ON SINGULAR MODULI FOR ARBITRARY DISCRIMINANTS

KRISTIN LAUTER AND BIANCA VIRAY

ABSTRACT. Let d_1 and d_2 be discriminants of distinct quadratic imaginary orders $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$ and let $J(d_1, d_2)$ denote the product of differences of CM j-invariants with discriminants d_1 and d_2. In 1985, Gross and Zagier gave an elegant formula for the factorization of the integer $J(d_1, d_2)$ in the case that d_1 and d_2 are relatively prime and discriminants of *maximal* orders. To compute this formula, they first reduce the problem to counting the number of simultaneous embeddings of $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$ into endomorphism rings of supersingular curves, and then solve this counting problem.

Interestingly, this counting problem also appears when computing class polynomials for invariants of genus 2 curves. However, in this application, one must consider orders $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$ that are *non*-maximal. Motivated by the application to genus 2 curves, we generalize the methods of Gross and Zagier and give a computable formula for $v_\ell(J(d_1, d_2))$ for any pair of discriminants $d_1 \neq d_2$ and any prime $\ell > 2$. In the case that d_1 is squarefree and d_2 is the discriminant of any quadratic imaginary order, our formula can be stated in a simple closed form. We also give a conjectural closed formula when the conductors of d_1 and d_2 are relatively prime.

1. INTRODUCTION

Let d_1 and d_2 be discriminants of distinct quadratic imaginary orders and write

$$J(d_1, d_2) := \prod_{\substack{[\tau_1],[\tau_2] \\ \text{disc } \tau_i = d_i}} (j(\tau_1) - j(\tau_2)),$$

where $[\tau_i]$ runs over all elements of the upper half-plane with discriminant d_i modulo $\mathrm{SL}_2(\mathbb{Z})$. In 1985, under the assumption that d_1 and d_2 are relatively prime and discriminants of *maximal* orders, Gross and Zagier showed that $J(d_1, d_2)^{\frac{8}{w_1 w_2}}$ is an integer and gave an elegant formula for its factorization.

Theorem. [GZ85, Thm. 1.3] *Let d_1 and d_2 be two relatively prime fundamental discriminants of imaginary quadratic fields. For any prime p dividing a positive integer of the form $d_1 d_2 - x^2$, choose i such that $p \nmid d_i$ and define $\epsilon(p) = \left(\frac{d_i}{p}\right)$, and extend the definition of ϵ by multiplicativity. Then*

$$J(d_1, d_2)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{x \in \mathbb{Z}, |x| < d_1 d_2 \\ x \equiv d_1 d_2 \bmod 2}} F\left(\frac{d_1 d_2 - x^2}{4}\right),$$

where $F(m) = \prod\limits_{n|m,n>0} n^{\epsilon(m/n)}$ and w_i denotes the number of roots of unity in the quadratic imaginary order of discriminant d_i.

Although it is not obvious from the definition, $F(m)$ is a non-negative power of a single prime. More precisely, $F(m)$ is a non-trivial power of ℓ if ℓ is the unique prime such that $v_\ell(m)$ is odd and $\epsilon(\ell) = -1$, and $F(m) = 1$ otherwise. This fact gives a particularly nice corollary, which can be thought of as saying that $J(d_1, d_2)$ is "highly factorizable."

Corollary. [GZ85, Cor. 1.6] *Let d_1 and d_2 be two relatively prime fundamental discriminants. Assume that ℓ divides $J(d_1, d_2)$. Then $\left(\frac{d_1}{\ell}\right), \left(\frac{d_2}{\ell}\right) \neq 1$ and ℓ divides a positive integer of the form $\frac{d_1 d_2 - x^2}{4}$.*

A factorization formula for $J(d_1, d_2)$, *without* assumptions on d_1 and d_2, would have important applications to the computation of minimal polynomials of Igusa invariants of CM abelian surfaces. In contrast to the case of genus 1 curves, these minimal polynomials do not have integer coefficients, and the denominators of the coefficients cause difficulty in the computation of these polynomials. As explained in [LV], the computation of the denominators can be reduced to counting the number of pairs of elements of a given norm and trace in certain maximal orders in a quaternion algebra. As becomes apparent in the proof in [GZ85], this counting problem is essentially equivalent to a factorization formula of $J(d_1, d_2)$, where d_1 and d_2 are the discriminants of the elements in question.

The discriminants that arise in the study of Igusa invariants are *not* necessarily relatively prime or fundamental. In particular, the results and techniques of Gross and Zagier do not suffice for the computation of the aforementioned denominators. This motivates the focus of this paper, which is to determine to what extent a factorization formula for $J(d_1, d_2)$ holds for *arbitrary* discriminants.

Before stating our main results, we must first discuss which aspects of [GZ85, Thm. 1.3] we hope to preserve. We note that the proof of [GZ85, Thm. 1.3] implicitly gives a mathematical interpretation of the quantities $F(m)$. Their interpretation is quite natural, and any nice generalization of [GZ85, Thm. 1.3] to arbitrary discriminants should retain this property. (This will be explained in more detail in §2.)

We prove that there is a generalization of $F(m)$ such that the expression for $J(d_1, d_2)$ in the Theorem above holds, and that retains this mathematical interpretation and many other nice properties of the original definition:

Theorem 1.1. *Let d_1, d_2 be any two distinct discriminants. Then there exists a function F that takes non-negative integers of the form $\frac{d_1 d_2 - x^2}{4}$ to (possibly fractional) prime powers. This function satisfies*

$$J(d_1, d_2)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{x^2 \leq d_1 d_2 \\ x^2 \equiv d_1 d_2 \bmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right). \tag{1.1}$$

Moreover, $F(m) = 1$ unless either (1) $m = 0$ and $d_2 = d_1 \ell^{2k}$ for some prime ℓ or (2) the Hilbert symbol $(d_1, -m)_\ell = -1$ at a unique finite prime ℓ and this prime divides m. In both of these cases $F(m)$ is a (possibly fractional) power of ℓ.

Remark 1.2. In most cases, $F(m)$ is actually an integer prime power. In particular, it is an integer prime power if m is coprime to the conductor of d_1 and at least one of d_1 or d_2 is odd. We explain this more in Theorem 1.5. However, fractional powers do appear. For instance, if $d_1 = -3$ and $d_2 = -12$, then $F(0) = 2^{1/3}$.

Theorem 1.1 easily implies a generalization of [GZ85, Cor 1.6] for *all* pairs of discriminants.

Corollary 1.3. *Let d_1 and d_2 be any two distinct discriminants. Assume that ℓ divides $J(d_1, d_2)$. Then either $d_2 = d_1\ell^{2k}$ for some k, or ℓ divides a positive integer m of the form $\frac{d_1 d_2 - x^2}{4}$ and the Hilbert symbol $(d_1, -m)_p = (d_2, -m)_p$ is nontrivial if and only if $p = \ell$. In particular, if $d_2 \neq d_1\ell^{2k}$ then $\left(\frac{d_1}{\ell}\right), \left(\frac{d_2}{\ell}\right) \neq 1$.*

Remark 1.4. The assumption that $d_2 \neq d_1\ell^{2k}$ is, in fact, necessary to conclude that $\left(\frac{d_1}{\ell}\right), \left(\frac{d_2}{\ell}\right) \neq 1$. For example, 11 divides $J(-7, -7 \cdot 11^2)$ even though 11 is split in $\mathbb{Q}(\sqrt{-7})$.

From the proof of Theorem 1.1, we can show that there is *no* extension of the definition of the quadratic character ϵ such that $F(m) = \prod_n n^{\epsilon(m/n)}$ for an arbitrary pair of discriminants (see §2, Example 2.3). We will instead generalize a different expression of $F(m)$ from [GZ85, Dor88]. If $-d_1$ is prime, d_2 is fundamental, and $\gcd(d_1, d_2) = 1$, then Gross and Zagier show that $v_\ell(F(m))$ can be expressed as a weighted sum of the number of integral ideals in $\mathcal{O}_{d_1}$ of norm m/ℓ^r for $r > 0$. Dorman extended this work to the case that d_1 is squarefree, d_2 is fundamental, and $\gcd(d_1, d_2) = 1$. We derive an expression for $v_\ell(F(m))$ which holds for *arbitrary* d_1 and d_2 and for primes $\ell > 2$ which are coprime to the conductor of d_1.

Theorem 1.5. *Let d_1 and d_2 be any two distinct discriminants, and let m be a non-negative integer of the form $\frac{d_1 d_2 - x^2}{4}$ and ℓ a fixed prime that is coprime to $\operatorname{cond}(d_1)$.*
If $m > 0$ and either $\ell > 2$ or 2 does not ramify in both $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, then $v_\ell(F(m))$ can be expressed as a weighted sum of the number of certain invertible integral ideals in $\mathcal{O}_{d_1}$ of norm m/ℓ^r for $r > 0$.
Moreover, if m is coprime to the conductor of d_1, then $v_\ell(F(m))$ is an integer and the weights are easily computed and constant; more precisely we have

$$v_\ell(F(m)) = \begin{cases} \frac{1}{e}\rho(m)\sum_{r\geq 1}\mathfrak{A}(m/\ell^r) & \text{if } \ell \nmid \operatorname{cond}(d_2), \\ \rho(m)\mathfrak{A}(m/\ell^{1+v(\operatorname{cond}(d_2))}) & \text{if } \ell | \operatorname{cond}(d_2), \end{cases} \tag{1.2}$$

where e is the ramification degree of ℓ in $\mathbb{Q}(\sqrt{d_1})$ and

$$\rho(m) = \begin{cases} 0 & \text{if } (d_1, -m)_p = -1 \text{ for } p|d_1, p \nmid f_1\ell, \\ 2^{\#\{p|(m,d_1):p\nmid f_2 \text{ or } p=\ell\}} & \text{otherwise,} \end{cases}$$

$$\mathfrak{A}(N) = \#\left\{ \mathfrak{b} \subseteq \mathcal{O}_{d_1} : \begin{array}{l} N(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible,} \\ p \nmid \mathfrak{b} \text{ for all } p|(N, f_2), p \nmid \ell d_1 \\ \mathfrak{p}^3 \nmid \mathfrak{b} \text{ for all } \mathfrak{p}|p|(N, f_2, d_1), p \neq \ell \end{array} \right\}.$$

If $m = 0$, then either $v_\ell(F(0)) = 0$ or $d_2 = d_1\ell^{2k}$ and

$$v_\ell(F(0)) = \frac{2}{w_1} \cdot \#\operatorname{Pic}(\mathcal{O}_{d_1}).$$

3

Under the same assumptions as in Theorem 1.5, formula (1.2) has an equivalent formulation as a product of local factors, see Proposition 7.12 in §7.

Theorems 1.1 and 1.5 combine to give a formula for $v_\ell(J(d_1, d_2))$ for any pair of discriminants $d_1 \neq d_2$ and any prime $\ell > 2$. Under certain conditions this formula simplifies further:

Corollary 1.6. *Let ℓ be a prime and let d_1, d_2 be any two distinct discriminants. Assume that either d_1 is squarefree or $\ell > 2$ and for all $x \equiv d_1 d_2 \bmod 2$ with $x^2 < d_1 d_2$, we have either*

$$\gcd\left(\operatorname{cond}(d_1), \frac{d_1 d_2 - x^2}{4}\right) = 1, \quad or \quad \left(d_1, \frac{x^2 - d_1 d_2}{4}\right)_p = -1 \text{ for some } p \neq \ell.$$

Then we have

$$v_\ell(J(d_1, d_2)^{\frac{8}{w_1 w_2}}) = H + \sum_{\substack{x^2 < d_1 d_2 \\ x^2 \equiv d_1 d_2 \bmod 4}} \begin{cases} \frac{1}{e}\rho(m_x)\sum_{r \geq 1}\mathfrak{A}(m_x/\ell^r) & \text{if } \ell \nmid \operatorname{cond}(d_2), \\ \rho(m_x)\mathfrak{A}(m_x/\ell^{1+v(\operatorname{cond}(d_2))}) & \text{if } \ell \mid \operatorname{cond}(d_2), \end{cases} \quad (1.3)$$

where $m_x := \frac{d_1 d_2 - x^2}{4}$ and $H = 0$ unless $d_2 = d_1 \ell^{2k}$ for some $k > 0$, in which case $H = \frac{2}{w_1} \cdot \# \operatorname{Pic}(\mathcal{O}_{d_1})$.

We conjecture that Theorem 1.5 holds even in the case that $\ell = 2$ ramifies in both $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$. However, the existence of multiple quadratic ramified extensions of $\mathbb{Q}_2^{\mathrm{unr}}$ causes difficulty in one of the steps of the proof, namely the proof of Proposition 8.1. It may be possible to get around this difficulty in our approach by a long and detailed case-by-case analysis. We did not undertake this analysis, and it would be interesting to determine a better method.

More generally, the local factor description of (1.2) that is given in §7 suggests a conjecture for any pairs of discriminants whose conductors are relatively prime.

Conjecture 1.7. *Let d_1 and d_2 be two distinct discriminants with relatively prime conductors. Write f for the product of the two conductors and for any prime p, let $d_{(p)} \in \{d_1, d_2\}$ be such that $p \nmid \operatorname{cond}(d_{(p)})$. Then, for any prime ℓ*

$$v_\ell(J(d_1, d_2)^2) = H + \sum_{\substack{x^2 < d_1 d_2 \\ x^2 \equiv d_1 d_2 \bmod 4}} \epsilon_\ell(x) \prod_{p \mid m_x, p \neq \ell} \begin{cases} 1 + v_p(m) & \left(\frac{d_{(p)}}{p}\right) = 1, p \nmid f, \\ 2 & \left(\frac{d_{(p)}}{p}\right) = 1, p \mid f, \text{ or} \\ & p \mid d_{(p)}, (d_{(p)}, -m)_p = 1, p \nmid f \\ 1 & \left(\frac{d_{(p)}}{p}\right) = -1, p \nmid f, v_p(m) \text{ even or} \\ & p \mid d_{(p)}, (d_{(p)}, -m)_p = 1, p \mid f, v_p(m) = 2 \\ 0 & \text{otherwise,} \end{cases}$$

where H, m_x are as above and

$$\epsilon_\ell(x) = \begin{cases} v_\ell(m_x) & \text{if } \ell \nmid f, \ell \mid d_\ell \\ \frac{1}{2}(v_\ell(m_x) + 1), & \text{if } \ell \nmid f d_{(p)}, v_\ell(m) \text{ odd,} \\ 0 & \text{if } \ell \nmid d_{(p)}, v_\ell(m) \text{ even,} \\ 1 & \text{otherwise.} \end{cases}$$

4

We verified this conjecture with `Magma` for all pairs of discriminants with relatively prime conductors and $|d_i| < 250$.

1.1. **Related previous work.** In 1989, Kaneko[Kan89] generalized part of [GZ85, Cor. 1.6] to arbitrary discriminants. More precisely, he proved that if d_1 and d_2 are arbitrary discriminants and ℓ is a prime dividing $J(d_1, d_2)$, then ℓ divides a positive integer of the form $\frac{1}{4}(d_1 d_2 - x^2)$. However, Kaneko did not obtain the stronger statement given in Corollary 1.3.

To the best of our knowledge, the only previous generalization of Theorem [GZ85, Thm. 1.3], conjectural or otherwise, was given in 1998 by Hutchinson. Hutchinson put forth conjectural extensions of the Gross-Zagier formula [Hut98] in the case that the gcd of d_1 and d_2 is supported at a single prime p that does not divide either conductor. While his formulations are very different from ours, we checked that the two formulas agree in many cases.

One of the contributions of the present paper is a generalization of Dorman's theory of maximal orders in a quaternion algebra with an optimal embedding of a maximal imaginary quadratic order [Dor89]. We generalize this theory to include imaginary quadratic orders which are *not* maximal. The first author, together with Goren, generalized Dorman's work in a different direction, to higher-dimensional abelian varieties, by giving a description of certain orders in a quaternion algebra over a totally real field, with an optimal embedding of the maximal order of a CM number field [GL13]. Since that work does not apply to optimal embeddings of non-maximal orders, it is neither weaker nor stronger than the generalization we give in this paper.

1.2. **Applications.** The results and techniques from Gross and Zagier's paper have had a number of applications over the years. For instance, [GZ85, Cor. 1.6] gives simple conditions which ensure that certain values of the j function are relatively prime to all sufficiently large primes. This has been used to bound the number of rational points on certain modular curves [Par05, Thm. 6.2] and to determine which twist of an elliptic curve to use for the CM method [RS10, pp.554-555]. In a different direction, the techniques of the paper have applications to CM liftings of supersingular elliptic curves. More precisely, work of Elkies [Elk89] combined with [GZ85] shows that liftings of supersingular elliptic curves over $\overline{\mathbb{F}}_\ell$ to elliptic curves with CM by a maximal order $\mathcal{O}$ are in bijection with embeddings of $\mathcal{O}$ into maximal orders of $\mathbb{B}_{\ell,\infty}$, the quaternion algebra ramified at ℓ and ∞. Furthermore, the work of Gross and Zagier together with work of Dorman [Dor89] gives a count for the number of such embeddings.

We expect the results in this paper to lead to similar applications. Indeed, Corollary 1.3 has already been used in work of Dose, Green, Griffin, Mao, Rolen, and Willis to study integrality properties of values at CM points of a certain non-holomorphic modular function [DGG+].

In a different direction, as mentioned above, new applications in arithmetic intersection theory are given by the present authors in [LV], where the results on counting embeddings of non-maximal orders presented here in Sections 6 and 7 are used to give formulas for the denominators of Igusa class polynomials. We note that in both of these examples the results and techniques of Gross and Zagier and Dorman are not sufficient; results on non-fundamental discriminants and pairs of discriminants with a common factor are needed.

1.3. **Outline.** We prove Theorem 1.1 in §2. The rest of the paper will focus on the proof of Theorem 1.5. In §3.1, we give a high-level overview of the whole proof and explain the

differences between the general case and the cases treated in [GZ85, Dor88]. In §3.2 we explain how various propositions and theorems come together to prove Theorem 1.5, and point the reader to the individual sections where each proposition or theorem is proved.

1.4. **Notation.** Throughout, ℓ will denote a fixed prime. By discriminant we mean a discriminant of a quadratic imaginary order. We say a discriminant is fundamental at a prime p if the associated quadratic imaginary order is maximal at p, and we say a discriminant is fundamental if it is fundamental at all primes p.

For a discriminant d, we write f for the conductor of d, and let $\widetilde{d}$ denote $d\ell^{-2v_\ell(f)}$. Note that $\widetilde{d}$ is fundamental at ℓ. For most of the paper, we will concern ourselves with two fixed distinct discriminants d_1, d_2; in this case, the above quantities will be denoted f_1, f_2 and $\widetilde{d}_1, \widetilde{d}_2$ respectively. We write $s_i := v_\ell(f_i)$.

We denote quadratic imaginary orders by $\mathcal{O}$ and write $\mathcal{O}_d$ for the quadratic imaginary order of discriminant d. We set $w_d := \#\mathcal{O}_d^\times$ and $\widetilde{w}_d := \#\mathcal{O}_{\widetilde{d}}^\times$. The notation w_i, $\widetilde{w}_i$ will refer to the special case $d = d_i$. If ℓ is ramified in $\mathcal{O}$, then $\mathfrak{l}$ will denote the unique prime ideal in $\mathcal{O}$ lying above ℓ. We write $\mathfrak{D}$ for the principal ideal generated by $\sqrt{d}$. In §5, we will give background on quadratic imaginary orders, and fix some more notation there.

Let H_d denote the ring class field of $\mathcal{O}_d$, and let $\widetilde{H}_{d_i} := H_{\widetilde{d}_i}$. Let μ_i denote a prime of $\mathcal{O}_{H_{d_i}}$ lying over ℓ. When $\ell \nmid f_1$, we let $\mathbb{W}$ denote $\mathcal{O}_{H_{d_1},\mu_1}$ and let π denote a uniformizer of $\mathbb{W}$.

ACKNOWLEDGEMENTS

2. PROOF OF THEOREM 1.1

By [ST68, §§5,6], there exists a number field K such that, for every prime q and every $[\tau]$ of fixed discriminant d, there exists an elliptic curve $E/\mathcal{O}_K$ with good reduction at all $\mathfrak{q}|q$ such that $j(E) = j(\tau)$. More specifically, we may take K to be the ring class field of $\mathcal{O}_d$, unless $d = -3p^{2k}$ or $-4p^{2k}$ for some prime p and positive integer k. In that case, we may assume that K is a finite extension of the ring class field of $\mathcal{O}_d$ ramified at p.

