ASIAN J. MATH.
Vol. 23, No. 4, pp. 651–680, August 2019

SUPERSINGULAR ABELIAN SURFACES AND EICHLER'S CLASS NUMBER FORMULA*

JIANGWEI XUE†, TSE-CHUNG YANG‡, AND CHIA-FU YU§

Abstract. In [Ann. Sci. École Norm. Sup. (4), 1969], Waterhouse classified simple abelian varieties over a prime field $\mathbb{F}_p$ in terms of lattices, except for the isogeny class that corresponds to the conjugacy class of Weil numbers $\pm\sqrt{p}$. He gave a description only for those with maximal endomorphism rings in this isogeny class, and suggested to apply Eichler's trace formula to compute the number of them. The main result of this paper gives an explicit formula for the number of isomorphism classes in this isogeny class, generalizing the classical formula for supersingular elliptic curves by Eichler and Deuring. To achieve this, we give a self-contained treatment of Eichler's trace formula for an arbitrary $\mathbb{Z}$-order in any totally definite quaternion algebra.

Key words. Supersingular abelian surfaces, class number formula, Brandt matrices, trace formula.

Mathematics Subject Classification. 11R52, 11G10.

1. Introduction. Throughout this paper p denotes a prime number. Let $\mathbf{D}$ be the quaternion $\mathbb{Q}$-algebra ramified exactly at $\{p, \infty\}$. For any supersingular elliptic curve X over $\bar{\mathbb{F}}_p$, its endomorphism algebra $\mathrm{End}^0_{\bar{\mathbb{F}}_p}(X) := \mathrm{End}_{\bar{\mathbb{F}}_p}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathbf{D}$, and its endomorphism ring $\mathrm{End}_{\bar{\mathbb{F}}_p}(X)$ is always a maximal order in $\mathbf{D}$. The classical theory of Deuring establishes a one-to-one correspondence between isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$ and ideal classes of a maximal order $\mathcal{O}_{\mathbf{D}} \subset \mathbf{D}$. Moreover, there is an explicit formula for the class number $h(\mathcal{O}_{\mathbf{D}})$ as follows

$$h(\mathcal{O}_{\mathbf{D}}) = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right), \tag{1.1}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. In (1.1), the main term $(p-1)/12$ is the mass for supersingular elliptic curves, which is also equal to $\zeta_{\mathbb{Q}}(-1)(1-p)$, where $\zeta_{\mathbb{Q}}(s)$ is the Riemann zeta function. The remaining terms are the adjustments for the isomorphism classes with extra automorphisms. As the points corresponding to these classes on the moduli space come from the reduction of elliptic fixed points (whose j-invariants are 0 or 1728), the latter sum is also called the elliptic part.

The goal of this paper is to provide an explicit description and concrete formula for the isomorphism classes inside certain isogeny class of supersingular abelian surfaces. The main tools are the Honda-Tate theory and extended methods in Eichler's class number formula.

Suppose that q is a power of the prime number p. An algebraic integer $\pi \in \bar{\mathbb{Q}}$ is said to be a *Weil q-number* if $|\pi| = \sqrt{q}$ for all embeddings of $\mathbb{Q}(\pi)$ into $\mathbb{C}$. The Honda-Tate theory [13, 25] establishes a bijection between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes Weil q-numbers. In [28], Waterhouse

*Received November 14, 2016; accepted for publication May 23, 2018.

†Collaborative Innovation Centre of Mathematics, School of Mathematics and Statistics, Wuhan University, Luojiashan, Wuhan, Hubei, 430072, P.R. China (xue_j@whu.edu.cn).

‡Institute of Mathematics, Academia Sinica, Astronomy-Mathematics Building, 6F, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan (tsechung@math.sinica.edu.tw).

