k+1}$ and the maximum of $P_{k+1}$ is $C^{k+1}k^k/L_{k+1}(k+1)^{k+1}$. Thus we obtain the desired bound $\prod_{i=1}^{k+1} x_i \leq C^{k+1}(k+1)^{k+1}\Pi_{k+1}$.

Next, we are going to relate Proposition 15 to our situation. The idea is to apply the bound for the $x_i = v_{\ell_i}(N)+1$ where the $\ell_i$ are primes and $L_i = \log(\ell_i)$ and $C = \log N - \sum_{i=1}^k L_i$.

For Proposition 16, we take $\ell_i$ to be the $i$-th smallest prime number $L_i = \log \ell_i$. We keep the same definition for $\Sigma_k$ and $\Pi_k$ as for Proposition 15. For any $N \in \mathbb{N}^*$, we define $\Psi(N)$ as the maximum number of distinct prime factors dividing a number smaller than $N$.

**Proposition 16.** $\tau(N) \leq \max_{1 \leq k \leq \Psi(N)} \frac{(\log(N)+\Sigma_k)^k}{k^k \Pi_k}$.

*Proof.* Let us take $N$ any integer. There exists an integer $1 \leq k \leq \Psi(N)$ such that $N$ has $k$ distinct prime factors. Let us label these primes $\ell_1(N), \ldots, \ell_k(N)$ and take

$$N' = \prod_{i=1}^{n} \ell_i^{v_{\ell_i(N)}(N)}.$$

We have $N' \leq N$ and $\tau(N) = \tau(N')$. With $x_i = v_{\ell_i}(N')+1$ and $C = \log(N)+\Sigma_k$ we have that $\sum_{i=1}^{k} x_i L_i = \log(N)' + \Sigma_k \leq \log(N) + \Sigma_k$ and applying Proposition 15 we obtain

$$\tau(N) = \tau(N') \leq \frac{(\log(N) + \Sigma_k)^k}{k^k \Pi_k}.$$

To prove the conjecture that $\tau(N)$ is negligible compared to $N$, we are going to use the bound from Proposition 16 with some bound on $\Psi(N)$. It is a classical result that $\Psi(N) = O(\log(N)/\log\log(N))$ (see [HW+79, Chapter 22] for instance).

**Proposition 17.** *For any* $\epsilon > 0$, $\tau(N) = O(N^\epsilon)$.

*Proof.* To prove our result we don't actually need a bound as tight as the one provided by Proposition 16. In particular, the sum and product $\Sigma_k, \Pi_k$ are a bit hard to estimate so we remove them with $\Sigma_k \leq \log N$ and $\Pi_k \geq 1$. Hence we get that

$$\tau(N) \leq \max_{1 \leq k \leq \Psi(N)} (\frac{2\log(N)}{k})^k.$$

We are going to prove that the max is reached for $k = \Psi(N)$ when $N$ is big enough. By the result on $\Psi(N)$, we know there exists a constant $c > 0$ such that $\Psi(N) \leq c\log(N)/\log\log(N)$.

The function $(\alpha/x)^x$ admits the derivative function $(\ln(\alpha/x)-1)(\alpha/x)^x$ which is positive over $]0, \alpha/e[$. Thus, $(\alpha/x)^x$ is increasing on this interval and this implies that when $N$ is big enough so that $c\log(N)/\log\log(N) \leq 2\log(N)/e$, the following inequalities hold

$$\max_{1 \leq k \leq \Psi(N)} (\frac{2\log(N)}{k})^k \leq (\frac{2\log(N)}{\Psi(N)})^{\Psi(N)} \leq (\frac{2\log\log(N)}{c})^{c\frac{\log(N)}{\log\log(N)}}.$$

Thus, we have proven that

$$\tau(N) \leq (N)^{\frac{c\log((2/c)\log\log(N))}{\log\log(N)}}$$

which is asymptotically dominated by $N^\epsilon$ for any $\epsilon > 0$.

## 5 A numerical application to the parameters of SETA

In this section, we are going to use Proposition 11 to provide a lower bound on the complexity of the brute-force algorithm to solve the $\mathfrak{O}$-UBER problem where $\mathfrak{O}$ is the quadratic order used in the SETA encryption scheme. This will give a lower bound on the hardness of SETA key recovery (using brute-force) and answer the interrogations left open in [DFFdSG+21, Section 5.3] on the concrete hardness of the uber isogeny problem. More precisely, with our new result, we are able to prove, under a few reasonable assumptions, that there exists a fitting choice of quadratic order $\mathfrak{O}$ such that the best brute force key recovery attack is hard enough for the claimed security level in [DFFdSG+21].