For each i, let L_i be the ring class field of $\mathcal{O}_{d_i}$, if $d_i \neq -3p^{2k}, -4p^{2k}$ for some prime p. If $d_i = -3p^{2k}$ or $-4p^{2k}$, let L_i be the minimal (finite) Galois extension of the ring class field of $\mathcal{O}_{d_i}$ such that the above properties hold. Let L be the compositum of L_1 and L_2 and let $\mathcal{O}_L$ be the ring of integers. Then, by the discussion above, for every $[\tau_i]$ of discriminant d_i and every prime q, there exists an elliptic curve $E/\mathcal{O}_L$ with good reduction at all $\mathfrak{q}|q$ such that $j(E) = j(\tau_i)$; we call let $E(\tau_i)$ denote such an elliptic curve.

Fix a rational prime ℓ and a prime μ of $\mathcal{O}_L$ lying over ℓ. Let A be the ring of integers of L_μ^{unr}. Then, by [GZ85, Prop 2.3], we have

$$v_\mu(j(\tau_1) - j(\tau_2)) = \frac{1}{2}\sum_n \#\operatorname{Isom}_{A/\mu^n}(E(\tau_1), E(\tau_2))$$

6

for all $[\tau_i]$ of discriminant d_i. Write E_i for $E(\tau_i)$. Since τ_i is an algebraic number of discriminant d_i, we have an isomorphism $\mathcal{O}_{d_i} \cong \mathrm{End}(E_i)$, and an embedding

$$\mathcal{O}_{d_i} \cong \mathrm{End}(E_i) \hookrightarrow \mathrm{End}_{A/\mu}(E_i).$$

For any $g \in \mathrm{Isom}_{A/\mu}(E_1, E_2)$ we obtain an isomorphism $\mathrm{End}_{A/\mu}(E_2) \cong \mathrm{End}_{A/\mu}(E_1)$ by conjugating by g. Thus we have an embedding (that depends on the choice of g) of $\mathcal{O}_{d_2} \hookrightarrow \mathrm{End}_{A/\mu}(E_1)$.

Definition 2.1. *Let $\iota\colon \mathcal{O} \hookrightarrow R$ be a map of $\mathbb{Z}$-modules. We say this map is **optimal at** p if*

$$(\iota(\mathcal{O}) \otimes \mathbb{Q}_p) \cap R = \iota(\mathcal{O}),$$

where the intersection takes place inside of $R \otimes \mathbb{Q}_p$

Proposition 2.2. *Let E be an elliptic curve over A that has good reduction and that has CM by an order $\mathcal{O}$. Write $\overline{E}_0$ for the reduction of E. Then the embedding*

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(\overline{E}_0)$$

is optimal at all primes $p \neq \ell$. It is optimal at ℓ if and only if $\mathcal{O}$ is maximal at ℓ.

Proof. If E has ordinary reduction, then this is a well-known result, see, for example [Lan87, §13, Thm. 12]. Assume that E has supersingular reduction. We write $\overline{E}_n$ for E mod μ^{n+1} and let $\phi \in \mathrm{End}(\overline{E}_0)$ be the image of a generator of $\mathcal{O}$. By [Vig80, Chap. II, Lemma 1.5] there is a unique maximal order in $\mathrm{End}(\overline{E}_0) \otimes \mathbb{Q}_\ell$ which consists of all integral elements. Therefore, the order $(\mathrm{End}(E) \otimes \mathbb{Q}) \cap \mathrm{End}(\overline{E}_0)$ must be maximal at ℓ, and so the embedding $\mathrm{End}(E) \hookrightarrow \mathrm{End}(\overline{E}_0)$ is optimal at ℓ if and only if $\mathrm{End}(E) = \mathcal{O}$ is maximal at ℓ.

By the Grothendieck existence theorem [Con04, Thm 3.4], we have that

$$\mathrm{End}(E) \to \varprojlim \mathrm{End}(\overline{E}_n)$$

is a bijection. So to complete the proof, it suffices to show that any element of $\mathrm{End}(E) \cap \mathbb{Q}(\phi)$ lifts to an element of $\mathrm{End}(\overline{E}_n) \otimes \mathbb{Z}[1/\ell]$ for all $n \geq 0$. Let $\psi \in \mathrm{End}(\overline{E}_0) \cap \mathbb{Q}(\phi)$. We may write $\psi := \frac{1}{f\ell^k}(a + b\phi)$ for some $a, b, f \in \mathbb{Z}$, $k \in \mathbb{Z}_{\geq 0}$, where $\ell \nmid f$. Since $\phi \in \mathrm{im}(\mathrm{End}(E) \to \mathrm{End}(\overline{E}_0))$, both ϕ and $a + b\phi$ are endomorphisms of $\overline{E}_n$, and of Γ_n, the ℓ-divisible group of E_n. The endomorphism ring $\mathrm{End}(\Gamma_n)$ is a $\mathbb{Z}_\ell$-module, so $\ell^k \psi = \frac{1}{f}(a + b\phi)$ is in $\mathrm{End}(\Gamma_n)$. Thus, by Serre-Tate [Con04, Thm 3.3], $\psi \in \mathrm{End}(\overline{E}_n) \otimes \mathbb{Z}[1/\ell]$. This completes the proof. $\square$

This proposition shows that $\ell | J(d_1, d_2)$ only if there exists a τ_1 such that there is an optimal embedding $\mathcal{O}_{\widetilde{d_2}} \hookrightarrow \mathrm{End}_{A/\mu}(E(\tau_1))$. Given such an optimal embedding, we can consider the sub-order R of $\mathrm{End}_{A/\mu}(E_1)$ that is generated by the images of $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$. A calculation shows that the discriminant of R is $\left(\frac{d_1 d_2 - x^2}{4}\right)^2$ for some $x \in \mathbb{Z}$ with $x^2 \leq d_1 d_2$ and $d_1 d_2 \equiv x^2 \bmod 4$.

For any non-negative integer m of the form $\frac{d_1 d_2 - x^2}{4}$, we define $F(m)$ to be the unique ideal in $\mathcal{O}_L$ such that for all rational primes ℓ and all primes $\mu | \ell$ in $\mathcal{O}_L$

$$v_\mu(F(m)) = \frac{4}{C w_1 w_2} \sum_{\substack{[\tau_i] \\ \mathrm{disc}(\tau_i) = d_i}} \sum_{n \geq 1} \# \left\{ f \in \mathrm{Isom}_{A/\mu^n}(E(\tau_1), E(\tau_2)) : \mathrm{disc}(R) = m^2 \right\},$$

where R is the suborder of $\text{End}_{A/\mu}(E(\tau_1))$ described above and $C = 1$ if $4m = d_1 d_2$ and $C = 2$ otherwise. (The presence of this C scalar is to agree with the convention set in [GZ85]. Since Gross and Zagier take the product over x-values, for every $m \neq d_1 d_2/4$ the value $F(m)$ appears twice in the product, once from x and once from $-x$.) From this definition and the previous discussion it is clear that

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x^2 \leq d_1 d_2 \\ x^2 \equiv d_1 d_2 \bmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right).$$

In addition, the condition defining $F(m)$ is Galois invariant, so $v_\mu(F(m)) = v_{\mu'}(F(m))$ for any μ, μ' lying over the same prime ℓ.

Assume that $F(m)$ is non-trivial. So there exists a prime ℓ and an elliptic curve $\overline{E}/\overline{\mathbb{F}}_\ell$ with embeddings $\iota_i \colon \mathcal{O}_{d_i} \hookrightarrow \text{End}(E)$ such that the images of ι_1 and ι_2 generate an order R of discriminant m^2. The endomorphism ring $\text{End}(\overline{E})$ is either an order in a quadratic imaginary field, or a maximal order in the quaternion algebra $\mathbb{B}_{\ell,\infty}$ ramified only at ℓ and ∞ [Lan87, Chap. 13 §2]. Since a maximal order in a quaternion algebra has no suborders of rank 3, if $m = 0$, then R must be a rank 2 $\mathbb{Z}$-module. Since $\mathcal{O}_{\widetilde{d}_i}$ is optimally embedded in $\text{End}_{A/\mu}(E(\tau_1))$ this implies that $\widetilde{d}_1 = \widetilde{d}_2$, i.e. that $d_2 = d_1 \ell^{2k}$ for some $k \in \mathbb{Z}_{\neq 0}$.

Now consider the case when m is nonzero. Then R is rank 4, and thus $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is $\mathbb{B}_{\ell,\infty}$, the quaternion algebra ramified only at ℓ and ∞. A straightforward calculation, which does not depend on ℓ, shows that

$$R \otimes_{\mathbb{Z}} \mathbb{Q} \cong \frac{\mathbb{Q}\langle i, j \rangle}{i^2 = d_1, j^2 = -m, ij = -ji} \cong \frac{\mathbb{Q}\langle i, j \rangle}{i^2 = d_2, j^2 = -m, ij = -ji}.$$

Since this quaternion algebra is ramified only at ℓ and ∞, this implies that the Hilbert symbol $(d_1, -m)_p = (d_2, -m)_p = 1$ if and only if $p \neq \ell$. In addition, ℓ divides the reduced discriminant of any order in $\mathbb{B}_{\ell,\infty}$, so $\ell | m$. Since $F(m)$ is a Galois invariant fixed ideal supported only at primes lying over ℓ, we may consider $F(m)$ to be just a fractional power of ℓ. This completes the proof of Theorem 1.1. □

Example 2.3. Assume that there is a quadratic character ϵ that is defined on every prime p that divides a positive integer of the form $\frac{1}{4}(d_1 d_2 - x^2)$. In addition, we assume that if $p \nmid \gcd(d_1, d_2)$ and if $p \nmid f_1 f_2$, then $\epsilon(p)$ agrees with the definition in [GZ85, Thm. 1.3], and that

$$F(m) = \prod_{n | m, n > 0} n^{\epsilon(m/n)}, \quad \text{where } m = \frac{d_1 d_2 - x^2}{4}. \tag{2.1}$$

Consider the following example. Let $d_1 = -3 \cdot 7 \cdot 11$ and $d_2 = 5d_1$. We will study the cases where $x^2 = 33^2$ and 99^2, i.e. when $m = 3^2 11^2 61$, and $3^2 11^2 59$ respectively. Equation (2.1) shows that

$$v_3(F(3^2 11^2 61)) = v_3(F(3^2 11^2 59)) = (4 + 2\epsilon(3))(1 + \epsilon(11) + \epsilon(11)^2),$$
$$v_{11}(F(3^2 11^2 61)) = v_{11}(F(3^2 11^2 59)) = (4 + 2\epsilon(11))(1 + \epsilon(3) + \epsilon(3)^2),$$
$$v_{61}(F(3^2 11^2 61)) = v_{59}(F(3^2 11^2 59)) = (1 + \epsilon(3) + \epsilon(3)^2)(1 + \epsilon(11) + \epsilon(11)^2).$$

On the other hand, we can also calculate $F(m)$ using the results in the proof of Theorem 1.1. Theorem 1.1 implies that $F(3^2 11^2 61)$ is supported only at 3 and that $F(3^2 11^2 59)$ is

supported only at 11. Moreover, the proof gives a method of determining whether $F(m)$ is a *nontrivial* power of 3, or 11 respectively, and the calculation shows that this is indeed the case. But the above expressions show that either 3 divides both $F(3^2 11^2 61)$ and $F(3^2 11^2 59)$, or it divides neither, which gives a contradiction.

3. Overview of proof of Theorem 1.5

Henceforth, we fix a non-negative integer m of the form $\frac{d_1 d_2 - x^2}{4}$ and a prime ℓ, and we assume that $\ell \nmid f_1$. We retain the notation fixed in §2. Recall from §2, that

$$v_\ell(F(m)) = e(\mu/\ell)^{-1} \frac{4}{C w_1 w_2} \sum_{\substack{[\tau_i] \\ \mathrm{disc}(\tau_i) = d_i}} \sum_{n \geq 1} \# \left\{ f \in \mathrm{Isom}_{A/\mu^n}(E(\tau_1), E(\tau_2)) : \mathrm{disc}(R) = m^2 \right\}.$$

3.1. **High-level strategy.** As discussed in §2, an element of $f \in \mathrm{Isom}_{A/\mu^n}$ gives rise to an embedding of $\mathcal{O}_{d_2} \hookrightarrow \mathrm{End}_{A/\mu^n}(E(\tau_1))$ that is optimal away from ℓ. We first show that the problem of counting elements in $\cup_{\tau_2} \mathrm{Isom}_{A/\mu^n}(E(\tau_1), E(\tau_2))$ is equivalent to counting elements in $\mathrm{End}_{A/\mu^n}(E(\tau_1))$ that have a fixed degree and trace and have a fixed action on the Lie algebra. To compute these elements we give detailed constructions of the endomorphism rings $\mathrm{End}_{A/\mu^n}(E(\tau_1))$, and show that the endomorphisms of a fixed degree and trace are in a finite-to-1 correspondence with ideals in $\mathcal{O}_{d_1}$ of a certain norm. We then classify how many of these endomorphisms have the desired action on the Lie algebra.

This high-level strategy is the same as that employed by Gross and Zagier in the case that $-d_1$ is prime, d_2 is fundamental, and $\gcd(d_1, d_2) = 1$, and, soon after, by Dorman in the case that d_1 is squarefree, d_2 is fundamental, and $\gcd(d_1, d_2) = 1$. However, the general case presents significantly more technical difficulties, which is perhaps not surprising, as it has been over 20 years since Gross-Zagier and Dorman published their papers.

First, the straightforward generalizations of the constructions of the endomorphism rings $\mathrm{End}_{A/\mu^n}(E(\tau_1))$ given in [GZ85, Dor89] to the case where $d_1 \equiv 0 \pmod 4$ and μ a prime of characteristic 2 completely fail, *even if d_1 is fundamental*. If d_1 is not fundamental, then many arguments in [GZ85, Dor89] fail since the localizations of $\mathcal{O}_{d_1}$ are not necessarily discrete valuation rings. In addition, the descriptions of the constructions given in [Dor89] in the case that d_1 is squarefree and ℓ is ramified were incomplete and the proofs were omitted. We give a construction that works generally for all d_1, not necessarily fundamental, and all primes ℓ regardless of the splitting behavior of ℓ; see §6 for more details.

The next difficulty arose in studying the elements of the endomorphism rings; this study takes place in §7. The elements of these endomorphisms rings give rise to a study of ideals in $\mathcal{O}_{d_1}$, an order that is not necessarily maximal. This leads to difficulties in two ways. The first is that, in the Picard group of a *non-maximal* order, we can no longer assume that every 2-torsion element is represented by a ramified prime ideal. The second is that there are many more invertible ideals of order p^n for n sufficiently large when $p | f_1$ than in the usual case.

The last point of difficulty is in determining the action on the Lie algebra in the case that d_1 and d_2 share a common factor. If d_1 and d_2 are relatively prime, the action is almost trivial to compute. Indeed, this step in [GZ85] was dealt with by a one line argument. The general case is significantly more involved; see §8 for more details.

3.2. **Detailed outline of proof.** Assume that d_1 is fundamental at ℓ and that either $\ell \nmid \gcd(d_1, \widetilde{d_2})$ or that $\ell > 2$. Let $\mathbb{W}$ be the maximal order of $\mathbb{Q}_\ell(\sqrt{d_1})^{\mathrm{unr}}$; we write π for the uniformizer of $\mathbb{W}$. Let $E/\mathbb{W}$ be an elliptic curve with CM by $\mathcal{O}_{d_1}$ and with good reduction. Note that the formula for $v_\ell(F(m))$ is local, and remains unchanged by unramified extensions so we may replace L with L_μ^{unr}. Further we may assume that L is the minimal extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$ such that every elliptic curve with CM by $\mathcal{O}_{d_i}$ for $i = 1, 2$ has good reduction at μ.

As discussed above, we will relate the elements of Isom_{A/μ^n} to certain endomorphisms. Fix $\widetilde{\delta} \in A$ a fixed root of $4z^2 - 4\widetilde{d_2}z + \widetilde{d_2}^2 - \widetilde{d_2}$, and $\delta := \ell^{s_2}\widetilde{\delta} - \frac{1}{2}\ell^{s_2}\widetilde{d_2}(1 - \ell^{s_2})$. (Note that with this definition δ satisfies $4z^2 - 4d_2z + d_2^2 - d_2$.) Now consider the following subsets of $\mathrm{End}_{A/\mu^n}(E)$.

$$S_n(E/A) := \left\{ \begin{array}{l} \phi \in \mathrm{End}_{A/\mu^n}(E): \quad \phi^2 - d_2\phi + \frac{1}{4}(d_2^2 - d_2) = 0, \\ \qquad\qquad\qquad\qquad \mathbb{Z}[\phi] \hookrightarrow \mathrm{End}_{A/\mu}(E) \text{ optimal away from } \ell \end{array} \right\},$$

$$S_n^{\mathrm{Lie}}(E/A) := \left\{ \begin{array}{l} \phi \in S_n(E/A): \quad \widetilde{\phi} := \ell^{-s_2}\phi_0 + \frac{1}{2}\widetilde{d_2}(1 - \ell^{s_2}) = \widetilde{\delta} \text{ in } \mathrm{Lie}(E \bmod \mu) \\ \qquad\qquad\qquad\qquad \phi = \delta \text{ in } \mathrm{Lie}(E \bmod \mu^n) \end{array} \right\}.$$

In §4 we show that

$$\sum_{\tau_2} \# \mathrm{Isom}_{A/\mu^n}(E, E(\tau_2)) = \begin{cases} 0 & \text{if } \ell \mid f_2 \text{ and } n > 1, \\ \widetilde{w_2} \dfrac{\# \mathrm{Pic}(\mathcal{O}_{d_2})}{\# \mathrm{Pic}(\mathcal{O}_{\widetilde{d_2}})} \# S_n^{\mathrm{Lie}}(E) & \text{otherwise.} \end{cases} \tag{3.1}$$

In order to relate $v_\ell(F(m))$ to the cardinalities of S_n^{Lie}, we must first partition these sets by m; recall that $v_\ell(F(m))$ counts isomorphisms that give rise to a suborder of $\mathrm{End}(E)$ of discriminant m^2. We define:

$$S_{n,m}(E/A) := \left\{ \phi \in S_n(E/A) : \mathrm{disc}(\mathcal{O}_{d_1}[\phi]) = m^2 \right\},$$
$$S_{n,m}^{\mathrm{Lie}}(E/A) := S_{n,m}(E/A) \cap S_n^{\mathrm{Lie}}(E/A).$$

From the definition of $F(m)$ and (3.1), we see that

$$\frac{Cw_1}{4} e(\mu/\ell) v_\ell(F(m)) = \begin{cases} \sum_{\tau_1} \sum_{n \geq 1} \# S_{n,m}^{\mathrm{Lie}}(E(\tau_1)/A) & \text{if } \ell \nmid f_2, \\ \dfrac{\widetilde{w_2}}{w_2} \dfrac{\# \mathrm{Pic}(\mathcal{O}_{d_2})}{\# \mathrm{Pic}(\mathcal{O}_{\widetilde{d_2}})} \sum_{\tau_1} \# S_{1,m}^{\mathrm{Lie}}(E(\tau_1)/A) & \text{if } \ell \mid f_2 \end{cases} \tag{3.2}$$

where $C = 1$ if $4m = d_1 d_2$ and $C = 2$ otherwise.