§Institute of Mathematics, Academia Sinica and NCTS, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan (chiafu@math.sinica.edu.tw).

developed a theory for studying the isomorphism classes and endomorphism rings of abelian varieties within a fixed simple isogeny class. If π is a Weil q-number, we denote by X_π the abelian variety over $\mathbb{F}_q$ associated to π, unique up to isogeny. For example, it is well known that every supersingular elliptic curve over $\bar{\mathbb{F}}_p$ admits a model over $\mathbb{F}_{p^2}$ that lies inside the isogeny class $\mathrm{Isog}(X_\pi)$ corresponding to the Weil p^2-number $\pi = -p$. Then (1.1) may be interpreted as a formula for the number of isomorphism classes in this isogeny class. When $q = p$ is a prime number, Waterhouse has proven the following result [28, Theorem 6.1].

THEOREM 1.1. *Suppose that $F = \mathbb{Q}(\pi)$ is not a totally real field. Then*
(1) The endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_p}(X_\pi) = \mathrm{End}_{\mathbb{F}_p}(X_\pi) \otimes_{\mathbb{Z}} \mathbb{Q}$ of X_π is commutative and coincides with F;
(2) All orders in F containing $R_0 = \mathbb{Z}[\pi, p\pi^{-1}]$ are endomorphism rings;
(3) There is a bijection between the set of R_0-ideal classes and the $\mathbb{F}_p$-isomorphism classes of abelian varieties isogenous to X_π.

In general there is no explicit description for R_0-ideal classes. However, the set of R_0-ideals is divided into finitely many genera and each genus has $h(R)$ ideal classes for some order $R \subseteq F$ containing R_0, where $h(R) := |\mathrm{Pic}(R)|$ denotes the class number of R. It is known that the class number $h(R)$ is a multiple of the class number $h(F)$ of F. As a consequence of Waterhouse's result (Theorem 1.1) the number of $\mathbb{F}_p$-isomorphism classes in $\mathrm{Isog}(X_\pi)$ is a multiple of the class number $h(F)$. Determining this multiple, nevertheless, requires an explicit description of genera of R_0-ideals.

The above is the general picture when $F = \mathbb{Q}(\pi)$ is not totally real for a Weil p-number π. The exceptional case where F is totally real corresponds to the unique conjugacy class of the Weil number $\pi = \sqrt{p}$, for which $F = \mathbb{Q}(\sqrt{p})$ is a real quadratic field. It was already known to Tate [25, Section 1, Examples] that X_π in this case is a supersingular abelian surface whose endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_p}(X_\pi)$ is isomorphic to the quaternion algebra D_{∞_1,∞_2} over F ramified only at the two real places of F. Different from the classical case of supersingular elliptic curves treated by Deuring, Waterhouse [28, Theorem 6.2] shows that $\mathrm{End}_{\mathbb{F}_p}(X_\pi)$ is not always a maximal order in D_{∞_1,∞_2}. A description of endomorphism rings of these abelian surfaces will be given in Section 6.1. Our main result gives explicit formulas for the number of $\mathbb{F}_p$-isomorphism classes of this isogeny class.

THEOREM 1.2. *Let $H(p)$ be the number of $\mathbb{F}_p$-isomorphism classes of abelian varieties in the simple isogeny class corresponding to the conjugacy class of Weil p-number $\pi = \sqrt{p}$. Then*
(1) $H(p) = 1, 2, 3$ for $p = 2, 3, 5$, respectively;
(2) For $p > 5$ and $p \equiv 3 \pmod 4$, one has

$$H(p) = \frac{1}{2}h(F)\zeta_F(-1) + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(K_1)}{8} + \frac{1}{4}h(K_2) + \frac{1}{3}h(K_3), \tag{1.2}$$

where $K_j := F(\sqrt{-j})$ for $j = 1, 2, 3$, and $h(K_j)$ denotes the class number of K_j.
(3) For $p > 5$ and $p \equiv 1 \pmod 4$, one has