*The SETA parameters.* The set of SETA keys is $\mathcal{E}_{\mathfrak{O}}(p)$ where $\mathfrak{O} = \mathbb{Z}[\sqrt{-n}]$ where $n$ is a solution of the quadratic equation $z^2 + nD^2 = N^2$ with $-n$ being a non-quadratic residue modulo all the prime divisors of $D$ and $p$, where $D, N$ and $p$ are the three main parameters of SETA.

The authors from the SETA paper [DFFdSG+21] provided an implementation of their protocol with given values for $p, D, N$. The characteristic $p$ is a 400 bits primes equal to $2 \cdot 8426067021^{12} - 1$, and the two other parameters are:

$$\begin{aligned} D &= 43^{12} \cdot 84719^{11}, \\ N &= 3^{21} \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 73 \cdot 257^{12} \cdot 313 \cdot 1009 \cdot 2857 \cdot 3733 \cdot 5519 \cdot 6961 \\ &\quad \cdot 53113 \cdot 499957 \cdot 763369 \cdot 2101657 \cdot 2616791 \cdot 7045009 \cdot 11959093 \\ &\quad \cdot 17499277 \cdot 20157451 \cdot 33475999 \cdot 39617833 \cdot 45932333. \end{aligned}$$

The concrete value of $n$ was not given in [DFFdSG+21] but several solutions can be found quite easily. Below, we computed one such solution where $n$ is easy to factor so that we could compute the conductor. For instance, we found the value:

$$\begin{aligned} n = 113 \cdot 337 \cdot 43913 \cdot 69522129914593554713466657355275000660185257908972492522431413808553767205401453148081325894556965991428307754649539266\\ 033342875068026023370667830770225304 57. \end{aligned}$$

Since, $n$ is square free and equal to $1 \mod 4$, the order $\mathfrak{O} = \mathbb{Z}[\sqrt{-n}]$ is the ring of integers of $\mathfrak{K} = \mathbb{Q}(\sqrt{-n})$. Under GRH, Littlewood [Lit28] proved the inequality

$$h(\mathfrak{O}) > (\frac{\pi}{12e^{\gamma}} + o(1))\frac{\sqrt{4n}}{\log\log(4n)}$$

where $\gamma$ is the Euler-Mascheroni constant with $e^{\gamma}/\pi \approx 0.56693$. To derive the concrete lower-bound in Corollary 4 from Proposition 11, we will use the simplifying Lemma 2, the classical lower bound on $h(\mathfrak{O})$ stated above and our upper-bound in Proposition 16 on the size of $\tau$.

**Lemma 2.** *For every 3 values $x, A, B > 0$ such that $x \geq \lambda A$ or $x \geq (1-\lambda)B$ for every $0 < \lambda < 1$. Then, $x \geq \frac{1}{2}\min(A, B)$.*

*Proof.* We are going to start with the intermediary result that $x \geq \lambda A$ or $x \geq (1-\lambda)B$ for every $0 < \lambda < 1$ imply that $x \geq \min_{0<\lambda<1} \max(\lambda A, (1-\lambda)B)$. The function $\lambda \mapsto \max(\lambda A, (1-\lambda)B)$ is decreasing on $]0, \lambda_m]$ and increasing on $[\lambda_m, 1[$ for the value $\lambda_m$ such that $\lambda_m A = (1-\lambda_m)B$. Thus, $\min_{0<\lambda<1} \max(\lambda A, (1-\lambda)B) = A\lambda_m$. If we assume that $x < \lambda_m A$, then it exists $\lambda_0 < \lambda_m$ such that $x < \lambda_0 A$. By our hypothesis we get that $x \geq (1-\lambda_0)B > (1-\lambda_m)B$ and this is a contradiction. To conclude it suffices to see that

$$\min_{0<\lambda<1} \max(\lambda A, (1-\lambda)B) \geq \frac{1}{2}\min(A, B).$$

**Corollary 4.** *Let the values $p, n$ be as above and $\mathfrak{O} = \mathbb{Z}[\sqrt{n}]$. Assuming GRH, the size of $\mathcal{E}_{\mathfrak{O}}(p)$ is bigger than $2^{269}$.*

*Proof.* Proposition 11 and Lemma 2 tells us that $\#\mathcal{E}_{\mathfrak{O}}(p)$ is bigger than $(1/2)\min(A, B)$ where:

$$A = h(\mathfrak{O}) \text{ and } B = \frac{h(\mathfrak{O})^2}{3(4p+4n+1)} \frac{p}{\max\limits_{0 \leq N \leq 4n^2/p} \tau(N)}.$$

Assuming that our $n$ is big enough for it to hold, we are going to use $A = h(\mathfrak{O}) > \frac{\pi}{24e^{\gamma}} \frac{\sqrt{4n}}{\log\log(4n)} > 2^{270}$. To get a lower bound on $B$, it remains to get an upper bound on $\max_{0 \leq N \leq 4n^2/p} \tau(N)$. We can compute this bound manually using Proposition 16. Indeed, it can be easily verified that $\Psi(4n^2/p) = 98$ and so we can simply compute

$$\frac{(\log(4n^2/p) + \Sigma_k)^k}{k^k \Pi_k} \text{ for all } 1 \leq k \leq 98.$$