Next we relate $\# S_{n,m}^{\mathrm{Lie}}(E/A)$ to $\# S_n(E/A)$ using the following result from §8:

$$\text{if } \ell \mid f_2, \quad \# S_1^{\mathrm{Lie}}(E(\tau_1)/A) = \begin{cases} \# S_1(E(\tau_1)/\mathbb{W}) & \text{if } \ell \mid \widetilde{d_2}, \\ \frac{1}{2} \# S_1(E(\tau_1)/\mathbb{W}) & \text{if } \ell \nmid \widetilde{d_2}, \end{cases} \tag{3.3}$$

$$\text{and if } \ell \nmid f_2, \quad \sum_n \# S_n^{\mathrm{Lie}}(E(\tau_1)/A) = \begin{cases} \sum_n \# S_n(E(\tau_1)/\mathbb{W}) & \text{if } \ell \nmid d_1, \ell \mid \widetilde{d_2}, \\ \frac{1}{2} \sum_n \# S_n(E(\tau_1)/\mathbb{W}) & \text{if } \ell \mid d_1 \text{ or } \ell \nmid \widetilde{d_2}. \end{cases} \tag{3.4}$$

10

Together with (3.2), these expressions yield

$$\frac{Cw_1}{4}e(\mu/\ell)v_\ell(F(m)) = \begin{cases} \sum_{\tau_1}\sum_{n\geq 1}\#S_{n,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell\nmid f_2 d_1 \text{ and } \ell|\widetilde{d}_2 \\ \frac{1}{2}\sum_{\tau_1}\sum_{n\geq 1}\#S_{n,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell\nmid f_2 \text{ and either } \ell\nmid\widetilde{d}_2 \text{ or } \ell|d_1, \\ \frac{\widetilde{w}_2\#\operatorname{Pic}(\mathcal{O}_{d_2})}{w_2\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d}_2})}\sum_{\tau_1}\#S_{1,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell|f_2,\widetilde{d}_2, \\ \frac{\widetilde{w}_2\#\operatorname{Pic}(\mathcal{O}_{d_2})}{2w_2\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d}_2})}\sum_{\tau_1}\#S_{1,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell|f_2, \ell\nmid\widetilde{d}_2. \end{cases}$$
(3.5)

Now we turn to the computation of $e(\mu/\ell)$; recall our running assumption that either $\ell > 2$ or $\ell\nmid \gcd(d_1,\widetilde{d}_2)$. Note that since d_1 is fundamental at ℓ, $L = L_{2,\mu}^{\mathrm{unr}}(\sqrt{d_1})$. Moreover, if $\ell|d_2$, then $\sqrt{d_1}\in L_{2,\mu}^{\mathrm{unr}}$, and if $\ell\nmid f_2$, then the only ramification comes from that of $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})/\mathbb{Q}$.

Assume that $\ell|f_2$. By local class field theory and [ST68, Theorem 9(2)], the ramification degree of $L/\mathbb{Q}_\ell^{\mathrm{unr}}(\sqrt{d_2})$ is ℓ^{s_2} if $\ell|\widetilde{d}_2$, $\ell^{s_2-1}(\ell+1)$ if ℓ in inert in $\mathbb{Q}(\sqrt{d_2})$, and $\ell^{s_2-1}(\ell-1)$ if ℓ is split in $\mathbb{Q}(\sqrt{d_2})$. By [Cox89, Theorem 7.24], this is equal to $\frac{\widetilde{w}_2}{w_2}\cdot\left(\#\operatorname{Pic}(\mathcal{O}_{d_2})/\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d}_2})\right)$. Thus, we have:

$$e(\mu/\ell) = \begin{cases} 1 & \text{if } \ell\nmid d_1 d_2, \\ 2 & \text{if } \ell|d_1 d_2, \ell\nmid f_2, \\ \frac{2\widetilde{w}_2\#\operatorname{Pic}(\mathcal{O}_{d_2})}{w_2\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d}_2})} & \text{if } \ell|f_2,\widetilde{d}_2, \\ \frac{\widetilde{w}_2\#\operatorname{Pic}(\mathcal{O}_{d_2})}{w_2\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d}_2})} & \text{if } \ell|f_2, \ell\nmid\widetilde{d}_2. \end{cases}$$

Combining this with (3.5), we obtain:

$$\frac{Cw_1}{2}v_\ell(F(m)) = \begin{cases} \frac{1}{e}\sum_{\tau_1}\sum_{n\geq 1}\#S_{n,m}(E(\tau_1)/A) & \text{if } \ell\nmid f_2, \\ \sum_{\tau_1}\#S_{1,m}^{\mathrm{Lie}}(E(\tau_1)/A) & \text{if } \ell|f_2. \end{cases}$$
(3.6)

It remains to compute $\sum_{\tau_1}\#S_{n,m}(E(\tau_1)/A)$.

Lemma 3.1. *Let* $m = 0$. *Then* $\#S_{n,0}(E/A) = 0$, *unless* $d_2 = d_1\ell^{2k}$, *in which case* $\#S_{n,0}(E/A) = 2$.

Proof. When $m = 0$, then $S_{n,m}(E/A)$ consists of elements in $\mathcal{O}_{d_1}$ with trace d_2 and norm $\frac{1}{4}(d_2^2 - d_2)$. In addition, the order generated by these elements must be optimally embedded at $p\neq\ell$. Thus $\#S_{n,0}(E/A) = 0$, unless $d_2 = d_1\ell^{2k}$, in which case $\#S_{n,0}(E/A) = 2$. $\square$

When $m\neq 0$ we will compute $\sum_{\tau_1}\#S_{n,m}(E(\tau_1)/A)$ by giving an explicit presentation for $\operatorname{End}_{\mathbb{W}/\pi^n}(E)$(§6), and then use this presentation to relate the elements of $S_{n,m}(E/\mathbb{W})$ to integral invertible ideals of norm $m\ell^{-r}$, where $r = 2n-1$ if ℓ is inert in $\mathbb{Q}(\sqrt{d_2})$ and $r = n$ otherwise(§7). More precisely we will prove in §7:

Theorem 3.2. *Assume that* $\ell\nmid f_1$ *and that* $m\neq 0$. *Then* $\sum_{\tau_1}\#S_{n,m}(E(\tau_1)/\mathbb{W})$ *is equal to an explicitly computable weighted sum of the number of certain invertible ideals of norm* $\ell^{-r}m$, *where* $r = 2n-1$ *if* $\ell\nmid d_1$ *and* $r = n$ *otherwise. If, in addition,* m *and* f_1 *are relatively prime, then*

$$\sum_{\tau_1}\#S_{n,m}(E(\tau_1)/\mathbb{W}) = \frac{Cw_1}{2}\rho(m)\mathfrak{A}(\ell^{-r}m),$$

11

where

$$\rho(m) = \begin{cases} 0 & \text{if } (d_1, -m)_p = -1 \text{ for } p|d_1, p \nmid f_1\ell, \\ 2^{\#\{p|(m,d_1):p\nmid f_2 \text{ or } p=\ell\}} & \text{otherwise.} \end{cases}$$

and

$$\mathfrak{A}(N) = \# \left\{ \mathfrak{b} \subseteq \mathcal{O}_{d_1} : \begin{array}{c} \mathrm{N}(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible,} \\ p \nmid \mathfrak{b} \text{ for all } p|\gcd(N, f_2), p \nmid \ell d_1 \\ \mathfrak{p}^3 \nmid \mathfrak{b} \text{ for all } \mathfrak{p}|p|\gcd(N, f_2, d_1), p \neq \ell \end{array} \right\}.$$

We will also prove in §7 that $\rho(m)\mathfrak{A}(\ell^{-r}m)$ can be expressed as a product of local factors. This completes the proof of Theorem 1.5. $\qquad\qquad\square$

4. Relating Isom_{A/μ^n} to S_n^{Lie}

We retain the notation from the previous section. From now on, we assume that $\ell \nmid f_1$. In this section, we prove

Proposition 4.1. *Let E be any elliptic curve over A with good reduction such that $E \cong \mathcal{O}_{d_1}$. Let d_2 be a quadratic imaginary discriminant different from d_1. Then*

$$\sum_{\tau_2} \# \mathrm{Isom}_{A/\mu^n}(E, E(\tau_2)) = \begin{cases} 0 & \text{if } \ell|f_2 \text{ and } n > 1, \\ \widetilde{w_2} \frac{\# \mathrm{Pic}(\mathcal{O}_{d_2})}{\# \mathrm{Pic}(\mathcal{O}_{\widetilde{d_2}})} \# S_n^{\mathrm{Lie}}(E) & \text{otherwise.} \end{cases}$$

where $e_2(\mu/\ell)$ is the ramification degree of L_μ^{unr} over the completion of the ring class field of $\mathcal{O}_{d_2}$ at the restriction of μ.

Proof. Assume that $\ell|f_2$. By [LT66] and by comparing ramification degrees of ℓ in L_2 and in $H_{\widetilde{d_2}}$, we see that $\mathrm{Isom}_{A/\mu^n}(E, E(\tau_2)) = \varnothing$ for all τ_2 of discriminant d_2. Henceforth, we restrict to the case that $\ell \nmid f_2$ or $n = 1$.

Let $E' = E(\tau_2)$ for some τ_2. Assume that $\mathrm{Isom}_{A/\mu^n}(E, E') \neq \varnothing$, and let $g \in \mathrm{Isom}_{A/\mu^n}(E, E')$. If $\theta' \in \mathrm{End}(E')$ is the unique element such that $c(\theta') = \delta$ in $\mathrm{Lie}(E')$, then $\theta'^g := g^{-1} \circ \theta \circ g \in \mathrm{End}(E \bmod \mu^n)$ has degree equal to $\frac{1}{4}(d_2^2 - d_2)$, trace equal to d_2, and $\theta'^g = \delta$ in $\mathrm{Lie}(E \bmod \mu^n)$. In addition, the order $\mathbb{Z}[\theta'^g]$ is p-optimally embedded in $\mathrm{End}(E \bmod \mu)$ for all $p \neq \ell$ by Proposition 2.2. If $p = \ell$, then $\widetilde{\theta'} := \ell^{-s_2}\theta' + \frac{1}{2}\widetilde{d_2}(1 - \ell^{s_2}) \in \mathrm{End}(E' \bmod \mu)$ and $c(\widetilde{\theta'}), c(\widetilde{\theta'}^g)$ are equal to $\widetilde{\delta}$ in $\mathrm{Lie}(E' \bmod \mu), \mathrm{Lie}(E \bmod \mu)$ respectively. Therefore, we have a set map

$$\bigsqcup_{[\tau_2]} \mathrm{Isom}_{A/\mu^n}(E, E(\tau_2)) \longrightarrow S_n^{\mathrm{Lie}}(E/A). \qquad\qquad (4.1)$$

Further, this map is surjective by the Serre-Tate lifting theorem [Con04, Thm. 3.3], the Grothendieck Existence theorem [Con04, Thm. 3.4], and the existence of canonical and quasi-canonical liftings (see [Gro86] in the supersingular case and [Meu07, Prop. 3.5] in the ordinary case). To complete the proof, we must determine the size of a fiber.

Let $g \in \mathrm{Isom}_{A/\mu^n}(E, E')$. Then the pairs $(E'' = E(\tau_2''), g'' \in \mathrm{Isom}_{A/\mu^n}(E, E''))$ such that $\theta''^{g''} = \theta'^{g'}$ is in bijection with isomorphisms $f: E' \bmod \mu^n \to E'' \bmod \mu^n$ such that the

diagram

$$
\begin{array}{ccc}
E' \bmod \mu^n & \xrightarrow{\ \theta'\ } & E' \bmod \mu^n \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\
E'' \bmod \mu^n & \xrightarrow{\ \theta''\ } & E'' \bmod \mu^n
\end{array}
$$

commutes. In particular, if $\theta'^{g'} = \theta''^{g''}$ then the diagram commutes when $n = 1$ with θ' and θ'' replaced with $\widetilde{\theta}'$ and $\widetilde{\theta}''$ respectively. By [GZ85, Prop. 2.7], there exist $\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d_2}})$ distinct isomorphism classes of pairs $(E' \bmod \mu, \theta' \in \operatorname{End}_{A/\mu}(E'))$. In particular, these isomorphisms classes correspond exactly to the isomorphism classes $(\widetilde{E}', \widetilde{\theta}' \in \operatorname{End}(\widetilde{E}'))$. So the above diagram commutes for arbitrary n if and only if it commutes for $n = 1$. (Recall if $\ell \mid f_2$, then we need only consider the case $n = 1$.)

Now it suffices to consider the case where $E' = E''$. In that case, we are interested in determining the number of automorphisms of $E' \bmod \mu^n$ which commute with θ'. Since the centralizer of θ' is exactly $\mathbb{Q}(\theta') \cap \operatorname{End}_{A/\mu^n}(E')$, there are exactly $\widetilde{w_2}$ such automorphisms. In summary, the fibers have cardinality

$$
\#\operatorname{Pic}(\mathcal{O}_{d_2}) \cdot \frac{1}{\#\operatorname{Pic}(\mathcal{O}_{\widetilde{d_2}})} \cdot \widetilde{w_2},
$$

which completes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

5. Background: quadratic imaginary orders

Let $\mathcal{O}$ be an order in a quadratic imaginary field, and let d be the discriminant of $\mathcal{O}$. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}$. If $\mathcal{O}$ is not maximal, then we can not necessarily write $\mathfrak{a}$ uniquely as a product of primes. However, we can always write $\mathfrak{a}$ uniquely as a product of primary ideals where no two ideals in the factorization are supported at the same prime. Precisely, for any prime $\mathfrak{p}$, define $\mathfrak{a}_{\mathfrak{p}} := \mathcal{O} \cap \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$. Then $\mathfrak{a} = \bigcap_{\mathfrak{p}} \mathfrak{a}_{\mathfrak{p}}$, and since for any 2 distinct primes $\mathfrak{p}, \mathfrak{q}$, $\mathfrak{a}_{\mathfrak{p}}$ and $\mathfrak{a}_{\mathfrak{q}}$ are co-maximal, we have that

$$
\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{a}_{\mathfrak{p}}.
$$

(See [Neu99, Prop 12.3] for more details.) If there is a unique prime $\mathfrak{p} \subseteq \mathcal{O}$ lying over p, then we will often write $\mathfrak{a}_p$ instead of $\mathfrak{a}_{\mathfrak{p}}$.

We will often be concerned with the special case where $\mathfrak{a} = \mathfrak{D} := \sqrt{d}\mathcal{O}$. If $p \mid d$ is odd, then for $a, b \in \mathcal{O}$, the difference $a - b \in \mathfrak{D}_p$ if and only if $\operatorname{Tr}(a) \equiv \operatorname{Tr}(b) \pmod{p^{v_p(d)}}$. If $p = 2 \mid d$, then $a - b \in \mathfrak{D}_2$ if and only if $a_0 \equiv b_0 \pmod{2^{v_2(d)-1}}$ and $a_1 \equiv b_1 \pmod 2$, where $a = a_0 + a_1 \frac{d+\sqrt{d}}{2}$ and $b = b_0 + b_1 \frac{d+\sqrt{d}}{2}$.

5.1. The Picard group.
The Picard group of $\mathcal{O}$, denoted $\operatorname{Pic}(\mathcal{O})$, is the group of invertible fractional ideals modulo fractional principal ideals. It is isomorphic to the form class group $C(d)$, the group of classes of primitive positive definite forms of discriminant d [Cox89, §7]. We will use this isomorphism to determine whether there exists an ideal in $2\operatorname{Pic}(\mathcal{O})$ of a certain norm. For more information on genus theory, i.e. the study of $\operatorname{Pic}(\mathcal{O})/2\operatorname{Pic}(\mathcal{O})$, see [Cox89].

13

Let $p_1, \ldots, p_j$ be the distinct odd primes dividing d. Define

$$k = \begin{cases} j & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 4 \pmod{16}, \\ j+1 & \text{if } d \equiv 8 \text{ or } 12 \pmod{16} \text{ or } d \equiv 16 \pmod{32}, \\ j+2 & \text{if } d \equiv 0 \pmod{32}. \end{cases}$$

For $i = 1, \ldots, j$, we define $\chi_{p_i}(a) := \left(\frac{a}{p_i}\right)$ for a coprime to p_i. For a odd, we also define $\chi_{-4}(a) := (-1)^{\frac{a-1}{2}}$, $\chi_8(a) := (-1)^{\frac{a^2-1}{8}}$. Then we define $\Psi \colon (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}^k$ as follows.

$$\Psi = \begin{cases} (\chi_{p_1}, \ldots, \chi_{p_j}) & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 4 \pmod{16}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_{-4}) & \text{if } d \equiv 12 \pmod{16} \text{ or } d \equiv 16 \pmod{32}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_8) & \text{if } d \equiv 8 \pmod{32}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_{-4}\chi_8) & \text{if } d \equiv 24 \pmod{32}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_{-4}, \chi_8) & \text{if } d \equiv 0 \pmod{32}. \end{cases}$$

For a prime p that divides d, but does not divide the conductor f of $\mathcal{O}$, we define

$$\Psi_p = \begin{cases} \chi_{p_i} & \text{if } p = p_i, \\ \chi_{-4} & \text{if } p = 2 \text{ and } d \equiv 12 \pmod{16}, \\ \chi_8 & \text{if } p = 2 \text{ and } d \equiv 8 \pmod{32}, \\ \chi_{-4} \cdot \chi_8 & \text{if } p = 2 \text{ and } d \equiv 24 \pmod{32}. \end{cases}$$

Let $\widehat{\Psi}_p$ be the projection of Ψ on the components that are complementary to the one that appears in Ψ_p.

For $p \nmid f$, we may extend Ψ_p to integers divisible by p by defining $\Psi_p(n)$ to be the Hilbert symbol $(d, n)_p$, for any integer n. Thus we can extend Ψ to $(\mathbb{Z}/f\mathbb{Z})^\times$, where f denotes the conductor of $\mathcal{O}$.

This map Ψ can be used to test when an ideal $\mathfrak{a}$ that is prime to f is a square in the Picard group.

Theorem 5.1 ([Cox89, §§3&7]). *For any positive integer m prime to the conductor f of $\mathcal{O}_d$, there exists an invertible ideal $\mathfrak{a}$ such that $\mathrm{N}(\mathfrak{a}) = m$ and $[\mathfrak{a}] \in 2\,\mathrm{Pic}(\mathcal{O}_d)$ if and only if $m \in \ker \Psi$.*

From this theorem, we can easily obtain the following corollary.

Corollary 5.2. *Let ℓ be a prime that divides d, but does not divide the conductor f. Let $\mathfrak{a}$ be an invertible integral ideal that is prime to the conductor. Then $[\mathfrak{a}] \in 2\,\mathrm{Pic}(\mathcal{O})$ if and only if $\mathrm{N}(\mathfrak{a}) \in \ker \widehat{\Psi}_\ell$.*

Proof. Define $\psi \colon (\mathbb{Z}/f\mathbb{Z})^\times \to \{\pm 1\}$ to be such that for any positive integer m that is coprime to f, $\psi(m) = 1$ if and only if there is an ideal in $\mathcal{O}$ of norm m. Using quadratic reciprocity, one can check that

$$\psi(m) = \prod_{p \mid \widetilde{d}} \Psi_p(m).$$

From this it is clear that $\mathrm{N}(\mathfrak{a}) \in \ker \widehat{\Psi}_\ell$ if and only if $\mathrm{N}(\mathfrak{a}) \in \ker \Psi$, which completes the proof. $\qquad\square$

5.2. **Genus class of ideals supported at the conductor.** Unfortunately, the map Ψ cannot be extended to all integers while still retaining the properties described in Theorem 5.1 and Corollary 5.2. This is because it is possible to have two invertible ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_d$ with the same norm, such that $\mathfrak{a}\mathfrak{b}^{-1} \notin 2\operatorname{Pic}(\mathcal{O}_d)$. This can only occur when the ideals are not relatively prime to f.

Let $\mathfrak{a}$ be an integral invertible ideal that is supported at a single prime p that divides the conductor, i.e. $\mathfrak{a}_{\mathfrak{q}} = \langle 1 \rangle$ for all $\mathfrak{q} \nmid p$. Let $\alpha \in \mathcal{O}$ be a generator for $\mathfrak{a}\mathcal{O}_p$ such that $\gcd(\mathrm{N}(\alpha), f)$ is supported only at p. Then $\mathfrak{a} \sim \widetilde{\mathfrak{a}}$ in $\operatorname{Pic}(\mathcal{O})$, where

$$\widetilde{\mathfrak{a}} := \mathcal{O}_p \cap \bigcap_{\mathfrak{q} \nmid p} (\alpha \mathcal{O}_{\mathfrak{q}}),$$

and $\mathrm{N}(\widetilde{\mathfrak{a}})$ is coprime to the conductor. Thus, the genus of $\mathfrak{a}$ is equal to $\Psi(\mathrm{N}(\widetilde{\mathfrak{a}}))$. Since every ideal can be factored uniquely into comaximal primary ideals, this gives a method of computing the genus class of any ideal.