$$H(p) = \begin{cases} 8\zeta_F(-1)h(F) + h(K_1) + \frac{4}{3}h(K_3) & \text{for } p \equiv 1 \pmod 8; \\ \left(\frac{45+\varpi}{2\varpi}\right)\zeta_F(-1)h(F) + \left(\frac{9+\varpi}{4\varpi}\right)h(K_1) + \frac{4}{3}h(K_3) & \text{for } p \equiv 5 \pmod 8; \end{cases} \tag{1.3}$$

where $\varpi := [O_F^\times : A^\times]$ and $A := \mathbb{Z}[\sqrt{p}] \subsetneq O_F$. The value of ϖ is either 1 or 3. The special value $\zeta_F(-1)$ of the Dedekind zeta-function $\zeta_F(s)$ in both (2) and (3) can be calculated by Siegel's formula (6.12).

The calculations for Theorem 1.2 will be carried out in Section 6.2. The main idea for the proof of Theorem 1.2 is to apply Eichler's class number formula ([10], [27, Chapter V, Corollary 2.5, p. 144]) for totally definite quaternion algebras. Eichler proved the class number formula in the case of Eichler O_F-orders. Based on Eichler's methods, Körner [18] worked out a similar class number formula for an arbitrary O_F-order. However, the class number formula established in [18] is not readily applicable in our case as the orders arising from the endomorphism rings of supersingular abelian surfaces as above do not necessarily contain the ring of integers $O_F \subset F$. A main part of this paper (Sections 2–5) is then devoted to proving a similar class number formula and mass formula for arbitrary $\mathbb{Z}$-orders. Our generalized Eichler class number formula is the following.

THEOREM 1.3 (Class number formula). *Let D be a totally definite quaternion algebra over a totally real number field F, and $\mathcal{O} \subset D$ an arbitrary order in D with center $A := Z(\mathcal{O})$. The class number of $\mathcal{O}$ is given by*

$$h(\mathcal{O}) = \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{w(B)>1} (2-\delta(B))h(B)(1-w(B)^{-1}) \prod_p m_p(B), \tag{1.4}$$

where the summation is over all the non-isomorphic orders B whose fraction field K is a quadratic extension of F embeddable into D, and

$$B \cap F = A, \qquad w(B) := [B^\times : A^\times] > 1.$$

Here $\mathrm{Mass}(\mathcal{O})$ *is given by Definition 3.3.2 and can be computed by the mass formula (5.6); $m_p(B)$ is the number of conjugacy classes of local optimal embeddings (3.6); and $\delta(B) = 1$ if B is closed under the complex conjugation $\iota \in \mathrm{Gal}(K/F)$, and 0 otherwise.*

In the course of proving the class number formula we realize a subtle point that the reduced norm of a $\mathbb{Z}$-order may strictly contain its center. This caused some confusion at first as there are possibly more than one choices for defining Brandt matrices as well as other terms in the proof (Remark 3.3.9). Thus one needs to examine every detail in the original proof in [10] and [27] (also see a proof in Brzezinski [6] for definite central division algebras of prime index) until the final formula goes through. Our definition of Brandt matrices is justified by representation theory (Section 4). We remark that the methods here are algebraic, therefore all results in Sections 2-4 make sense and remain valid when F is replaced by an arbitrary global function field, and A by any S-order (whose normalization is the S-ring of integers), possibly except for Theorems 3.3.3 and 3.3.7 and Corollary 3.3.8 in characteristic 2; also see Remark 4.2.2.

The explicit formulas given in Theorem 1.2 are proved in Section 6. Based on these formulas, we used Magma [5] to evaluate the numbers $H(p)$ for $p < 10000$ and make the tables for values of related terms for $p < 200$ in Section 7.

Based on Theorem 1.2 we give explicit formulas for the number of superspecial abelian surfaces over any finite field $\mathbb{F}_q$ of odd degree over $\mathbb{F}_p$ in a sequel paper [33]. In the case where $\mathbb{F}_q$ is of even degree extension over $\mathbb{F}_p$, the corresponding explicit formulas for superspecial abelian surfaces are just proved in [34]. Thus, we now have explicit formulas for numbers of superspecial abelian surfaces over all finite fields.