As expected, the maximum is obtained for $k = 98$ and we have that

$$\max_{0 \leq N \leq 4n^2/p} \tau(N) < 2^{105}.$$

Thus, using the bound on $h(\mathfrak{O})$, we get that $B > 2^{279}$. So, under GRH and the assumption that $n$ is big enough so that our simplification of the Littlewood bound hold, we get that

$$\#\mathcal{E}_{\mathbb{Z}[\sqrt{-n}]}(p) > 2^{269}.$$

## 6 Conclusion and open problems.

We have given a new generic lower bound on the size of $\mathcal{E}_{\mathfrak{O}}(p)$ and proved that our bound was useful in practice applying it in a concrete example taken from isogeny-based cryptography. While our bound seems satisfying for the example we took, its behavior is a bit counter-intuitive as it tends to 0 when the discriminant of $\mathfrak{O}$ tends to infinity and $p$ is fixed. It is an interesting question to see if this asymptotic behavior is intrinsic to our method or if we could derive a better bound. We have also observed that studying the case where $p$ divides

the discriminant of $\mathfrak{O}$ could lead to interesting improvements. Finally, it could be interesting to see if we could adapt our analysis to the case of embeddings of quadratic ordres of distinct discriminants inside the same quaternion order and see how the resulting bound would compare with the results from the Singular moduli litterature (the ones from [LV15] for instance).

## References


ADFMP20. Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 411–439. Springer, 2020.

BE92. Jacek Brzezinski and M Eichler. On the imbeddings of imaginary quadratic orders in definite quaternion orders. 1992.

BKV19. Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. Csi-fish: Efficient isogeny based signatures through class group computations. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 227–247. Springer, 2019.

Brz83. Juliusz Brzezinski. On orders in quaternion algebras. *Communications in algebra*, 11(5):501–522, 1983.

CK19. Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Number-Theoretic Methods in Cryptology 2019*, 2019.

CLG09. Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, Jan 2009.

CLM+18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 395–427. Springer, 2018.

Cou06. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

CS21. Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 2021.

CSV21. Sara Chari, Daniel Smertnig, and John Voight. On basic and bass quaternion orders. *Proceedings of the American Mathematical Society, Series B*, 8(2):11–26, 2021.

Deu41. Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14(1):197–272, Dec 1941.

DFFdSG+21. Luca De Feo, Tako Boris Fouotsa, Cyprien Delpech de Saint Guilhem, Péter Kutas, Antonin Leroux, Christophe Petit, Javier Silva, and Benjamin Wesolowski. Séta: Supersingular encryption from torsion attacks. In *ASIACRYPT*, 2021.

Dor87. David R Dorman. Global orders in definite quaternion algebras as endomorphism rings for reduced cm elliptic curves. *Théorie des nombres (Quebec, PQ, 1987)*, pages 108–116, 1987.

EHL+20. Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. *Open Book Series*, 4(1):215–232, 2020.

Eic36. Martin Eichler. Untersuchungen in der zahlentheorie der rationalen quaternionenalgebren. 1936.

HW+79. Godfrey Harold Hardy, Edward Maitland Wright, et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

IK21. Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53. American Mathematical Soc., 2021.

JDF11. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

Kan89. Masanobu Kaneko. Supersingular $j$-invariants as singular moduli mod $p$. 1989.

Kat76. N Katz. An overview of deligne's proof of the riemann hypothesis for varieties over finite fields. *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 275–305, 1976.

LB20. Jonathan Love and Dan Boneh. Supersingular curves with small non-integer endomorphisms. *Open Book Series*, 4(1):7–22, 2020.

Lit28. John E Littlewood. On the class-number of the corpus p ( $\sqrt{-k}$). *Proceedings of the London Mathematical Society*, 2(1):358–372, 1928.

LV15. Kristin Lauter and Bianca Viray. On singular moduli for arbitrary discriminants. *International Mathematics Research Notices*, 2015(19):9206–9250, 2015.

Onu21. Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields and Their Applications*, 69:101777, 2021.

QKL+21. Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E Stange. Improved torsion-point attacks on sidh variants. In *Annual International Cryptology Conference*, pages 432–470. Springer, 2021.

RS06. Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006.

Voi21. John Voight. *Quaternion algebras*. Springer Nature, 2021.

Wes21. Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. Cryptology ePrint Archive, Report 2021/1583, 2021. https://ia.cr/2021/1583.

ZG85. Don Zagier and B. Gross. On singular moduli. *Journal Fur Die Reine Und Angewandte Mathematik - J REINE ANGEW MATH*, 1985:191–220, 01 1985.