6. Parametrizing endomorphism rings of supersingular elliptic curves

Let ℓ be a fixed prime and let $\mathcal{O}$ be a quadratic imaginary order of discriminant d such that $\ell \nmid f := \operatorname{cond}(d)$. We assume that ℓ is not split in $\mathcal{O}$. Let $\mathbb{W}$ be the ring of integers in $\mathbb{Q}_\ell^{\mathrm{unr}}(\sqrt{d})$, and write π for the uniformizer. By the theory of complex multiplication [Lan87, §10.3], the isomorphism classes of elliptic curves that have CM by $\mathcal{O}$ are in bijection with $\operatorname{Pic}(\mathcal{O})$, and every elliptic curve E with CM by $\mathcal{O}$ has a model defined over $\mathbb{W}$. Moreover, by [ST68, Cor. 1], we may assume that E has good reduction.

Fix a presentation $\mathbb{B}_{\ell,\infty}$ of the quaternion algebra ramified at ℓ and ∞, and fix an embedding $L := \operatorname{Frac}(\mathcal{O}) \hookrightarrow \mathbb{B}_{\ell,\infty}$. The goal of this section is to define, for every $[\mathfrak{a}] \in \operatorname{Pic}(\mathcal{O})$, a maximal order $R(\mathfrak{a}) \subset \mathbb{B}_{\ell,\infty}$ such that

(1) $R(\mathfrak{a}) \cap L = \mathcal{O}$,
(2) The optimal embedding $\mathcal{O} \hookrightarrow R(\mathfrak{a})$ is isomorphic to the embedding $\operatorname{End}(E(\mathfrak{a})) \hookrightarrow \operatorname{End}(E(\mathfrak{a}) \bmod \pi)$, where $E(\mathfrak{a})$ is the elliptic curve with CM by $\mathcal{O}$ that corresponds to $\mathfrak{a}$, and
(3) $\mathfrak{b}^{-1} R(\mathfrak{a}) \mathfrak{b} = R(\mathfrak{a}\mathfrak{b})$.

Since we will use these maximal orders in the next section to compute the sets $S_{n,m}(E(\mathfrak{a}))$, we also want the orders $R(\mathfrak{a})$ to be fairly explicit.

Our construction of these maximal orders $R(\mathfrak{a})$ generalizes the work of Gross-Zagier [GZ85] and Dorman [Dor89], where they defined maximal orders with these properties under the assumption that $-d$ is prime [GZ85] or d is squarefree [Dor89]. We treat arbitrary discriminants d, correct errors and omissions in some proofs in [Dor89], and treat the ramified case in detail, giving complete definitions and proofs.

Note that Goren and the first author have given a different generalization of Dorman's work [GL13] to higher dimensions, which works for CM fields K, characterizing superspecial orders in a quaternion algebra over the totally real field K^+ with an optimal embedding of $\mathcal{O}_{K^+}$. That work also corrects the proofs of [Dor89], but in a slightly different way than we do here, and does not handle the ramified case or non-maximal orders.

6.0.1. *Outline.* In §6.1, we give an explicit presentation of $\mathbb{B}_{\ell,\infty}$ that we will work with throughout. The construction of the maximal orders $R(\mathfrak{a})$ depends on whether ℓ is inert

or ramified in $\mathcal{O}$. The inert case is discussed in detail in §6.2, and the construction in the ramified case is given in §6.3. In these sections we also prove that our construction satisfies conditions (1) and (3). While the construction of $R(\mathfrak{a})$ is different in the ramified case, many of the proofs go through as in the inert case with minor modifications. Because of this, in §6.3, we only explain the modifications and omit the rest of the proofs. In §6.4, we show that these constructions also satisfy property (2).

6.1. **Representations of quaternion algebra.** Given a fixed embedding $\iota\colon L \hookrightarrow \mathbb{B}_{\ell,\infty}$, the quaternion algebra $\mathbb{B}_{\ell,\infty}$ can be written uniquely as $\iota(L) \oplus \iota(L)j$, where $j \in \mathbb{B}_{\ell,\infty}$ is such that $j\iota(\alpha)j^{-1} = \iota(\overline{\alpha})$, for all $\alpha \in L$. Thus j^2 defines a unique element in $\mathbb{Q}^{\times}/\mathrm{N}(L^{\times})$. From now on, we will represent $\mathbb{B}_{\ell,\infty}$ as a sub-algebra of $\mathrm{M}_2(L)$ as follows.

$$\mathbb{B}_{\ell,\infty} = \left\{ [\alpha : \beta] := \begin{pmatrix} \alpha & \beta \\ j^2\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in L \right\}. \tag{6.1}$$

Under this representation, $\iota\colon L \hookrightarrow \mathbb{B}_{\ell,\infty}, \quad \iota(\alpha) = [\alpha, 0]$.

If ℓ is unramified in $\mathcal{O}$ then we may assume that $j^2 = -\ell q$, where q is a prime such that $-\ell q \in \ker \Psi$ and $q \nmid d$. If ℓ is ramified, then we may assume that $j^2 = -q$ where $-q \in \ker \widehat{\Psi}_\ell$, $-q \notin \ker \Psi_\ell$ and $q \nmid d$. (Recall that Ψ, $\widehat{\Psi}_\ell$ and Ψ_ℓ were defined in §5.) In both cases, these conditions imply that q is split in $\mathcal{O}$.

6.2. **The inert case.** Let $\mathfrak{a} \subseteq \mathcal{O}$ be an integral invertible ideal such that $\gcd(f, \mathrm{N}(\mathfrak{a})) = 1$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ lying over q. For any $\lambda \in \mathcal{O}$ such that

  (1) $\lambda\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subseteq \mathcal{O}$, and
  (2) $\mathrm{N}(\lambda) \equiv -\ell q \pmod{d}$,

we define

$$R(\mathfrak{a}, \lambda) := \left\{ [\alpha, \beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\ell^{n-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda\beta \in \mathcal{O} \right\}.$$

From this definition, it is clear that if λ' satisfies (1) and (2) and $\lambda \equiv \lambda' \pmod{\mathfrak{D}}$, then $R(\mathfrak{a}, \lambda) = R(\mathfrak{a}, \lambda')$. We claim that, for any $\mathfrak{a}$ and λ satisfying conditions (1) and (2), $R(\mathfrak{a}, \lambda)$ is a maximal order.

Remark 6.1. Although Dorman [Dor89] does not include condition (1) in his definition, it is, in fact, necessary. Without this assumption $R(\mathfrak{a}, \lambda)$ is not closed under multiplication, even if d is squarefree. This was already remarked on in [GL13].

Remark 6.2. Write $\lambda = \lambda_0 + \lambda_1\frac{d+\sqrt{d}}{2}$. If d is odd, then the congruence class of $\lambda \bmod \mathfrak{D}$ is determined by $\lambda_0 \bmod d$. In addition, the condition that $\mathrm{N}(\lambda) \equiv -\ell q \pmod{d}$ is equivalent to the condition that $\lambda_0^2 \equiv -\ell q \pmod{d}$. Therefore, if d is odd, then we may think of λ as an integer, instead of as an element of $\mathcal{O}$. This was the point of view taken in [GZ85, Dor89].

Lemma 6.3. $R(\mathfrak{a}, \lambda)$ *is an order.*

Proof. We will show that $R(\mathfrak{a}, \lambda)$ is closed under multiplication. All other properties are easily checked. Consider

$$\left[\frac{a_1}{\sqrt{d}}, \frac{b_1}{\sqrt{d}} \right], \left[\frac{a_2}{\sqrt{d}}, \frac{b_2}{\sqrt{d}} \right] \in R(\mathfrak{a}, \lambda).$$

Their product is in $R(\mathfrak{a}, \lambda)$ if and only if

  (1) $a_1a_2 + \ell q b_1\overline{b}_2 \in \mathfrak{D}$

(2) $a_1 b_2 - \bar{a}_2 b_1 \in \mathfrak{D}\mathfrak{q}^{-1}\bar{\mathfrak{a}}\mathfrak{a}^{-1}$

(3) $a_1 a_2 + \ell q b_1 \bar{b}_2 - \lambda a_1 b_2 + \lambda \bar{a}_2 b_1 \in d\mathcal{O}$

Claim 1: Note that $a_1 a_2 + \ell q b_1 \bar{b}_2$ can be rewritten as

$$(a_1 - \lambda b_1)a_2 + \lambda b_1(a_2 - \lambda b_2) + \lambda b_1(\lambda b_2 - \overline{\lambda b_2}) + (N(\lambda) + \ell q)b_1 \bar{b}_2. \tag{6.2}$$

Using the definition of $R(\mathfrak{a}, \lambda)$ and the fact that for any $c \in \mathcal{O}$, $(c - \bar{c}) \in \mathfrak{D}$, one can easily check that (6.2) is in $\mathfrak{D}$.

Claim 2: We rewrite $a_1 b_2 - \bar{a}_2 b_1$ as $(a_1 - \lambda b_1)b_2 - (\bar{a}_2 - \overline{\lambda b_2})b_1 + b_1(\lambda b_2 - \overline{\lambda b_2})$. From this description, one can easily check that $a_1 b_2 - \bar{a}_2 b_1 \in \mathfrak{D}\mathfrak{q}^{-1}\bar{\mathfrak{a}}\mathfrak{a}^{-1}$.

Claim 3: Let $a_i' \in \mathcal{O}$ be such that $a_i = \lambda b_i + \sqrt{d}a_i'$. Then we can rewrite $a_1 a_2 + \ell q b_1 \bar{b}_2 - \lambda a_1 b_2 + \lambda \bar{a}_2 b_1$ as

$$\lambda^2 b_1 b_2 + \sqrt{d}\lambda(b_1 a_2' + a_1' b_2) + d a_1' a_2' + \ell q b_1 \bar{b}_2 - \lambda^2 b_1 b_2 - \lambda\sqrt{d}a_1' b_2 + N(\lambda)\bar{b}_2 b_1 - \lambda\sqrt{d}b_1\bar{a}_2' \tag{6.3}$$

$$= d a_1' a_2' + (N(\lambda) + \ell q)b_1 \bar{b}_2 + \lambda\sqrt{d}b_1(a_2' - \bar{a}_2'). \tag{6.4}$$

Similar arguments as above show that (6.4) is in $d\mathcal{O}$. $\square$

Lemma 6.4. *The discriminant of $R(\mathfrak{a}, \lambda)$ is ℓ^2, and so $R(\mathfrak{a}, \lambda)$ is a maximal order.*

Proof. To prove this lemma, we will use an auxiliary (non-maximal) order

$$\widetilde{R}(\mathfrak{a}) := \left\{ [\alpha, \beta] : \alpha \in \mathcal{O}, \beta \in \bar{\mathfrak{a}}\mathfrak{a}^{-1} \right\}.$$

One can easily check that this is an order. Let ω_1, ω_2 be a $\mathbb{Z}$-basis for $\bar{\mathfrak{a}}\mathfrak{a}^{-1}$. Then

$$[1, 0], \; [(d + \sqrt{d})/2, 0], \; [0, \omega_1], \; [0, \omega_2]$$

is a $\mathbb{Z}$-basis for $\widetilde{R}(\mathfrak{a})$. Using these basis elements, one can show that $\operatorname{disc}(\widetilde{R}(\mathfrak{a})) = (\ell q d)^2$.

We claim that $\widetilde{R}(\mathfrak{a})$ is related to $R(\mathfrak{a}, \lambda)$ by the following exact sequence,

$$0 \to \widetilde{R}(\mathfrak{a}) \to R(\mathfrak{a}, \lambda) \xrightarrow{[\alpha, \beta] \mapsto \beta} \mathfrak{q}^{-1}\mathfrak{D}^{-1}\bar{\mathfrak{a}}\mathfrak{a}^{-1}/\bar{\mathfrak{a}}\mathfrak{a}^{-1} \to 0.$$

This exact sequence implies that $\left[R(\mathfrak{a}, \lambda) : \widetilde{R}(\mathfrak{a}) \right] = qd$, and thus the lemma follows.

Proof of claim: Exactness on the left is straightforward. Exactness on the right holds since for any $\beta \in \mathfrak{q}^{-1}\mathfrak{D}^{-1}\bar{\mathfrak{a}}\mathfrak{a}$, $[\lambda\beta, \beta] \in R(\mathfrak{a}, \lambda)$. The order $\widetilde{R}(\mathfrak{a})$ is clearly in $\ker([\alpha, \beta] \mapsto \beta)$, and the reverse containment follows since $\beta \in \bar{\mathfrak{a}}\mathfrak{a}^{-1}$ implies that $\lambda_{\mathfrak{a}}\beta$, and hence α, is in $\mathcal{O}$. $\square$

Given an ideal $\mathfrak{a}$, we will now construct a $\lambda = \lambda_{\mathfrak{a}}$ satisfying conditions (1) and (2). Since we want our orders $R(\mathfrak{a}) := R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ to satisfy

$$R(\mathfrak{a})\mathfrak{b} = \mathfrak{b}R(\mathfrak{a}\mathfrak{b}),$$

the relationship between $\lambda_{\mathfrak{a}}$ and $\lambda_{\mathfrak{a}\mathfrak{b}}$ will be quite important. In fact, the relation

$$R(\mathcal{O})\mathfrak{a} = \mathfrak{a}R(\mathfrak{a})$$

shows that $R(\mathfrak{a})$ is determined from $R(\mathcal{O})$ and so $\lambda_{\mathfrak{a}} \bmod \mathfrak{D}$ is determined by $\lambda_{\mathcal{O}} \bmod \mathfrak{D}$.

6.2.1. *Defining* $\lambda_{\mathfrak{a}}$. For all invertible ramified primes p, fix two elements $\lambda^{(p)}, \widetilde{\lambda}^{(p)} \in \mathcal{O}$ with norm congruent to $-\ell q \bmod p^{v(d)}$ such that $\lambda^{(p)} \not\equiv \widetilde{\lambda}^{(p)} \pmod{\mathfrak{D}_p}$. For all non-invertible ramified primes p, fix $\lambda^{(p)} \in \mathcal{O}$ such that $\mathrm{N}(\lambda^{(p)}) \equiv -\ell q \pmod{p^{v(d)}}$.

For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ that is prime to $\mathfrak{D}$, let $M(\mathfrak{p})$ denote a fixed integer that is divisible by $\mathrm{N}(\mathfrak{p})$ and congruent to $1 \pmod{d}$. For any product of invertible ramified primes $\mathfrak{b}_d := \prod_{\substack{\mathfrak{p} \text{ invertible} \\ \mathfrak{p}|\mathfrak{D}}} \mathfrak{p}^{e_{\mathfrak{p}}}$, we write $\lambda_{\mathfrak{b}_d}$ for any element in $\mathcal{O}$ such that

$$
\lambda_{\mathfrak{b}_d} \bmod \mathfrak{D}_p \equiv \begin{cases} \lambda^{(p)} & \text{if } e_p \equiv 0 \pmod{2} \\ \widetilde{\lambda}^{(p)} & \text{if } e_p \equiv 1 \pmod{2} \end{cases}
$$

for all invertible ramified primes $\mathfrak{p}$ and $\lambda_{\mathfrak{b}_d} \equiv \lambda^{(p)} \pmod{\mathfrak{D}_p}$ for all non-invertible primes. These conditions imply that $\lambda_{\mathfrak{b}_d}$ is well-defined modulo $\mathfrak{D}$.

Let $\mathfrak{a}$ be an invertible integral ideal $\mathcal{O}$ such that $\gcd(\mathrm{N}(\mathfrak{a}), f) = 1$. Then we may factor $\mathfrak{a}$ as $\mathfrak{a}'\mathfrak{a}_d$, where $\mathfrak{a}'$ is prime to the discriminant and $\mathfrak{a}_d$ is supported only on invertible ramified primes. We define $\lambda_{\mathfrak{a}} := \left(\prod_{\mathfrak{p}|\mathfrak{a}'} M(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a}')} \right) M(\mathfrak{q})\lambda_{\mathfrak{a}_d}$. Note that it follows from this definition that $\lambda_{\mathfrak{a}}$ is well-defined modulo $\mathfrak{D}$ and, importantly, that $\lambda_{\mathfrak{a}}$ satisfies $\lambda_{\mathfrak{a}}\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subset \mathcal{O}$ and $\mathrm{N}(\lambda_{\mathfrak{a}}) \equiv -\ell q \bmod d$.

Lemma 6.5. *Let $\mathfrak{a}, \mathfrak{b}$ be two invertible ideals in $\mathcal{O}$ that are prime to the conductor. Assume that $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{b}$ are both integral. Then*

$$
R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mathfrak{b} = \mathfrak{b}R(\mathfrak{a}\mathfrak{b}, \lambda_{\mathfrak{a}\mathfrak{b}}).
$$

Proof. We will show that $R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mathfrak{b} \subseteq \mathfrak{b}R(\mathfrak{a}\mathfrak{b}, \lambda_{\mathfrak{a}\mathfrak{b}})$. The reverse containment then follows by letting $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ and $\mathfrak{b} = \mathfrak{b}^{-1}$. Note that if $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2^{-1}$ with $\mathfrak{b}_i$ integral, we may rewrite $\mathfrak{b}$ as $\mathfrak{b}_1\overline{\mathfrak{b}_2}\,\mathrm{N}(\mathfrak{b}_2)^{-1}$. Since $\mathrm{N}(\mathfrak{b}_2)^{-1}$ is in the center of $\mathbb{B}_{\ell,\infty}$ and $R(\mathfrak{a}, \lambda_{\mathfrak{a}}) = R(N\mathfrak{a}, \lambda_{N\mathfrak{a}})$ for any integer N, we may reduce to the case where $\mathfrak{b}$ is integral. We will also assume that $\mathfrak{b} = \mathfrak{p}$ is prime; the general result follows from multiplicativity.

We can write

$$
\mathfrak{p}R(\mathfrak{a}\mathfrak{p}, \lambda_{\mathfrak{a}\mathfrak{p}}) = \left\{ [\tilde{\alpha}, \tilde{\beta}] : \tilde{\alpha} \in \mathfrak{p}\mathfrak{D}^{-1}, \tilde{\beta} \in \mathfrak{q}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\overline{\mathfrak{p}}\mathfrak{a}^{-1}, \tilde{\alpha} - \lambda_{\mathfrak{a}\mathfrak{p}}\tilde{\beta} \in \mathfrak{p} \right\}.
$$

Take $[\alpha, \beta] \in R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ and $\gamma \in \mathfrak{p}$; the product equals $[\gamma\alpha, \overline{\gamma}\beta]$. One can easily see that $\gamma\alpha \in \mathfrak{p}\mathfrak{D}^{-1}$ and that $\overline{\gamma}\beta \in \mathfrak{q}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\overline{\mathfrak{p}}\mathfrak{a}^{-1}$. It remains to show that $\gamma\alpha - \lambda_{\mathfrak{a}\mathfrak{p}}\overline{\gamma}\beta \in \mathfrak{p}$.

Consider the case where $\mathfrak{p}$ is unramified. Since $\lambda_{\mathfrak{a}\mathfrak{p}} = M(\mathfrak{p})\lambda_{\mathfrak{a}}$, we may rewrite $\gamma\alpha - \lambda_{\mathfrak{a}\mathfrak{p}}\overline{\gamma}\beta$ as

$$
(\gamma - \overline{\gamma}M(\mathfrak{p}))\alpha + \overline{\gamma}M(\mathfrak{p})(\alpha - \lambda_{\mathfrak{a}}\beta).
$$

Since $p|M(\mathfrak{p})$ and $M(\mathfrak{p}) \equiv 1 \pmod{d}$, one can easily check that $(\gamma - \overline{\gamma}M(\mathfrak{p}))\alpha$ and $\overline{\gamma}M(\mathfrak{p})(\alpha - \lambda_{\mathfrak{a}}\beta)$ are in $\mathfrak{p}$.

Now consider the case where $\mathfrak{p}$ is ramified. Then $\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{a}\mathfrak{p}} \in \mathfrak{D}_{\mathfrak{p}'}$ for all ramified $\mathfrak{p}' \neq \mathfrak{p}$, so it is clear that $v_{\mathfrak{p}'}(\gamma\alpha - \lambda_{\mathfrak{a}\mathfrak{p}}\overline{\gamma}\beta) \geq 0$ for all $\mathfrak{p}' \neq \mathfrak{p}$. It remains to show that $v_{\mathfrak{p}}(\gamma\alpha - \overline{\gamma}\lambda_{\mathfrak{a}\mathfrak{p}}\beta) \geq 1$.