In [19] Qun Li, the first and third named authors study conjugacy classes of maximal orders of a definite quaternion algebra over a real quadratic field with a fixed reduced unit group. As a consequence, we obtain refined explicit formulas for the numbers of superspecial abelian surfaces with Frobenius endomorphism $\sqrt{q}$ and with a given reduced automorphism group. In [31] the first and third named authors extend our methods and obtain an explicit formula for the number of the supersingular abelian surfaces with Frobenius endomorphism $\sqrt{q}$. We intend to work on other supersingular isogeny classes in the future.

2. Preliminaries.

2.1. **Notations and definitions.** Let F be a number field with ring of integers O_F and $A \subseteq O_F$ a $\mathbb{Z}$-order in F. Let D be a finite-dimensional central simple F-algebra, and $\mathcal{O}$ an A-order in D. The order $\mathcal{O}$ is said to be a *proper* A-order if $\mathcal{O} \cap F = A$. Similarly, for any finite field extension K/F, we say an order $B \subseteq O_K$ is a *proper* A-order if $B \cap F = A$. An order B is called a *quadratic proper* A-order if B is a proper A-order and the fraction field K of B is a quadratic extension of F. It does not necessarily mean that B is an A-module generated by 2 elements. In fact, we will be interested only in those quadratic proper A-orders B for which K is a totally imaginary quadratic extension of F in the case that F is totally real.

We will need the adelic language in the subsequent sections. For any place v of F, denote by F_v the completion of F at v and $O_v \subset F_v$ the ring of integers if v is a finite place. Let $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_p \mathbb{Z}_p$ be the pro-finite completion of $\mathbb{Z}$. Given any $\mathbb{Z}$-module Y, we write

$$\widehat{Y} := Y \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}, \quad \text{and} \quad Y_p := Y \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

If Y is also an O_F-module, then Y_p factors into $\prod_{v|p} Y_v$, where $Y_v := Y \otimes_{O_F} O_v$. We are mostly concerned with the case where Y is a finite-dimensional $\mathbb{Q}$-vector space or a $\mathbb{Z}$-module of finite rank. For example, $\widehat{\mathcal{O}} = \prod_p \mathcal{O}_p$, $\widehat{A} = \prod_p A_p$, and $\widehat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ is the ring of finite adeles of $\mathbb{Q}$. Similarly, $\widehat{F} = F \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = F \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}} = \prod'_{v:\,\text{finite}} F_v$ is the ring of finite adeles of F, and $\widehat{D} = D \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}} = D \otimes_F \widehat{F}$ is the finite adele ring of D. Thus, $\widehat{\mathcal{O}}^\times \subset \widehat{D}^\times$ and $\widehat{A}^\times \subset \widehat{F}^\times$ are open compact subgroups of the finite idele groups $\widehat{D}^\times$ and $\widehat{F}^\times$, respectively.

A *lattice* $I \subset D$ is a finitely generated $\mathbb{Z}$-module that spans D over $\mathbb{Q}$. Its *associated left order* $\mathcal{O}_l(I)$ is defined to be $\mathcal{O}_l(I) := \{x \in D \mid xI \subseteq I\}$. Similarly, one defines the associated right order $\mathcal{O}_r(I)$. The lattice I is said to be a right $\mathcal{O}$-ideal if $I\mathcal{O} \subseteq I$. A right $\mathcal{O}$-ideal is not necessarily contained in $\mathcal{O}$, and those that lie in $\mathcal{O}$ are called *integral* right $\mathcal{O}$-ideals.

Any right $\mathcal{O}$-ideal I is uniquely determined by its completion $\widehat{I} \subset \widehat{D}$, as $I = \widehat{I} \cap D$. For any $g \in \widehat{D}^\times$, we set

$$gI := g\widehat{I} \cap D, \qquad g\mathcal{O}g^{-1} := g\widehat{\mathcal{O}}g^{-1} \cap D.$$

Then gI is again a right $\mathcal{O}$-ideal and $g\mathcal{O}g^{-1}$ is an order in D.