First consider the case when $\mathfrak{p}|2$. Rewrite $\gamma\alpha - \lambda_{\mathfrak{a}\mathfrak{p}}\overline{\gamma}\beta$ as

$$
\gamma(\alpha - \lambda_{\mathfrak{a}}\beta) + \gamma(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{a}\mathfrak{p}})\beta + \lambda_{\mathfrak{a}\mathfrak{p}}\beta(\gamma - \overline{\gamma}). \tag{6.5}
$$

From the definition of $\lambda_{\mathfrak{a}}$, we see that $v_{\mathfrak{p}}(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{a}\mathfrak{p}}) = v_{\mathfrak{p}}(\mathfrak{D}) - 1$. Thus $\gamma(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{a}\mathfrak{p}})\beta$ is a $\mathfrak{p}$-adic unit if $v_{\mathfrak{p}}(\beta) = -v_{\mathfrak{p}}(\mathfrak{D})$ and $v_{\mathfrak{p}}(\gamma) = 1$, and in $\mathfrak{p}$ otherwise. Moreover, the same

18

characterization holds for $\lambda_{\mathfrak{a}\mathfrak{p}}\beta(\gamma - \overline{\gamma})$. Since $\#\mathcal{O}/\mathfrak{p} = 2$, a sum of two $\mathfrak{p}$-adic units is in $\mathfrak{p}$. Hence, we conclude that $v_{\mathfrak{p}}(\gamma\alpha - \overline{\gamma}\lambda_{\mathfrak{a}\mathfrak{p}}\beta) \geq 1$.

If p is odd, then $v_{\mathfrak{p}}(\beta) \geq -1$. Combining the last two terms in equation 6.5, we see that we need to prove that $v_{\mathfrak{p}}((\gamma\lambda_{\mathfrak{a}} - \overline{\gamma}\lambda_{\mathfrak{a}\mathfrak{p}})\beta) \geq 1$, so it suffices to prove that $v_{\mathfrak{p}}(\gamma\lambda_{\mathfrak{a}} - \overline{\gamma}\lambda_{\mathfrak{a}\mathfrak{p}}) \geq 2$. From the definition of $\lambda_{\mathfrak{a}}$, we see that $\lambda_{\mathfrak{a}} + \lambda_{\mathfrak{a}\mathfrak{p}} \in \mathfrak{p}$, and since $\gamma \in \mathfrak{p}$, $\gamma + \overline{\gamma} \in \mathfrak{p}^2$. Thus $\gamma(\lambda_{\mathfrak{a}} + \lambda_{\mathfrak{a}\mathfrak{p}}) - (\gamma + \overline{\gamma})\lambda_{\mathfrak{a}\mathfrak{p}} = \gamma\lambda_{\mathfrak{a}} - \overline{\gamma}\lambda_{\mathfrak{a}\mathfrak{p}}$ is in $\mathfrak{p}^2$. $\square$

6.3. **The ramified case.** Let $\mathfrak{a} \subseteq \mathcal{O}$ be an integral invertible ideal such that $\gcd(f, \mathrm{N}(\mathfrak{a})) = 1$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ lying over q. For any $\lambda \in \mathcal{O}$ such that

(1) $\lambda\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subseteq \mathcal{O}$, and
(2) $\mathrm{N}(\lambda) \equiv -q \pmod{d/\ell}$,

we define
$$R(\mathfrak{a}, \lambda) := \left\{ [\alpha, \beta] : \alpha \in \mathfrak{l}\mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\mathfrak{l}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda\beta \in \mathcal{O} \right\}.$$
From this definition, it is clear that if λ' satisfies (1) and (2) and $\lambda \equiv \lambda' \pmod{\mathfrak{D}\mathfrak{l}^{-1}}$, then $R(\mathfrak{a}, \lambda) = R(\mathfrak{a}, \lambda')$. We claim that, for any $\mathfrak{a}$ and λ, $R(\mathfrak{a}, \lambda)$ is a maximal order.

Lemma 6.6. $R(\mathfrak{a}, \lambda)$ *is an order.*

Proof. We will show that $R(\mathfrak{a}, \lambda)$ is closed under multiplication. All other properties are easily checked. Consider
$$\left[\frac{a_1}{\sqrt{d}}, \frac{b_1}{\sqrt{d}} \right], \left[\frac{a_2}{\sqrt{d}}, \frac{b_2}{\sqrt{d}} \right] \in R(\mathfrak{a}, \lambda).$$
Their product is in $R(\mathfrak{a}, \lambda)$ if and only if

(1) $a_1 a_2 + q b_1 \overline{b}_2 \in \mathfrak{l}\mathfrak{D}$
(2) $a_1 b_2 - \overline{a}_2 b_1 \in \mathfrak{l}\mathfrak{D}\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}$
(3) $a_1 a_2 + q b_1 \overline{b}_2 - \lambda a_1 b_2 + \lambda \overline{a}_2 b_1 \in d\mathcal{O}$

The proof of these claims goes through exactly as in the inert case, after replacing every q in the inert case with q/ℓ, and after noting that $a_i, \overline{a}_i \in \mathfrak{l}$ and $b_i, \overline{b}_i \in \mathfrak{l}\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}$. $\square$

Lemma 6.7. *The discriminant of* $R(\mathfrak{a}, \lambda)$ *is* ℓ^2*, and so* $R(\mathfrak{a}, \lambda)$ *is a maximal order.*

Proof. This proof is exactly the same as in the inert case after replacing q with q/ℓ. $\square$

6.3.1. *Defining $\lambda_{\mathfrak{a}}$.* For all invertible ramified primes p, fix two elements $\lambda^{(p)}, \widetilde{\lambda}^{(p)} \in \mathcal{O}$ with norm congruent to $-q$ mod $p^{v(d/\ell)}$ such that $\lambda^{(p)} \not\equiv \widetilde{\lambda}^{(p)} \pmod{\mathfrak{D}_p}$. If $p = \ell$ and $\ell \neq 2$, then in addition we assume that $\lambda_{\ell,0} = -\lambda_{\ell,1}$. For all non-invertible ramified primes p, fix $\lambda^{(p)} \in \mathcal{O}$ such that $\mathrm{N}(\lambda^{(p)}) \equiv -q \pmod{p^{v(d/\ell)}}$.

For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ that is coprime to $\mathfrak{D}$, let $M(\mathfrak{p})$ denote a fixed integer that is divisible by $\mathrm{N}(\mathfrak{p})$ and congruent to $1 \pmod{d}$. For any product of invertible ramified primes $\mathfrak{b}_d := \prod_{\substack{\mathfrak{p} \text{ invertible} \\ \mathfrak{p}|\mathfrak{D}}} \mathfrak{p}^{e_{\mathfrak{p}}}$, we write $\lambda_{\mathfrak{b}_d}$ for any element in $\mathcal{O}$ such that

$$\lambda_{\mathfrak{b}_d} \bmod \mathfrak{D}_p \equiv \begin{cases} \lambda^{(p)} & \text{if } e_p \equiv 0 \pmod{2}, \\ \widetilde{\lambda}^{(p)} & \text{if } e_p \equiv 1 \pmod{2}. \end{cases}$$

for all invertible ramified primes $\mathfrak{p}$ and $\lambda_{\mathfrak{b}_d} \equiv \lambda^{(p)} \pmod{\mathfrak{D}_p}$ for all non-invertible primes. These conditions imply that $\lambda_{\mathfrak{b}_d}$ is well-defined modulo $\mathfrak{D}$.

Let $\mathfrak{a}$ be an invertible integral ideal $\mathcal{O}$ such that $(\mathrm{N}(\mathfrak{a}), f) = 1$. Then we may factor $\mathfrak{a}$ as $\mathfrak{a}'\mathfrak{a}_d$, where $\mathfrak{a}'$ is coprime to the discriminant and $\mathfrak{a}_d$ is supported only on invertible ramified primes. We define $\lambda_{\mathfrak{a}} := \left(\prod_{\mathfrak{p} | \mathfrak{a}'} M(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a}')} \right) M(\mathfrak{q}) \lambda_{\mathfrak{a}_d}$. Note that $\lambda_{\mathfrak{a}}$ is well-defined modulo $\mathfrak{D}$ and that $\lambda_{\mathfrak{a}}$ satisfies $\lambda_{\mathfrak{a}} \mathfrak{q}^{-1} \overline{\mathfrak{a}} \mathfrak{a}^{-1} \subset \mathcal{O}$ and $\mathrm{N}(\lambda_{\mathfrak{a}}) \equiv -q \mod d/\ell$.

Remark 6.8. Since $\lambda_{\mathfrak{a}} \equiv \lambda_{\mathfrak{a}\mathfrak{l}} \pmod{\mathfrak{D}\mathfrak{l}^{-1}}$ for any integral invertible ideal $\mathfrak{a}$, the corresponding orders $R(\mathfrak{a})$, $R(\mathfrak{a}\mathfrak{l})$ are equal. This is not surprising, since $E(\mathfrak{a}) \cong E(\mathfrak{a}\mathfrak{l})$ modulo π.

Lemma 6.9. *Let $\mathfrak{a}, \mathfrak{b}$ be two invertible ideals in $\mathcal{O}$ that are coprime to the conductor. We assume that $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{b}$ are integral. Then*

$$R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mathfrak{b} = \mathfrak{b}R(\mathfrak{a}\mathfrak{b}, \lambda_{\mathfrak{a}\mathfrak{b}}).$$

Proof. As in the proof of Lemma 6.5, it suffices to prove that $R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mathfrak{b} \subset \mathfrak{b}R(\mathfrak{a}\mathfrak{b}, \lambda_{\mathfrak{a}\mathfrak{b}})$ and we can reduce to the case where $\mathfrak{b}$ is prime.

We can write

$$\mathfrak{p}R(\mathfrak{a}\mathfrak{p}, \lambda_{\mathfrak{a}\mathfrak{p}}) = \left\{ [\tilde{\alpha}, \tilde{\beta}] : \tilde{\alpha} \in \mathfrak{p}\mathfrak{l}\mathfrak{D}^{-1}, \tilde{\beta} \in \mathfrak{q}^{-1}\mathfrak{l}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\overline{\mathfrak{p}}\mathfrak{a}^{-1}, \tilde{\alpha} - \lambda_{\mathfrak{a}\mathfrak{p}}\tilde{\beta} \in \mathfrak{p} \right\}.$$

Take $[\alpha, \beta] \in R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ and $\gamma \in \mathfrak{p}$: the product equals $[\gamma\alpha, \overline{\gamma}\beta]$. One can easily see that $\gamma\alpha \in \mathfrak{p}\mathfrak{l}\mathfrak{D}^{-1}$ and that $\overline{\gamma}\beta \in \mathfrak{q}^{-1}\mathfrak{l}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\overline{\mathfrak{p}}\mathfrak{a}^{-1}$. It remains to show that $\gamma\alpha - \lambda_{\mathfrak{a}\mathfrak{p}}\overline{\gamma}\beta \in \mathfrak{p}$.

We will focus on the case where $\mathfrak{b} = \mathfrak{l}$; if $\mathfrak{b} \neq \mathfrak{l}$, then the proof is exactly as in Lemma 6.5. We can rewrite $\gamma\alpha - \lambda_{\mathfrak{a}\mathfrak{l}}\overline{\gamma}\beta$ as

$$\gamma(\alpha - \lambda_{\mathfrak{a}}\beta) + \gamma\beta(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{a}\mathfrak{l}}) + \lambda_{\mathfrak{a}\mathfrak{l}}\beta(\gamma - \overline{\gamma}).$$

It is straightforward to see that the first and third terms are in $\mathfrak{l}$. The second term is in $\mathfrak{l}$ since $v_{\mathfrak{l}}(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{a}\mathfrak{l}}) = v_{\mathfrak{l}}(\mathfrak{D}) - 1$. This completes the proof. $\qquad\square$

6.4. **Elliptic curves with complex multiplication.**

Lemma 6.10. *Let R be a maximal order of $\mathbb{B}_{\ell,\infty}$ such that $R \cap L = \mathcal{O}$, where the intersection takes place using the embedding of $\mathbb{B}_{\ell,\infty} \subset \mathrm{M}_2(L)$ given in (6.1). Then there is an integral invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ coprime to the conductor such that R is conjugate to $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ by an element of $L^{\times}$.*

Proof. Since R is a maximal order in $\mathbb{B}_{\ell,\infty}$, $\mathcal{O}$ must be maximal at ℓ [Vig80, Chap. 2, Lemma 1.5]. Therefore we can define $R(\mathcal{O}, \lambda_{\mathcal{O}})$ as in §6.2 or §6.3 depending on whether ℓ is inert or ramified in $\mathcal{O}$. Since $R(\mathcal{O})$ and R both have $\mathcal{O}$ optimally embedded, by [Eic57, Thm. 4, p.118], there exists an invertible ideal $\mathfrak{a}'$ such that $R = \mathfrak{a}'^{-1}R(\mathcal{O})\mathfrak{a}'$. We may write $\mathfrak{a}'$ as $\theta\mathfrak{a}$, where $\theta \in L^{\times}$ and $\mathfrak{a}$ is integral and coprime to the conductor. Thus, Lemmas 6.5 and 6.9 show that $R = \theta^{-1}R(\mathfrak{a}, \lambda_{\mathfrak{a}})\theta$.

$\qquad\square$

Fix an element $[\tau^{(0)}]$ of discriminant d, and let $E = E(\tau^{(0)})$ be an elliptic curve over $\mathbb{W}$ with $j(E) = j(\tau^{(0)})$ and good reduction at π. Then we have an optimal embedding of $\mathcal{O} \cong \mathrm{End}(E)$ into $\mathrm{End}_{\mathbb{W}/\pi}(E)$, a maximal order in $\mathbb{B}_{\ell,\infty}$. Thus, by Lemma 6.10, there is an element $[\mathfrak{a}_0] \in \mathrm{Pic}(\mathcal{O})$ such that the pair

$$(\mathrm{End}(E \bmod \mathfrak{l}), \iota \colon \mathcal{O} = \mathrm{End}(E) \hookrightarrow \mathrm{End}(E \bmod \mathfrak{l}))$$

is conjugate to $R(\mathfrak{a}_0)$ with the diagonal embedding $\mathcal{O} \hookrightarrow R(\mathfrak{a}_0)$. Now let $\sigma \in \mathrm{Gal}(H/L)$ and consider the pair
$$\left(\mathrm{End}(E^\sigma \bmod \mathfrak{l}), \iota \colon \mathcal{O} \hookrightarrow \mathrm{End}(E^\sigma \bmod \mathfrak{l})\right).$$
By class field theory, $\mathrm{Gal}(H/L) \cong \mathrm{Pic}(\mathcal{O})$; let $\mathfrak{a} = \mathfrak{a}_\sigma$ be an invertible ideal that corresponds to σ; note that $\mathfrak{a}$ is unique as an element of $\mathrm{Pic}(\mathcal{O})$. We assume that $\mathfrak{a}$ is integral and coprime to the conductor. Since $\mathrm{Hom}(E^\sigma, E)$ is isomorphic to $\mathfrak{a}$ as a left $\mathrm{End}(E)$-module, we have $\mathrm{End}(E^\sigma \bmod \mathfrak{l}) = \mathfrak{a}\,\mathrm{End}(E)\mathfrak{a}^{-1}[\mathrm{CF67},\ \mathrm{Chap.\ XIII}]$. Thus, by Lemmas 6.5 and 6.9, the pair corresponding to E^σ is conjugate to $R(\mathfrak{a}_0\bar{\mathfrak{a}})$.

Now define
$$R_n(\mathfrak{a}) := \left\{ [\alpha,\beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\ell^{n-1}\mathfrak{D}^{-1}\bar{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda_{\mathfrak{a}}\beta \in \mathcal{O} \right\}, \quad \text{if } \ell \nmid d,$$
$$R_n(\mathfrak{a}) := \left\{ [\alpha,\beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\mathfrak{l}^{n}\mathfrak{D}^{-1}\bar{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda_{\mathfrak{a}}\beta \in \mathcal{O} \right\}, \qquad \text{if } \ell | d.$$

One can easily check that $R_1(\mathfrak{a}) = R(\mathfrak{a})$, that $\bigcap_n R_n(\mathfrak{a}) = \mathcal{O}$ and that
$$R_n(\mathfrak{a}) = \begin{cases} \mathcal{O} + \ell^{n-1}R_1(\mathfrak{a}) & \text{if } \ell \nmid d, \\ \mathcal{O} + \mathfrak{l}^{n-1}R_1(\mathfrak{a}), & \text{if } \ell | d. \end{cases} \tag{6.6}$$

Then by $[\mathrm{Gro86},\ \mathrm{Prop.\ 3.3}]$, $\mathrm{End}_{\mathbb{W}/\pi^n}(E^\sigma) \cong R_n(\mathfrak{a}_0\bar{\mathfrak{a}})$.

7. Proof of Theorem 3.2

Retain the notation from §3.2 and let $S_{n,m}(E)$ denote $S_{n,m}(E/\mathbb{W})$. In this section, we prove Theorem 3.2, which we restate here for the reader's convenience.

Theorem. *Assume that $\ell \nmid f_1$ and that $m \neq 0$. Then $\sum_{\tau_1} \#S_{n,m}(E(\tau_1)/\mathbb{W})$ is equal to an explicitly computable weighted sum of the number of certain invertible ideals of norm $\ell^{-r}m$, where $r = 2n - 1$ if $\ell \nmid d_1$ and $r = n$ otherwise. If, in addition, m and f_1 are relatively prime, then*
$$\sum_{\tau_1} \#S_{n,m}(E(\tau_1)/\mathbb{W}) = \frac{Cw_1}{2}\rho(m)\mathfrak{A}(\ell^{-r}m),$$
where $C = 1$ if $4m = d_1d_2$ and $C = 2$ otherwise,
$$\rho(m) = \begin{cases} 0 & \text{if } (d_1, -m)_p = -1 \text{ for } p|d_1, p \nmid f_1\ell, \\ 2^{\#\{p|(m,d_1):p\nmid f_2 \text{ or } p=\ell\}} & \text{otherwise}. \end{cases}$$
and
$$\mathfrak{A}(N) = \#\left\{ \mathfrak{b} \subseteq \mathcal{O}_{d_1} : \begin{array}{l} \mathrm{N}(\mathfrak{b}) = N,\ \mathfrak{b} \text{ invertible}, \\ p \nmid \mathfrak{b} \text{ for all } p|\gcd(N, f_2), p \nmid \ell d_1 \\ \mathfrak{p}^3 \nmid \mathfrak{b} \text{ for all } \mathfrak{p}|p|\gcd(N, f_2, d_1), p \neq \ell \end{array} \right\}.$$

Remark 7.1. In the general case, i.e. if m is not coprime to f_1, $\sum_{\tau_1} \#S_{n,m}(E(\tau_1))$ is still computable; in fact, the proof provides an algorithm.

Proof. If ℓ is split in $\mathcal{O}_{d_1}$, then the Hilbert symbol $(d_1, -m)_\ell = 1$. Therefore, by the proof of Theorem 1.1, $\sum_{\tau_1} \#S_{n,m}(E(\tau_1)) = 0$, and so each invertible ideal of norm $\ell^{-r}m$ is said to have weight 0. Now restrict to the case where m and f_1 are relatively prime. Since $(d_1, -m)_\infty = -1$, by class field theory, there exists a finite prime $p \neq \ell$ such that $(d_1, -m)_p = -1$. If p is

inert in $\mathbb{Q}(\sqrt{d_1})$ then this implies that $v_p(m) \equiv 1 \pmod{2}$ and thus $\mathfrak{A}(m\ell^{-r}) = 0$ for all r. If p is ramified in $\mathbb{Q}(\sqrt{d_1})$ then $\rho(m) = 0$. So we conclude that if ℓ is split in $\mathcal{O}_{d_1}$ then both sides are 0.