Given an ideal $\mathfrak{a} \subsetneq A$, we write $A_{\mathfrak{a}}$ for the $\mathfrak{a}$-adic completion $\varprojlim A/\mathfrak{a}^n$ of A, and $Y_{\mathfrak{a}} := Y \otimes_A A_{\mathfrak{a}}$ for any finitely generated A-module Y.

Given a finite set S, most of the time we write $|S|$ for the cardinality of S, though sometimes it is more convenient to write it as $\#S$.

2.2. **Locally principal ideals.** A right $\mathcal{O}$-ideal I is said to be *locally principal* with respect to $A = \mathcal{O} \cap F$ if $I_{\mathfrak{m}}$ is a principal $\mathcal{O}_{\mathfrak{m}}$-ideal for every maximal ideal $\mathfrak{m}$ of A. Similarly, I is said to be locally principal with respect to $\mathbb{Z}$ if I_p is a principal $\mathcal{O}_p$-ideal for every prime p. However, these two definitions are equivalent. Clearly one has the decomposition $\mathcal{O}_p = \prod_{\mathfrak{m}|p} \mathcal{O}_{\mathfrak{m}}$ arising from $A_p = \prod_{\mathfrak{m}|p} A_{\mathfrak{m}}$. It follows that the ideal I_p is $\mathcal{O}_p$-principal if and only if $I_{\mathfrak{m}}$ is $\mathcal{O}_{\mathfrak{m}}$-principal for every $\mathfrak{m}|p$. Thus, there is no confusion when I is said to be a locally principal right $\mathcal{O}$-ideal.

Any locally principal right $\mathcal{O}$-ideal I is of the form $g\mathcal{O}$ for some $g \in \widehat{D}^\times$. We have

$$\mathcal{O}_r(I) = \mathcal{O}, \qquad \mathcal{O}_l(I) = g\mathcal{O}g^{-1}. \tag{2.1}$$

Define $I^{-1} := \mathcal{O}g^{-1}$. Then I^{-1} is a left $\mathcal{O}$-ideal whose associated right order is $\mathcal{O}_l(I)$, and

$$I^{-1}I = \mathcal{O}, \qquad II^{-1} = g\mathcal{O}g^{-1} = \mathcal{O}_l(I). \tag{2.2}$$

Note that I is a locally principal right $\mathcal{O}_r(I)$-ideal if and only if it is a locally principal left $\mathcal{O}_l(I)$-ideal. Thus if we say that (a lattice) I is locally principal, without any reference to orders, it is understood that I is locally principal for both $\mathcal{O}_l(I)$ and $\mathcal{O}_r(I)$.

Given two locally principal right $\mathcal{O}$-ideals I and J, we write $I \simeq J$ if they are isomorphic as right $\mathcal{O}$-ideals. This happens if and only if there exists $g \in D^\times$ such that $gI = J$. Denote by $\mathrm{Cl}(\mathcal{O})$ the set of isomorphism classes of locally principal right $\mathcal{O}$-ideals in D. The map $g \mapsto g\mathcal{O}$ for $g \in \widehat{D}^\times$ induces a natural bijection

$$D^\times \backslash \widehat{D}^\times / \widehat{\mathcal{O}}^\times \simeq \mathrm{Cl}(\mathcal{O}).$$

The class number of $\mathcal{O}$ will be denoted by $h = h(\mathcal{O}) := |\mathrm{Cl}(\mathcal{O})|$.