From now on we assume that the prime ℓ does not split in $\mathcal{O}_{d_1}$. Therefore, by §6.4, for every $[\tau_1]$ of discriminant d_1 there exists an integral invertible ideal $\mathfrak{a} = \mathfrak{a}_{\tau_1}$, such that $\mathrm{End}_{\mathbb{W}/\pi^n}(E(\tau_1)) \cong R_n(\mathfrak{a})$. Furthermore, the elements $\mathfrak{a}_{\tau_1}$ can be chosen in a way that is compatible with the Galois action; we will assume that this is the case. Since $R_n(\mathfrak{a}) \subset \mathbb{B}_{\ell,\infty}$, henceforth Tr, N, and disc will refer to the reduced trace, reduced norm, and reduced discriminant, respectively, in the quaternion algebra. With the identification of $\mathrm{End}_{\mathbb{W}/\pi^n}(E(\tau_1))$ with $R_n(\mathfrak{a})$, $S_{n,m}(E(\tau_1))$ consists of elements $[\alpha, \beta]$ in $R_n(\mathfrak{a})$ such that

$$\mathrm{Tr}([\alpha, \beta]) = d_2, \ \mathrm{N}([\alpha, \beta]) = \frac{1}{4}(d_2^2 - d_2), \ \mathrm{disc}(\mathcal{O}_{d_1} \oplus \mathcal{O}_{d_1}[\alpha, \beta]) = m^2,$$

and such that $\mathbb{Z} \oplus \mathbb{Z}[\alpha, \beta]$ in $(\mathbb{Q} \oplus \mathbb{Q}[\alpha, \beta]) \cap R(\mathfrak{a})$ has index a power of ℓ. Let t denote the trace of $\frac{1}{2}(d_1 + \sqrt{d_1})[\alpha, \beta]^{\vee}$. Then a calculation shows that $4m = d_1 d_2 - (d_1 d_2 - 2t)^2$, or equivalently that $t = \frac{1}{2}\left(d_1 d_2 \pm \sqrt{d_1 d_2 - 4m}\right)$. The values of $\mathrm{Tr}([\alpha, \beta])$ and $\mathrm{Tr}\left(\frac{1}{2}(d_1 + \sqrt{d_1})[\alpha, \beta]^{\vee}\right)$ imply that $\alpha = \frac{(d_1 d_2 - 2t) + d_2\sqrt{d_1}}{2\sqrt{d_1}}$, so α is uniquely determined by t. In turn, t is uniquely determined by m if $4m = d_1 d_2$, and otherwise t is determined by a choice of sign. Define

$$S_{n,m}^t(E) := \left\{ [\alpha, \beta] \in S_{n,m}(E) : \mathrm{Tr}\left(\frac{1}{2}(d_1 + \sqrt{d_1})[\alpha, \beta]^{\vee}\right) = t \right\},$$

where t and m satisfy $4m = d_1 d_2 - (d_1 d_2 - 2t)^2$. We will prove that $\sum_{\tau_1} \#S_{n,m}^t(E(\tau_1))$ is a weighted sum of integral ideals of norm m/ℓ^r and if $\gcd(m, f_1) = 1$ then $\sum_{\tau_1} \#S_{n,m}^t(E(\tau_1)) = \frac{w_1}{2}\rho(m)\mathfrak{A}(\ell^{-r}m)$. The theorem follows immediately from these two claims and the above discussion.

Proposition 7.2. *Let* $[\alpha, \beta] \in R_n(\mathfrak{a})$ *as above, and define* $\mathfrak{b} := \beta \mathfrak{r}^{-1} \mathfrak{D}\overline{\mathfrak{a}}^{-1}\mathfrak{a}$*, where* $\mathfrak{r} = \ell^{n-1}\mathfrak{q}^{-1}$ *if* ℓ *is inert in* $\mathcal{O}_{d_1}$ *and* $\mathfrak{r} = \mathfrak{l}^n \mathfrak{q}^{-1}$ *if* ℓ *is ramified. Then* $\mathfrak{b}$ *is an integral invertible ideal of* $\mathcal{O}_{d_1}$ *with the following properties*

$$\mathrm{N}(\mathfrak{b}) = m\ell^{-r}, \tag{7.1}$$

$$\mathfrak{b} \sim \mathfrak{r} \pmod{2\,\mathrm{Pic}(\mathcal{O}_{d_1})}. \tag{7.2}$$

(Recall that $r = 2n - 1$ is $\ell \nmid d_1$ and $r = n$ otherwise.)

Proof. By the definition of $R_n(\mathfrak{a})$, we see that $\beta \in \mathfrak{r}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}$ and since $\mathrm{N}([\alpha, \beta]) = \frac{1}{4}(d_2^2 - d_2)$ we deduce that β satisfies

$$\beta\overline{\beta} = \begin{cases} \frac{1}{\ell q}\left(\frac{1}{4}(d_2^2 - d_2) - \alpha\overline{\alpha}\right) & \text{if } \ell \text{ is inert in } \mathcal{O}_{d_1}, \\ \frac{1}{q}\left(\frac{1}{4}(d_2^2 - d_2) - \alpha\overline{\alpha}\right) & \text{if } \ell \text{ is ramified in } \mathcal{O}_{d_1}. \end{cases}$$

Since $\alpha = \left(d_1 d_2 - 2t + d2\sqrt{d_1}\right)/(2\sqrt{d_1})$ and $m = \frac{1}{4}\left(d_1 d_2 - (d_1 d_2 - 2t)^2\right)$, in both cases the formula simplifies to $\beta\overline{\beta} = \mathrm{N}(\mathfrak{r}\mathfrak{D}^{-1})m\ell^{-r}$. From these conditions, it is clear that $\mathfrak{b}$ is integral, invertible, has norm $m\ell^{-r}$, and is equal to $\mathfrak{r}$ in $\mathrm{Pic}(\mathcal{O}_{d_1})/2\,\mathrm{Pic}(\mathcal{O}_{d_1})$. $\square$

We obtain further conditions on the ideal $\mathfrak{b}$ by using the condition that the index of $\mathbb{Z} \oplus \mathbb{Z}[\alpha, \beta]$ in $(\mathbb{Q} \oplus \mathbb{Q}[\alpha, \beta]) \cap R(\mathfrak{a})$ is not divisible by any prime $p \neq \ell$.

Lemma 7.3. *Let p be a prime that divides $\gcd(m, f_2)$ and does not divide d_1. Then p divides the index of $\mathbb{Z} \oplus \mathbb{Z}\phi_{\mathfrak{ac}}$ in $(\mathbb{Q} \oplus \mathbb{Q}\phi_{\mathfrak{ac}}) \cap R(\mathfrak{ac})$ if and only if $\mathfrak{b} \subset p\mathcal{O}_{d_1}$.*

Proof. It is straightforward to show that a prime p' divides the index if and only if

$$\frac{d_2 - p'd_2}{2p'^2} + \frac{1}{p'}[\alpha, \beta] = \left[\frac{d_2 - p'd_2}{2p'^2} + \frac{d_1 d_2 - 2t + d_2\sqrt{d_1}}{2p'\sqrt{d_1}}, \frac{\beta}{p'} \right]$$

$$= \left[\frac{p'(d_1 d_2 - 2t) + d_2\sqrt{d_1}}{2p'^2\sqrt{d_1}}, \frac{\beta}{p'} \right] \in R(\mathfrak{a}) \otimes \mathbb{Z}_{p'}.$$

Consider a prime p satisfying the assumptions of the lemma. Since p divides m and f_2,

$$\alpha' := \frac{p(d_1 d_2 - 2t) + d_2\sqrt{d_1}}{2p\sqrt{d_1}} = \frac{1}{\sqrt{d_1}} \left(\frac{d_1 d_2(p-1) - 2tp}{2p} + \frac{d_2}{p}\frac{d_1 + \sqrt{d_1}}{2} \right) \in p\mathfrak{D}^{-1}.$$

If $\mathfrak{b} = \beta\mathfrak{r}\mathfrak{D}\overline{\mathfrak{a}}^{-1}\mathfrak{a} \subseteq p\mathcal{O}_{d_1}$, then we have that $\frac{\beta}{p} \in \mathfrak{r}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}$, and vice versa. As $p \nmid d_1$, this happens exactly when $\left[\frac{\alpha'}{p}, \frac{\beta}{p} \right] \in (R(\mathfrak{a}) \otimes \mathbb{Z}_p)$, which, as stated above, is equivalent to p dividing the index. $\square$

Lemma 7.4. *Let p be a prime that divides $\gcd(m, d_1, f_2)$ that does not divide ℓf_1. If $\mathfrak{b} \subset \mathfrak{p}^3\mathcal{O}_{d_1}$, where $\mathfrak{p}$ is the unique prime lying over p, then p divides the index of $\mathbb{Z} \oplus \mathbb{Z}\phi_{\mathfrak{ac}}$ in $(\mathbb{Q} \oplus \mathbb{Q}\phi_{\mathfrak{ac}}) \cap R(\mathfrak{ac})$.*

Proof. If $\mathfrak{b} \subset \mathfrak{p}^3\mathcal{O}_{d_1}$, then the same arguments as above show that $\alpha' \in p\mathfrak{D}^{-1}$ and $\beta \in \mathfrak{p}^3\mathfrak{r}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}$. To show that $[\alpha', \beta] \in p(R(\mathfrak{a}) \otimes \mathbb{Z}_p)$, we are left to show that $v_{\mathfrak{p}}(\alpha' - \lambda\beta) \geq 2$.

We first prove this when p is odd. Since $p \nmid f_1$, $v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}(\lambda\beta) \geq 3 - v_p(d) = 2$. Note that

$$\mathrm{N}(\alpha') = \frac{-1}{4p^2 d_1} \left(p^2(d_1 d_2 - 2t)^2 - d_2^2 d_1 \right) = \frac{m}{d_1} + \frac{d_2(d_2 - p^2)}{4p^2}.$$

Given that $p|f_2$ and $p||d_1$, we have $v_p(\mathrm{N}(\alpha')) \geq 2$ and so $v_{\mathfrak{p}}(\alpha') \geq 2$. By the strong triangle equality $v_{\mathfrak{p}}(\alpha' - \lambda\beta) \geq 2$.

Now consider the case when $p = 2$. As above, we have that $v_{\mathfrak{p}}(\beta) \geq 3 - v_p(d_1)$, which is non-negative. We may rewrite

$$\mathrm{N}(\alpha') = \frac{m}{d_1} + \frac{d_2}{4}\left(\frac{d_2}{4} - 1 \right). \tag{7.3}$$

Since $2|f_2$, 4 divides $\frac{d_2}{4}\left(\frac{d_2}{4} - 1 \right)$. Thus, either $v_{\mathfrak{p}}(\alpha'), v_{\mathfrak{p}}(\lambda\beta) \geq 2$, in which case the proof proceeds as above, or $v_{\mathfrak{p}}(\alpha') = v_{\mathfrak{p}}(\lambda\beta)$. Assume we are in the latter case. Since $\#\mathcal{O}/\mathfrak{p} = 2$, we have $v_{\mathfrak{p}}(\alpha' - \lambda\beta) > v_{\mathfrak{p}}(\lambda\beta) = v_{\mathfrak{p}}(\beta)$. This completes the proof unless $v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}(\alpha') = 0$. If $v_{\mathfrak{p}}(\beta) = 0$, then $v_p(d_1) = 3$ and $v_p(m) = 3$. By assumption, $(d_1, -m)_2 = (d_2, -m)_2 = 1$ so we must have that $\frac{d_2}{4} \equiv 1 \pmod{8}$. Thus, $\mathrm{N}(\alpha') \equiv \mathrm{N}(\beta) \pmod 8$. A calculation shows that this gives $v_{\mathfrak{p}}(\alpha' - \lambda\beta) \geq 2$. $\square$

Together, these two lemmas prove:

Proposition 7.5. *If there exists a prime $p|\gcd(m, f_2)$, $p \neq \ell$ such that either*

    (1) *p is inert in $\mathcal{O}_{d_1}$, or*
    (2) *$\gcd(p, f_1) = 1$ and p is ramified in $\mathcal{O}_{d_1}$ and $v_p(m) > 2$,*
then $S_{n,m}^t(E(\tau_1)) = \varnothing$ for all τ_1.

Proof. If $p|\gcd(m, f_2)$ and p is inert in $\mathcal{O}_{d_1}$ then any integral ideal $\mathfrak{b}$ with norm $m\ell^{-r}$ will be contained in $p\mathcal{O}_{d_1}$. Thus there are no embeddings of $\mathcal{O}_{d_1}$ which are optimal at p and thus the set $S_{n,m}^t(E(\tau_1))$ is empty.

Similarly, if $(p, f_1) = 1$ and p is ramified in $\mathcal{O}_{d_1}$, with $v_p(m) > 2$, then any integral ideal $\mathfrak{b}$ with norm $m\ell^{-r}$ will be divisible by $\mathfrak{p}^3$ and again there are no embeddings of $\mathcal{O}_{d_1}$ which are optimal at p. $\qquad\square$

We have obtained a map from $S_{n,m}^t(E(\tau_1))$ to invertible integral ideals in $\mathcal{O}_{d_1}$ satisfying conditions (7.1), (7.2), and the additional conditions:

$$\mathfrak{b} \nsubseteq p\mathcal{O}_{d_1}, \text{ for any } p|(m, f_2), p \neq \ell, p \nmid d_1 \tag{7.4}$$

$$\mathfrak{b} \nsubseteq \mathfrak{p}^3\mathcal{O}_{d_1}, \text{ for any } \mathfrak{p}|p|(d_1, m, f_2), p \neq \ell, p \nmid f_1. \tag{7.5}$$

Note that the codomain does not depend on $\mathfrak{a}$, and hence is independent of τ_1. Thus, we can extend the domain of the map to $\bigcup_{\tau_1} S_{n,m}^t(E(\tau_1))$.

Remark 7.6. Note that the codomain of the map is explicitly computable. This follows from the results in §5.

In the rest of the section, we will prove that for each ideal $\mathfrak{b}$ that satisfies (7.1),(7.2),(7.4) and (7.5), there is an algorithm that computes whether $\mathfrak{b} = \beta\mathfrak{r}^{-1}\mathfrak{D}\bar{\mathfrak{a}}^{-1}\mathfrak{a}$ for some $\beta, \mathfrak{a}$ such that $[\alpha, \beta] \in R(\mathfrak{a}) \cap S_{n,m}^t(E(\mathfrak{a}))$. If so, the algorithm also computes the size of the fiber lying over $\mathfrak{b}$, i.e. the number of pairs $(\beta, \mathfrak{a})$ such that the above condition holds. This will show that $\sum_{\tau_1} \#S_{n,m}^t(E(\tau_1))$ is a weighted sum on invertible integral ideals, namely each ideal satisfying (7.1),(7.2),(7.4) and (7.5) is weighted by the size of its fiber, and every ideal not satisfying one of (7.1),(7.2),(7.4) and (7.5) is weighted by 0. In the case where m is coprime to f_1, we will show that this weighted sum agrees with the formula given in the statement of Theorem 3.2.

Let $\mathfrak{b}$ be an invertible integral ideal satisfying (7.1) and (7.2). Since $\mathfrak{b} \sim \mathfrak{r} \pmod{2\operatorname{Pic}(\mathcal{O}_{d_1})}$, there exists an integral invertible ideal $\mathfrak{a}$, well-defined as an element of $\operatorname{Pic}(\mathcal{O}_{d_1})/(\operatorname{Pic}(\mathcal{O}_{d_1}))[2]$, and an element $\gamma_{\mathfrak{a}} \in \mathbb{Q}(\sqrt{d_1})$ such that $\mathfrak{b} = \gamma_{\mathfrak{a}}\mathfrak{r}^{-1}\mathfrak{a}\bar{\mathfrak{a}}^{-1}$. (Since $\operatorname{Pic}(\mathcal{O}_{d_1})$ is finite, there is an algorithm to find $\mathfrak{a}$, and thus an algorithm to compute $\gamma_{\mathfrak{a}}$.) For any $[\mathfrak{c}] \in \operatorname{Pic}(\mathcal{O}_{d_1})[2]$, let $\epsilon_{\bar{\mathfrak{c}}^2}/\operatorname{N}(\bar{\mathfrak{c}})$ be a principal generator for $\bar{\mathfrak{c}}/\mathfrak{c}$, and let $\gamma_{\mathfrak{a}\mathfrak{c}} := \gamma_{\mathfrak{a}}\epsilon_{\bar{\mathfrak{c}}^2}/\operatorname{N}(\bar{\mathfrak{c}})$. Then $\mathfrak{b}$ is also equal to $\gamma_{\mathfrak{a}\mathfrak{c}}\mathfrak{r}^{-1}\mathfrak{a}\mathfrak{c}(\bar{\mathfrak{a}\mathfrak{c}})^{-1}$. Let $\beta_{\mathfrak{a}\mathfrak{c}} = \gamma_{\mathfrak{a}\mathfrak{c}}/\sqrt{d_1}$. Since $\mathfrak{b}$ is integral, $\beta_{\mathfrak{a}\mathfrak{c}} \in \mathfrak{r}\mathfrak{D}^{-1}\overline{\mathfrak{a}\mathfrak{c}}(\mathfrak{a}\mathfrak{c})^{-1}$.

By the arguments at the beginning of the proof of Proposition 7.2, we see that if $\mathfrak{b}$ is the image of an element in $R(\mathfrak{a}\mathfrak{c})$, then the element must be of the form

$$\phi_{\mathfrak{a}\mathfrak{c}} := \left[\frac{(d_1 d_2 - 2t) + d_2\sqrt{d_1}}{2\sqrt{d_1}}, \omega\beta_{\mathfrak{a}\mathfrak{c}}\right],$$

where $\omega \in \mathcal{O}_{d_1}^\times$. As $\alpha := \frac{(d_1 d_2 - 2t) + d_2\sqrt{d_1}}{2\sqrt{d_1}} \in \mathfrak{D}^{-1}$ and $\omega\beta_{\mathfrak{a}\mathfrak{c}} \in \mathfrak{r}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}\mathfrak{c}}(\mathfrak{a}\mathfrak{c})^{-1}$, it is left to determine

(1) if $\alpha - \omega\lambda_{\mathfrak{a}\mathfrak{c}}\beta_{\mathfrak{a}\mathfrak{c}} \in \mathcal{O}_{d_1}$, and
(2) if $\mathbb{Z} \oplus \mathbb{Z}\phi_{\mathfrak{a}\mathfrak{c}}$ in $(\mathbb{Q} \oplus \mathbb{Q}\phi_{\mathfrak{a}\mathfrak{c}}) \cap R(\mathfrak{a}\mathfrak{c})$ has index a power of ℓ.

If both conditions hold, then $\mathfrak{b}$ is the image of $\phi_{\mathfrak{a}\mathfrak{c}} \in R(\mathfrak{a}\mathfrak{c})$.

We first calculate the number of $\phi_{\mathfrak{a}\mathfrak{c}}$ satisfying Condition (1).

24

Condition (1): Henceforth, we will assume, without loss of generality, that $\mathfrak{a}$ and $\mathfrak{c}$ are coprime to d_1. As a result, we have $\lambda_{\mathfrak{ac}} = (\prod_{\mathfrak{p}|\mathfrak{c}} M(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{c})})\lambda_\mathfrak{a} \equiv \lambda_\mathfrak{a} \pmod{d_1}$. Thus

$$\omega \lambda_{\mathfrak{ac}} \gamma_{\mathfrak{ac}} \equiv \omega(\epsilon_{\bar{\mathfrak{c}}^2}(\prod_{\mathfrak{p}|\mathfrak{c}} M(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{c})})/\operatorname{N}(\mathfrak{c}))\lambda_\mathfrak{a}\gamma_\mathfrak{a} \pmod{\mathfrak{D}}.$$

Since $\alpha - \omega\lambda_{\mathfrak{ac}}\beta_{\mathfrak{ac}} \in \mathcal{O}_{d_1}$ if and only if $\alpha\sqrt{d_1} - \omega\lambda_{\mathfrak{ac}}\gamma_{\mathfrak{ac}} \in \mathfrak{D}$, this in turn occurs if and only if

$$a - \omega(\epsilon_{\bar{\mathfrak{c}}^2}(\prod_{\mathfrak{p}|\mathfrak{c}} M(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{c})})/\operatorname{N}(\mathfrak{c}))\lambda_\mathfrak{a}\gamma_\mathfrak{a} \in \mathfrak{D},$$

where $a := \alpha\sqrt{d_1}$. Note that $\operatorname{N}(\lambda_\mathfrak{a}\gamma_\mathfrak{a}) \equiv \operatorname{N}(a) \pmod{d_1}$ and that $\omega\epsilon_{\bar{\mathfrak{c}}^2}(\prod_{\mathfrak{p}|\mathfrak{c}} M(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{c})})/\operatorname{N}(\bar{\mathfrak{c}})$ has norm congruent to 1 modulo d_1. To complete the proof, we need the following two lemmas. The first lemma shows that, as $\mathfrak{c}$ ranges over all elements of $\operatorname{Pic}(\mathcal{O})[2]$ and ω ranges over all elements of $\mathcal{O}^\times$, the element $(\epsilon_{\bar{\mathfrak{c}}^2}(\prod_{\mathfrak{p}|\mathfrak{c}} M(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{c})})/\operatorname{N}(\mathfrak{c}))\omega$ ranges over all congruences classes modulo $\mathfrak{D}$ that have norm congruent to 1 $\pmod{d}$. The second lemma counts the number of such congruence classes of elements γ such that $\alpha - \gamma\beta \in \mathcal{O}_{d_1}$.

Lemma 7.7. *Let $\mathcal{O} = \mathcal{O}_d$. Then the morphism*

$$\operatorname{Pic}(\mathcal{O})[2] \longrightarrow \frac{\{\gamma \in (\mathcal{O}/\mathfrak{D})^\times : \operatorname{N}(\gamma) \equiv 1 \bmod d\}}{\mathcal{O}^\times}$$

that sends $[\mathfrak{c}] \mapsto \epsilon_{\mathfrak{c}^2}\prod_{\mathfrak{p}|\mathfrak{c}} M(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{c})}/\operatorname{N}(\mathfrak{c})$, where $\mathfrak{c}$ is any integral representative coprime to $\mathfrak{D}$, is an isomorphism.

Proof. An easy computation shows that the map is a well-defined group homomorphism. We will show that the groups have the same cardinality, and then show that the map is surjective. When $d = -3$ or -4, one can check that both sides are trivial. Henceforth we assume that $d < -4$ so that $\mathcal{O}^\times = \pm 1$.

The exact sequence

$$0 \to \operatorname{Pic}(\mathcal{O})[2] \to \operatorname{Pic}(\mathcal{O}) \xrightarrow{\times 2} \operatorname{Pic}(\mathcal{O}) \to \operatorname{Pic}(\mathcal{O})/2\operatorname{Pic}(\mathcal{O}) \to 0$$

shows that $\#\operatorname{Pic}(\mathcal{O})[2] = \#(\operatorname{Pic}(\mathcal{O})/2\operatorname{Pic}(\mathcal{O}))$, which by [Cox89, Prop. 3.11 & Thm 7.7] is equal to 2^{k-1} (see §5 for the definition of k). Let $\gamma := \gamma_0 + \gamma_1\frac{d+\sqrt{d}}{2} \in \mathcal{O}$ be such that $\operatorname{N}(\gamma) \equiv \gamma_0^2 + \frac{d(d-1)}{4}\gamma_1^2 \equiv 1 \pmod{d}$. We need to determine the number of γ modulo $\mathfrak{D}$ that satisfy this equation. For each odd prime $p|d$, we have 2 choices for $\gamma \bmod \mathfrak{D}_p$, namely $\gamma \equiv \pm 1 \bmod \mathfrak{D}_p$. When $p = 2|d$ we have the following possibilities

$$
\begin{array}{ll}
d \equiv 4 \pmod{16} & \gamma \equiv 1 \bmod \mathfrak{D}_2, \\
d \equiv 12 \pmod{16} & \gamma \equiv 1, \text{ or } \frac{1}{2}(d + \sqrt{d}) \bmod \mathfrak{D}_2, \\
v_2(d) = 3 \text{ or } 4 & \gamma \equiv \pm 1 \bmod \mathfrak{D}_2, \\
v_2(d) \geq 5 & \gamma \equiv \pm 1 \bmod \mathfrak{D}_2 \text{ or } \gamma \equiv \frac{1}{2}(d + \sqrt{d} \pm \sqrt{4 + d}) \bmod \mathfrak{D}_2.
\end{array}
$$

Note that if $v_2(d) \geq 5$ then $1 + d/4 \equiv 1 \pmod{8}$ so $\frac{1}{2}\sqrt{4+d}$ exists modulo $2^{v(d)-1}$. This case-by-case analysis shows

$$\#\left\{\gamma \in \mathcal{O}/\sqrt{d} : \operatorname{N}(\gamma) \equiv 1 \pmod{d}\right\} = 2^k,$$

and so the quotient by ± 1 has cardinality 2^{k-1}.

25

Proof of surjectivity: Fix a nontrivial $\gamma := \gamma_0 + \gamma_1 \frac{d+\sqrt{d}}{2}$ in the codomain, i.e. γ is such that $\gamma_0^2 + d\gamma_0\gamma_1 + \gamma_1^2 \frac{d^2-d}{4} \equiv 1 \bmod d$ and $\gamma \not\equiv 1 \bmod \mathfrak{D}$. Then fix non-zero values of $e_0, e_1 \in \mathbb{Z}$ and a positive integer N coprime to d such that

$$e_0^2 + de_0e_1 + e_1^2 \frac{d^2-d}{4} = N^2, \quad e_0 \equiv N\gamma_0 \pmod{\frac{d}{(2,d)}}, \quad e_1 \equiv N\gamma_1 \pmod{(2,d)}.$$

(This is possible because conics satisfy weak approximation.) Define $\epsilon := \frac{1}{(e_0,e_1)}\left(e_0 + e_1\frac{d+\sqrt{d}}{2}\right)$. Then $\mathrm{N}(\epsilon) = \left(\frac{N}{(e_0,e_1)}\right)^2$, and since $p \nmid \epsilon$, ϵ must generate a square ideal, say $\mathfrak{c}^2$. Additionally, $N = \mathrm{N}(\mathfrak{c})(e_0,e_1)$. Therefore, $[\mathfrak{c}] \mapsto \gamma$, thus completing the proof of surjectivity and of the Lemma. $\qquad\square$

Lemma 7.8. *Fix $a, b \in \mathcal{O}_d$. Assume that $\mathrm{N}(a) \equiv \mathrm{N}(b) \pmod{d}$. If $\mathrm{N}(a)$ is coprime to the conductor f of d, then there exists an element $c \in \mathcal{O}$, such that*

$$\mathrm{N}(c) \equiv 1 \pmod{d} \text{ and } a - cb \in \mathfrak{D}. \tag{7.6}$$

Moreover, regardless of whether $\mathrm{N}(a)$ is coprime to f, if there exists $c \in \mathcal{O}$ satisfying (7.6), then the number of such c modulo $\mathfrak{D}$ equals $\widetilde{\rho}_d(a_0, a_1)$ where $a := a_0 + a_1\frac{d+\sqrt{d}}{2}$,

$$\widetilde{\rho}_d^{(2)}(s,t) := \left\{ \begin{array}{ll} 2 & \text{if } d \equiv 12 \bmod 16, s \equiv t \bmod 2 \\ & \text{or if } 8 \mid d, v(s) \geq v(d) - 2 \\ 1 & \text{otherwise} \end{array} \right\} \cdot \left\{ \begin{array}{ll} 2 & \text{if } 32 \mid d, 4 \mid (s - 2t) \\ 1 & \text{otherwise} \end{array} \right\}$$

$$\widetilde{\rho}_d(s,t) := \widetilde{\rho}_d^{(2)}(s,t) \cdot 2^{\#\{p: v_p(s) \geq v_p(d) > 0, p \neq 2\}}.$$

Remark 7.9. If $\mathrm{N}(a)$ is coprime to f, then $\widetilde{\rho}_d(a_0, a_1)$ has a simpler expression; it is equal to $2^{\#\{p: p \mid (d, \mathrm{N}(a))\}}$.

Proof. First we will prove existence of c in the case where $\mathrm{N}(a)$ is coprime to the conductor. Write $a := a_0 + a_1\frac{d+\sqrt{d}}{2}$ and $b := b_0 + b_1\frac{d+\sqrt{d}}{2}$. By our assumption on $\mathrm{N}(a), \mathrm{N}(b)$, we see that $a_0^2 \equiv b_0^2 \pmod{p^{v(d)}}$ for all odd p and that $a_0^2 - \frac{d}{4}a_1^2 \equiv b_0^2 - \frac{d}{4}b_1^2 \pmod{2^{v(d)}}$. Since $\mathrm{N}(a)$ is coprime to the conductor, we get that $a_0 \equiv \pm b_0 \pmod{p^{v(d)}}$ for all odd primes. From the description of the elements of norm 1 mod d in the proof of Lemma 7.7, it is clear that there is a c, with $\mathrm{N}(c) \equiv 1 \pmod{d}$ such that $a \equiv bc \pmod{\mathfrak{D}_p}$ for all odd p.

It remains to show that if $2 \mid d$, then there is such a c that satisfies $a \equiv bc \pmod{\mathfrak{D}_2}$. The norm congruence as well as the co-primality assumption shows

(1) If $d \equiv 12 \bmod 16$, then either $a_0 \equiv a_1 \pmod 2$ and $b_0 \equiv b_1 \pmod 2$ (when $\mathrm{N}(a) \equiv 0 \pmod 2$) or $a_0 \not\equiv a_1 \pmod 2$ and $b_0 \not\equiv b_1 \pmod 2$ ($\mathrm{N}(a) \equiv 1 \pmod 2$).
(2) If $v_2(d) = 8$, then $a_0 \equiv \pm b_0 \pmod 4$ and $a_1 \equiv b_1 \pmod 2$.

The description of possible $c \in \mathcal{O}$ such that $\mathrm{N}(c) \equiv 1 \pmod d$ given in Lemma 7.7 completes the proof of existence.

Henceforth we assume that there exists a $c \in \mathcal{O}$ such that $\mathrm{N}(c) \equiv 1 \pmod d$ and $a \equiv bc \pmod{\mathfrak{D}}$. Since $\mathrm{N}(c) \equiv 1 \pmod d$ we may replace b with bc and assume that $a \equiv b \pmod{\mathfrak{D}}$.

Let $c' = c_0' + c_1'\frac{d+\sqrt{d}}{2} \in \mathcal{O}$ be such that $a \equiv c'b \pmod{\mathfrak{D}}$. Since $a \equiv b \pmod{\mathfrak{D}}$, we must have $(c' - 1)b \in \mathfrak{D}$ and $\mathrm{N}(c') \equiv 1 \pmod d$. Therefore for all odd primes $p \mid d$, either $c_0' \equiv 1 \pmod{p^{v(d)}}$ or $v_p(b_0) \geq v_p(d)$, and hence $v_p(a_0) \geq v_p(d)$. So for odd p, there are 2 choices for c' modulo $\mathfrak{D}_p$ if $v_p(a_0) \geq v_p(d)$ and otherwise c' is uniquely determined modulo $\mathfrak{D}_p$.

Now let $p = 2$. Then we have the following possibilities for c'

$$
\begin{array}{ll}
d \equiv 4 \pmod{16} & c' \equiv 1 \bmod \mathfrak{D}_2 \\
d \equiv 12 \pmod{16} & \text{either } c' \equiv 1 \bmod \mathfrak{D}_2, \text{ or} \\
 & c' \equiv \tfrac{1}{2}(d + \sqrt{d}) \bmod \mathfrak{D}_2, \text{ and } a_0 \equiv a_1 \pmod 2, \\
v_2(d) = 3 \text{ or } 4 & \text{either } c' \equiv 1 \bmod \mathfrak{D}_2, \text{ or} \\
 & c' \equiv -1 \bmod \mathfrak{D}_2, \text{ and } v_p(b_0), v_p(a_0) \geq v_p(d) - 2, \\
v_2(d) \geq 5 & \text{either } c' \equiv 1 \bmod \mathfrak{D}_2, \text{ or} \\
 & c' \equiv -1 \bmod \mathfrak{D}_2, \text{ and } v_p(b_0), v_p(a_0) \geq v_p(d) - 2, \text{ or} \\
 & c' \equiv \tfrac{1}{2}(d + \sqrt{d} \pm \sqrt{4+d}) \bmod \mathfrak{D}_2 \text{ and } a_0 \equiv 2a_1 \pmod 4.
\end{array}
$$

In the last case, when $v_2(d) \geq 5$, if $a_0 \equiv 2a_1 \pmod 4$ *and* $v_p(a_0) \geq v_p(d) - 2$, then c' may take on all values modulo $\mathfrak{D}_2$ that have norm congruent to 1 modulo d. This case-by-case analysis shows that there are $\widetilde{\rho}_d^{(2)}(a_0, a_1)$ choices for c' modulo $\mathfrak{D}_2$. This completes the proof. $\qquad\square$

Remark 7.10. The assumption that $\mathrm{N}(a)$ is coprime to the conductor in Lemma 7.8 is crucial for the existence of c. Let's assume that p divides the conductor and $v_p(d) = 2$. Then if $p^2 \mid \mathrm{N}(a)$, the congruence $a_0^2 \equiv b_0^2 \pmod{p^2}$, only implies that $a_0 \equiv b_0 \equiv 0 \pmod p$, *not* that $a_0 \equiv \pm b_0 \pmod{p^2}$, which is what is needed to prove existence.

Now we return to the proof of the theorem. Recall that we are determining for which $[\mathfrak{c}] \in \mathrm{Pic}(\mathcal{O})[2]$ we have

(1) $\alpha - (\epsilon_{\bar{\mathfrak{c}}^2}/\mathrm{N}(\bar{\mathfrak{c}}))\omega\lambda_{\mathfrak{a}}\beta_{\mathfrak{a}} \in \mathcal{O}_{d_1}$, and
(2) $\mathbb{Z} \oplus \mathbb{Z}\phi_{\mathfrak{ac}}$ in $(\mathbb{Q} \oplus \mathbb{Q}\phi_{\mathfrak{ac}}) \cap R(\mathfrak{ac})$ has index a power of ℓ.

Assume that there exists a $[\mathfrak{c}] \in \mathrm{Pic}(\mathcal{O})$ and $\omega \in \mathcal{O}_{d_1}^{\times}$ such that (1) holds. Then Lemmas 7.7 and 7.8 show that there are $\widetilde{\rho}_d(-t, d_2)$ elements of $\mathrm{Pic}(\mathcal{O})[2]$ and $\frac{w_1}{2}$ choices for ω such that (1) is satisfied. In addition, the proofs of Lemmas 7.7 and 7.8 give an algorithm for testing whether there exists a $[\mathfrak{c}] \in \mathrm{Pic}(\mathcal{O})$ and $\omega \in \mathcal{O}_{d_1}^{\times}$ such that (1) holds.

Remark 7.11. If m and f_1 are coprime, then the proofs of these lemmas also show that there does exist a $[\mathfrak{c}] \in \mathrm{Pic}(\mathcal{O})$ and $\omega \in \mathcal{O}_{d_1}^{\times}$ such that (1) holds.

Condition (2): Now we determine which of these $\frac{w_1}{2}\widetilde{\rho}_d(-t, d_2)$ elements also have the desired index. Condition (2) is satisfied if and only if $\mathbb{Z}[\phi_{\mathfrak{ac}}]$ is optimally embedded in $R(\mathfrak{ac})$ at every prime $p \neq \ell$.

From the proof of Lemma 7.3, we see that the only primes different from ℓ that can divide the index of $\mathbb{Z} \oplus \mathbb{Z}\phi_{\mathfrak{ac}}$ in $(\mathbb{Q} \oplus \mathbb{Q}\phi_{\mathfrak{ac}}) \cap R(\mathfrak{ac})$ are the primes p that divide $\gcd(m, f_2)$. If p is such a prime that does not divide d_1, then for any preimage of an invertible ideal $\mathfrak{b}$ satisfying conditions (7.1), (7.2), (7.4), (7.5), Lemma 7.3 ensures that p does not divide the index. So if the gcd of m, d_1, and f_2 is trivial, then the size of the fiber is equal to the number of elements satisfying condition (1), which was shown above to be either 0 or $\frac{w_1}{2}\widetilde{\rho}_d(-t, d_2)$.

Now consider the case that there exists a prime $p \mid \gcd(m, d_1, f_2)$, $p \neq \ell$. Then we have $v_p(m) \geq 2$. If $p \nmid f_1$, then Lemma 7.4 shows that $v_p(m) = 2$ and the condition on the index is equivalent to determining whether

$$
\alpha' - (\epsilon_{\bar{\mathfrak{c}}^2}/\mathrm{N}(\bar{\mathfrak{c}}))\omega\lambda_{\mathfrak{a}}\beta_{\mathfrak{a}} \notin p\mathcal{O}_{d_1}, \quad \text{where } \alpha' := \frac{p(d_1 d_2 - 2t) + d_2\sqrt{d_1}}{2p\sqrt{d_1}}.
$$

Note that the norm of $\alpha'\sqrt{d_1}$ (see (7.3)) and the norm of $\sqrt{d_1}\omega\lambda_{\mathfrak{a}}\beta_{\mathfrak{a}}$ are both congruent to $-\ell^r m$ modulo $p^{2+v_p(d_1)}$. This is a stronger congruence than the one between $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$

27

that we used to invoke Lemma 7.8. This stronger congruence allows us to show that exactly half of the $\frac{w_1}{2}\widetilde{\rho}_d(-t,d_2)$ elements of $\mathrm{Pic}(\mathcal{O})[2]$ are such that $\alpha' - (\epsilon_{\bar{c}^2}/\mathrm{N}(\bar{c}))\omega\lambda_{\mathfrak{a}}\beta_{\mathfrak{a}} \notin p\mathcal{O}_{d_1}$. (One proves this by using arguments almost identical to those in Lemma 7.8.) Furthermore, at each prime, these conditions are independent. So for each prime dividing $\gcd(m,d_1,f_2)$, the size of the fiber consisting of elements satisfying both Conditions (1) and (2), is divided in half.

In summary, the number of $[\mathfrak{c}] \in \mathrm{Pic}(\mathcal{O})[2]$ and $\omega \in \mathcal{O}_{d_1}^{\times}$ that satisfy conditions (1) and (2) above is bounded above by $\frac{w_1}{2}\widetilde{\rho}_d(-t,d_2)2^{-\#\{p\,|\,(m,d_1,f_2),\,p\nmid\ell f_1\}}$, with equality if $\gcd(m,f_1)=1$. If m is not coprime to the conductor (in which case $w_1=2$), then the number of $[\mathfrak{c}]$ is either 0, or is of the form 2^k with

$$\#\{p : p|\gcd(m,d_1), p\nmid f_1f_2\} \le k \le v_2(\widetilde{\rho}_d(-t,d_2)) - \#\{p|\gcd(m,d_1,f_2), p\nmid\ell f_1\}.$$

This proves that $\sum_{\tau_1} \#S_{n,m}^t(E(\tau_1))$ is a weighted sum of ideals with a fixed norm, and the proof gives an algorithm for computing this weighted sum.

From now on assume that $\gcd(m,f_1)=1$. So far we have shown that

$$\sum_{\tau_1}\#S_{n,m}^t(E(\tau_1)) = \frac{w_1\widetilde{\rho}_d(-t,d_2)}{2^{1+\#\{p|\gcd(m,d_1,f_2),p\neq\ell\}}} \cdot \#\left\{\mathfrak{b}\subseteq\mathcal{O} : \text{satisfying } (7.1),(7.2),(7.4),(7.5)\right\}.$$

Note that it follows from Corollary 5.2 that an ideal $\mathfrak{b}$ of norm $\ell^{-r}m$ satisfies $\mathfrak{b} \sim \mathfrak{r}$ $(\mathrm{mod}\ 2\,\mathrm{Pic}(\mathcal{O}_{d_1}))$ if and only if $\widehat{\Psi}_\ell(m\ell^{-r}\,\mathrm{N}(\mathfrak{r})) = \mathbf{1}$. In particular, either all ideals of norm $\ell^{-r}m$ satisfy (7.2), or none do. Therefore

$$\#\left\{\mathfrak{b}\subseteq\mathcal{O} : \text{satisfying } (7.1),(7.2),(7.4),(7.5)\right\} = \begin{cases} \mathfrak{A}(m\ell^{-r}) & \text{if } \widehat{\Psi}_\ell(m\ell^{-r}\,\mathrm{N}(\mathfrak{r})) = \mathbf{1}, \\ 0 & \text{otherwise.} \end{cases}$$

By the definition of q in §6, $m\ell^{-r}\,\mathrm{N}(\mathfrak{r}) = -m$ in $\mathbb{Z}/f_1\mathbb{Z}$. Since m is coprime to f_1, $-m$ is congruent to a non-zero square modulo f_1 and so $\Psi_p(-m)=1$ for all $p|f_1$. (Recall from §5 that if $p|d_1$ and $p\nmid f_1$, then $\Psi_p(-m)=(d_1,-m)_p$.) Therefore

$$\#\left\{\mathfrak{b}\subseteq\mathcal{O} : \text{satisfying } (7.1),(7.2),(7.4),(7.5)\right\} = \begin{cases} \mathfrak{A}(m\ell^{-r}) & \text{if } \rho(m)\neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

By Remark 7.9, we know that

$$\frac{w_1\widetilde{\rho}_d(-t,d_2)}{2^{1+\#\{p|\gcd(m,d_1,f_2),p\neq\ell\}}} = \frac{w_1}{2}2^{\#\{p|\gcd(m,d_1):p\nmid f_2 \text{ or } p=\ell\}},$$

which completes the proof. $\qquad\square$

Proposition 7.12. *Fix a prime ℓ and a positive integer m of the form $\frac{1}{4}(d_1d_2-x^2)$. Assume that m and f_1 are coprime. Then*

$$\rho(m)\mathfrak{A}(\ell^{-r}m) = \varepsilon_\ell(\ell^{-r}m)\prod_{p|m,p\neq\ell}\begin{cases} 1+v_p(m) & \left(\frac{d_1}{p}\right)=1, p\nmid f_2, \\ 2 & \left(\frac{d_1}{p}\right)=1, p|f_2, \\ \frac{1}{2}\left(1+(-1)^{v_p(m)}\right) & \left(\frac{d_1}{p}\right)=-1, p\nmid f_2, \\ 2 & p|d_1,(d_1,-m)_p=1, p\nmid f_2 \\ 1 & p|d_1,(d_1,-m)_p=1, p|f_2, v_p(m)\leq 2 \\ 0 & \text{otherwise,} \end{cases}$$

28

where

$$\varepsilon_\ell(N) = \begin{cases} 0 & \text{if either } N \notin \mathbb{Z} \text{ or } \ell \nmid d_1 \text{ and } v_\ell(N) \equiv 1 \pmod 2, \\ 2 & \text{if } N \in \mathbb{Z} \text{ and } \ell | d_1, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Recall that

$$\rho(m) = \begin{cases} 0 & \text{if } (d_1, -m)_p = -1 \text{ for } p|d_1, p \neq \ell d_1, \\ 2^{\#\{p|\gcd(m,d_1):p\nmid f_2 \text{ or } p=\ell\}} & \text{otherwise,} \end{cases}$$

and

$$\mathfrak{A}(N) = \# \left\{ \mathfrak{b} \subseteq \mathcal{O}_{d_1} : \begin{array}{l} N(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible}, \\ p \nmid \mathfrak{b} \text{ for all } p|\gcd(N, f_2), p \nmid \ell d_1 \\ \mathfrak{p}^3 \nmid \mathfrak{b} \text{ for all } \mathfrak{p}|p|\gcd(N, f_2, d_1), p \neq \ell \end{array} \right\}.$$

If $\ell^{-r}m$ is not an integer, then one can easily see that both sides are 0. One can also check that both sides are 0 if $v_\ell(\ell^{-r}m) \equiv 1 \pmod 2$ and $\ell \nmid d_1$. So we may assume that $v_\ell(m) \geq r$ and that if $v_\ell(\ell^{-r}m) \equiv 1 \pmod 2$ then $\ell | d_1$.

Under these assumptions, it is an exercise to show that the number of invertible integral ideals $\mathfrak{b}$ of norm $\ell^{-r}m$ is equal to

$$\prod_{p|m, p\nmid \ell d_1} \begin{cases} 1 + v_p(m) & \text{if } \left(\frac{d_1}{p}\right) = 1, \\ \frac{1}{2}(1 + (-1)^{v_p(m)}) & \text{if } \left(\frac{d_1}{p}\right) = -1, \end{cases}$$

(here we use that ℓ is not split in $\mathcal{O}_{d_1}$.) If we impose the condition that $p \nmid \mathfrak{b}$ for all $p|\gcd(m\ell^{-r}, f_2), p \nmid \ell d_1$, then for any $p|f_2, p \nmid d_1\ell$ the local factor becomes 0 if p is inert in $\mathcal{O}_{d_1}$ and 2 if p is split. If we additionally assume that $\mathfrak{p}^3 \nmid \mathfrak{b}$ for all $\mathfrak{p}|p|\gcd(\ell^{-r}m, f_2, d_1), p \neq \ell$, then we introduce a local factor at p that is 0 when $p|d_1, p \neq \ell$ and $v_p(m) \geq 3$. In summary, we have

$$\mathfrak{A}(\ell^{-r}m) = \prod_{p|m, p\neq \ell} \begin{cases} 1 + v_p(m) & \text{if } \left(\frac{d_1}{p}\right) = 1, p \nmid f_2, \\ 2 & \text{if } \left(\frac{d_1}{p}\right) = 1, p | f_2, \\ \frac{1}{2}\left(1 + (-1)^{v_p(m)}\right) & \text{if } \left(\frac{d_1}{p}\right) = -1, p \nmid f_2, \\ 0 & \text{if } \left(\frac{d_1}{p}\right) = -1, p | f_2, \\ 0 & \text{if } p|(d_1, f_2), v_p(m) \geq 3, \\ 1 & \text{otherwise.} \end{cases} \tag{7.7}$$

It is clear from the definition of $\rho(m)$ that

$$\rho(m) = \prod_{p|\gcd(d_1,m)} \begin{cases} 0 & \text{if } (d_1, -m)_p = -1, p \neq \ell, \\ 1 & \text{if } (d_1, -m)_p = 1, p|f_2, p \neq \ell \\ 2 & \text{otherwise.} \end{cases}$$

Combining these products completes the proof. ∎

8. Relating S_n^{Lie} to S_n

We retain the notation from the previous sections. In this section we prove the following proposition.

Proposition 8.1. *Assume that d_1 is fundamental at ℓ and that either $\ell > 2$ or $\gcd(d_1, \widetilde{d_2})$ is odd. Fix $[\tau_1]$ of discriminant d_1, and let m be a nonnegative integer divisible by ℓ. Then if $\ell | f_2$, we have:*

$$\#S_{1,m}^{\mathrm{Lie}}(E(\tau_1)/A) = \begin{cases} \frac{1}{2}\#S_{1,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell \nmid \widetilde{d_2}, \\ \#S_{1,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell | \widetilde{d_2}, \end{cases}$$

and if $\ell \nmid f_2$, we have:

$$\sum_n \#S_{n,m}^{\mathrm{Lie}}(E(\tau_1)/A) = \begin{cases} \frac{1}{2}\sum_n \#S_{n,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell | d_1 \text{ or } \ell \nmid \widetilde{d_2}, \\ \sum_n \#S_{n,m}(E(\tau_1)/\mathbb{W}) & \text{if } \ell \nmid d_1, \ell | \widetilde{d_2}. \end{cases}$$

We first prove a lemma which will be useful in the proof of Proposition 8.1. Recall that if $S_{n,m}(E) \neq \emptyset$ for some elliptic curve E, then by §7, $m = \frac{1}{4}\left(d_1 d_2 - (d_1 d_2 - 2t)^2\right)$, where $2t = \mathrm{Tr}((d_1 + \sqrt{d_1})\phi^\vee)$ for some $\phi \in S_{n,m}(E)$.

Lemma 8.2. *Assume that $s_2 = 0$. If $S_{1,m}(E(\tau_1)) \neq \emptyset$ for some τ_1 of discriminant d_1 then $v_\ell(m) = 1$ if $\ell | d_1 \widetilde{d_2}$ and $\ell \nmid \gcd(d_1, \widetilde{d_2})$, and $v_\ell(m) > 1$ if $\ell | \gcd(d_2, \widetilde{d_2})$ and $\ell \neq 2$.*

Proof. This follows from a simple calculation. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Proof of Proposition 8.1. Write E for $E(\tau_1)$. Recall that

$$S_{n,m}^{\mathrm{Lie}}(E/A) = \left\{ \phi \in S_{n,m}(E/A) : c(\phi) = \delta, \text{ and } c(\widetilde{\phi}) \equiv \widetilde{\delta} \bmod \mu \right\}.$$

Assume first that $m = 0$. Then $d_2 = d_1 \ell^{2s_2}$, $\widetilde{d_2} = d_1$, and we may assume that $\widetilde{\delta} = \frac{1}{2}(d_1 + \sqrt{d_1})$. Since $S_{1,m}(E(\tau_1)) = \{\frac{1}{2}(\ell^{2s_2}d_1 \pm \ell^{s_2}\sqrt{d_1})\}$, $\#S_{1,m}^{\mathrm{Lie}}(E) = \frac{1}{2}\#S_{1,m}(E)$ if $\ell \nmid d_1$ and $\#S_{1,m}^{\mathrm{Lie}}(E) = \#S_{1,m}(E)$ if $\ell | d_1$.

Henceforth we assume that $m > 0$. In this case E must be supersingular and we may embed $\mathrm{End}(E)$ into $\mathrm{M}_2(\mathbb{Q}(\sqrt{d_1}))$ as described in §6.

Let $\phi \in S_{n,m}(E/\mathbb{W})$; then $v_\ell(m) \geq 2n - 1$ if $\ell \nmid d_1$ and $v_\ell(m) \geq n$ if $\ell | d_1$. To determine if $\phi \in S_{n,m}^{\mathrm{Lie}}(E)$, we must determine $c(\phi)$ and $c(\widetilde{\phi})$. Since c factors through the formal group, we will consider elements in $\mathbb{B}_{\ell,\infty} \cap \mathbb{Z}_\ell \otimes \mathrm{End}_{A/\mu^r}(E)$. By the theory of complex multiplication, we know that $c([\alpha, 0]) = \alpha$ for any $\alpha \in \mathcal{O}$. Since c is a homomorphism, we have

$$(c(\phi) - \delta)(c(\phi^\vee) - \delta) = \frac{1}{4}(d_2^2 - d_2) - d_2\delta + \delta^2 = 0,$$

and similarly for $\widetilde{\phi}$ and $\widetilde{\delta}$. In addition, $c(\widetilde{\phi}) - \delta + c(\widetilde{\phi}^\vee) - \delta = d_2 - 2\delta = -\sqrt{\widetilde{d_2}}$. Therefore, at least one of $c(\widetilde{\phi}), c(\widetilde{\phi_0})$ is congruent to $\widetilde{\delta}$ modulo μ, and both are congruent to $\widetilde{\delta}$ modulo μ if and only if $\ell | \widetilde{d_2}$. This information is already enough to prove the proposition under the assumption that $\ell | f_2$ or $\ell \nmid d_2$.

Assume that $\ell | d_2$, $s_2 = 0$ and $\ell \nmid d_1$. Then by Lemma 8.2, $S_{n,m}(E/\mathbb{W}) = \emptyset$ for all $n > 1$. Since A is a degree 2 ramified extension of $\mathbb{W}$, this implies that $S_{n,m}(E/A) = \emptyset$ for all $n > 2$. Further, the arguments from the previous paragraph show that $S_{1,m}^{\mathrm{Lie}}(E/A) = S_{1,m}(E/\mathbb{W})$. It remains to consider $S_{2,m}^{\mathrm{Lie}}(E/A)$. Although $S_{2,m}(E/A) = S_{1,m}(E/\mathbb{W})$, which may be nonempty, δ is not congruent modulo μ^2 to any element of $\mathbb{W}$. In particular δ is not congruent to $c(\phi)$ or $c(\phi^\vee)$ modulo μ^2. Therefore $S_{2,m}^{\mathrm{Lie}}(E/A) = \emptyset$, and so $\sum_n \#S_{n,m}^{\mathrm{Lie}}(E/A) = \sum_n \#S_{n,m}(E/\mathbb{W})$ as claimed.

The remaining case is when $s_2 = 0$ (so $\widetilde{d}_2 = d_2$) and $\ell | \gcd(d_1, \widetilde{d}_2)$. By assumption, we may restrict to the case where $\ell > 2$, which implies that $A = \mathbb{W}$. The above arguments show that $S_{1,m}^{\text{Lie}}(E/A) = S_{1,m}(E/A)$. In addition, since $v_\mu((c(\phi) - \delta) + (c(\phi^\vee) - \delta))) = 1$, at least one of $v_\mu(c(\phi) - \delta), v_\mu(c(\phi^\vee) - \delta)$ is 1; without loss of generality we will assume that $v_\mu(c(\phi^\vee) - \delta) = 1$.

To conclude anything further, we must first determine a more complete description of c. From the results in §7, we have that any $\phi \in S_{n,m}(E/\mathbb{W})$ can be written as

$$\phi = \left[\frac{1}{2\sqrt{d_1}} \left(d_1 d_2 - 2t + d_2 \sqrt{d_1} \right), 0 \right] + [\beta, 0] \cdot [0, 1]$$

for some $\beta \in \mathbb{Q}(\sqrt{d_1})$ with $N(\beta) = m/(-qd_1)$. Thus,

$$c(\phi) - \delta = \frac{1}{2\sqrt{d_1}} \left(d_1 d_2 - 2t - \sqrt{d_2 d_1} \right) \pm \beta \sqrt{-q} \quad \text{in } A/\mu^n, \text{ and}$$

$$c(\phi^\vee) - \delta = \frac{1}{2\sqrt{d_1}} \left(2t - d_1 d_2 - \sqrt{d_2 d_1} \right) \mp \beta \sqrt{-q} \quad \text{in } A/\mu^n.$$

Note that $v_\mu(\beta) = v_\mu(\beta \sqrt{-q}) = v_\ell(m) - 1$, and

$$v_\mu \left(d_1 d_2 - 2t - \sqrt{d_2 d_1} \right) + v_\mu \left(2t - d_1 d_2 - \sqrt{d_2 d_1} \right) = 2 v_\ell(m).$$

Since by Lemma 8.2, $v_\ell(m) > 1$ and by assumption we have $v_\mu(c(\phi^\vee) - \delta) = 1$, we must have

$$v_\mu \left(\frac{1}{2\sqrt{d_1}} \left(d_1 d_2 - 2t - \sqrt{d_2 d_1} \right) \right) = 2(v_\ell(m) - 1).$$

If $v_\ell(m) > 2$, then $c(\phi) \equiv \delta \pmod{\mu^n}$ if and only if $n \le v_\ell(m) - 1$.

Assume that $v_\ell(m) = 2$ and recall that $-q \notin \mathbb{Q}_\ell^{\times 2}$. If $d_1 d_2 \in \mathbb{Q}_\ell^{\times 2}$, then $c(\phi) - \delta \in \mu^2$ only if $\beta \in \mu^2$. However, $v_\mu(\beta) = v_\ell(m) - 1 = 1$, so we must have $c(\phi) - \delta \in \mu \setminus \mu^2$. If $d_1 d_2 \notin \mathbb{Q}_\ell^{\times 2}$, then since ℓ is odd we have $-qd_1 d_2 \in \mathbb{Q}_\ell^{\times 2}$. Therefore, we may rewrite $c(\phi) - \delta$ as a linear combination of the $\mathbb{Q}_\ell(\sqrt{d_1})$-linearly independent elements 1 and $\sqrt{-q}$ as follows:

$$\frac{1}{2\sqrt{d_1}} (d_1 d_2 - 2t) + \sqrt{-q} \left(\pm \beta - \sqrt{\frac{d_2}{-4qd_1}} \sqrt{d_1} \right).$$

From this expression, we see that $c(\phi) \equiv \delta \bmod \mu^2$ if and only if $v_\ell(d_1 d_2 - 2t) > 1$ and $\pm \beta / \sqrt{d_1} \equiv \sqrt{\frac{d_2}{-4qd_1}} \bmod \mu$, which would imply that $N(\beta) \equiv d_2/4q \bmod \ell^2$. However, $N(\beta) = m/(-qd_1)$ which, under the assumption that $v_\ell(d_1 d_2 - 2t) > 1$, implies that $N(\beta) \equiv d_2/(-4q) \bmod \ell^2$. Therefore we must have that $c(\phi) - \delta \in \mu \setminus \mu^2$.

31

In summary, we have shown that for $n > 2$, we have $\#S_{n,m}^{\mathrm{Lie}}(E/A) = \frac{1}{2}\#S_{n+1,m}(E/A)$. In addition, by Lemma 8.2, $S_{1,m}(E/A) = S_{2,m}(E/A)$. Hence, we have

$$\sum_n \#S_{n,m}^{\mathrm{Lie}}(E/A) = \#S_{1,m}^{\mathrm{Lie}}(E/A) + \sum_{n \geq 2} \#S_{n,m}^{\mathrm{Lie}}(E/A)$$

$$= S_{1,m}(E/A) + \sum_{n \geq 3} \frac{1}{2}\#S_{n,m}(E/A)$$

$$= \frac{1}{2}\#S_{1,m}(E/A) + \frac{1}{2}\#S_{2,m}(E/A) + \sum_{n \geq 3} \frac{1}{2}\#S_{n,m}(E/A),$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

REFERENCES

[CF67]   J.W.S Cassels and A. Fröhlich, *Algebraic number theory*, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union., Academic Press, London, 1967. MR0215665 (35 #6500)

[Con04]   Brian Conrad, *Gross-Zagier revisited*, Heegner points and Rankin *L*-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 67–163, DOI 10.1017/CBO9780511756375.006. With an appendix by W. R. Mann. MR2083211 (2005h:11121)

[Cox89]   David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication. MR1028322 (90m:11016)

[Dor89]   David R. Dorman, *Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 108–116. MR1024555 (90j:11043)

[Dor88]   _____, *Special values of the elliptic modular function and factorization formulae*, J. Reine Angew. Math. **383** (1988), 207–220, DOI 10.1515/crll.1988.383.207. MR921991 (89k:11026)

[DGG$^+$]   Valerio Dose, Nathan Green, Michael Griffin, Tianyi Mao, Larry Rolen, and John Willis, *Singular moduli for a distinguished non-holomorphic modular function*. Preprint, to appear in *Proc. Amer. Math. Soc.*

[Eic57]   Martin Eichler, *Lectures on modular correspondences*, Bombay, Tata Institute of Fundamental Research, 1957. Notes by S.S. Rangachari.

[Elk89]   Noam D. Elkies, *Supersingular primes for elliptic curves over real number fields*, Compositio Math. **72** (1989), no. 2, 165–172. MR1030140 (90i:11058)

[GL13]   Eyal Goren and Kristin Lauter, *A Gross–Zagier formula for quaternion algebras over totally real fields*, Algebra Number Theory **7** (2013), no. 6, 1405–1450, DOI 10.2140/ant.2013.7.1405. MR3107568

[Gro86]   Benedict H. Gross, *On canonical and quasicanonical liftings*, Invent. Math. **84** (1986), no. 2, 321–326, DOI 10.1007/BF01388810. MR833193 (87g:14051)

[GZ85]   Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220. MR772491 (86j:11041)

[Hut98]   Tim Hutchinson, *A conjectural extension of the Gross-Zagier formula on singular moduli*, Tokyo J. Math. **21** (1998), no. 1, 255–265, DOI 10.3836/tjm/1270042000. MR1621530 (99j:11131)

[Kan89]   Masanobu Kaneko, *Supersingular j-invariants as singular moduli* mod p, Osaka J. Math. **26** (1989), no. 4, 849–855. MR1040429 (91c:11033)

[Lan87]   Serge Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987. With an appendix by J. Tate. MR890960 (88c:11028)

[LV]   Kristin Lauter and Bianca Viray, *An arithmetic intersection formula for denominators of Igusa class polynomials*. Preprint, available at `arXiv:1210.7841`.

[LT66] Jonathan Lubin and John Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59. MR0238854 (39 #214)

[Meu07] Volker Meusers, *Canonical and quasi-canonical liftings in the split case*, Astérisque **312** (2007), 87–98 (English, with English and French summaries). MR2340373 (2008g:11101)

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859 (2000m:11104)

[Par05] Pierre J. R. Parent, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$*, Compos. Math. **141** (2005), no. 3, 561–572, DOI 10.1112/S0010437X04001022. MR2135276 (2006a:11076)

[RS10] K. Rubin and A. Silverberg, *Choosing the correct elliptic curve in the CM method*, Math. Comp. **79** (2010), no. 269, 545–561, DOI 10.1090/S0025-5718-09-02266-2. MR2552240 (2010i:11091)

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488)

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980 (French). MR580949 (82i:12016)

MICROSOFT RESEARCH, 1 MICROSOFT WAY, REDMOND, WA 98062, USA

E-mail address: klauter@microsoft.com

URL: http://research.microsoft.com/en-us/people/klauter/default.aspx

UNIVERSITY OF WASHINGTON, DEPARTMENT OF MATHEMATICS, BOX 354350, SEATTLE, WA 98195, USA

E-mail address: bviray@math.washington.edu

URL: http://math.washington.edu/~bviray