2.3. **Norms of ideals.** We study some properties of the norms of ideals in the present setting (the ground ring A is not necessarily integrally closed). For any A-lattice I in D, define the norm of I (over A) by

$$\mathrm{Nr}_A(I) := \left\{ \sum_{i=1}^m a_i \,\mathrm{Nr}(x_i) \text{ for some } m \in \mathbb{N} \,\middle|\, a_i \in A,\ x_i \in I \right\} \subset F,$$

where $\mathrm{Nr} : D \to F$ denotes the reduced norm map. The formation of reduced norms of lattices commutes with completions. That is, for any ideal $\mathfrak{a} \subsetneq A$,

$$\mathrm{Nr}_A(I)_{\mathfrak{a}} = \mathrm{Nr}_{A_{\mathfrak{a}}}(I_{\mathfrak{a}}). \tag{2.3}$$

The inclusion $\subseteq$ is obvious as $I \subseteq I_{\mathfrak{a}}$. Since $\mathrm{Nr}_A(I)$ is a finitely generated A-module, $\mathrm{Nr}_A(I)_{\mathfrak{a}} = \mathrm{Nr}_A(I) \otimes A_{\mathfrak{a}}$ is the completion of $\mathrm{Nr}_A(I)$ with respect to the $\mathfrak{a}$-adic topology. In particular, $\mathrm{Nr}_A(I)_{\mathfrak{a}}$ is closed in $\mathrm{Nr}_{A_{\mathfrak{a}}}(I_{\mathfrak{a}})$. Let $\mathrm{Nr}_{\mathrm{Set}}$ be the set theoretic image under the reduced norm map. Note that Nr is continuous with respect to the $\mathfrak{a}$-adic topology, and I is dense in $I_{\mathfrak{a}}$. We have

$$\mathrm{Nr}_{\mathrm{Set}}(I_{\mathfrak{a}}) = \mathrm{Nr}_{\mathrm{Set}}(\bar{I}) \subseteq \overline{\mathrm{Nr}_{\mathrm{Set}}(I)} \subseteq \mathrm{Nr}_A(I)_{\mathfrak{a}},$$

where the overline denotes the closure in the $\mathfrak{a}$-adic topology. Since $\mathrm{Nr}_{A_{\mathfrak{a}}}(I_{\mathfrak{a}})$ is spanned by $\mathrm{Nr}_{\mathrm{Set}}(I_{\mathfrak{a}})$ over $A_{\mathfrak{a}}$, we obtain the other inclusion needed for the verification of (2.3).

Let $\widetilde{A}_l := \mathrm{Nr}_A(\mathcal{O}_l(I))$ and $\widetilde{A}_r := \mathrm{Nr}_A(\mathcal{O}_r(I))$. Clearly, $\mathrm{Nr}_A(I)$ is a module over the ring $\widetilde{A} := \widetilde{A}_l\widetilde{A}_r$. Here extra caution is needed since that $\widetilde{A}_l$ (or $\widetilde{A}_r$) may strictly contain A even if $\mathcal{O}_l(I)$ (or $\mathcal{O}_r(I)$) is a proper A-order. An example will be given in Section 5.2 by taking $I = \mathbb{O}_8$, where $\mathbb{O}_8$ is a certain nonmaximal order in the quaternion algebra D_{∞_1,∞_2}. We do not know the relation between $\widetilde{A}_l$ and $\widetilde{A}_r$ in general. However, $\mathrm{Nr}_A(I)$ is reasonably well behaved when I is locally principal.

Suppose that I is a locally principal right ideal for a proper A-order $\mathcal{O}$. By (2.1), $\widetilde{A} = \widetilde{A}_l = \widetilde{A}_r = \mathrm{Nr}_A(\mathcal{O})$. If we write $I = g\mathcal{O}$ for some $g \in \widehat{D}^\times$, then $\mathrm{Nr}_A(I) = \mathrm{Nr}(g)\,\mathrm{Nr}_A(\mathcal{O}) = \mathrm{Nr}(g)\widetilde{A}$. Hence Nr_A sends locally principal right $\mathcal{O}$-ideals to invertible $\widetilde{A}$-modules. This property enables us to define Brandt matrices for an arbitrary proper A-order $\mathcal{O}$ in Section 3.

2.4. **Multiplicative properties.** Let I and J be two A-lattices in D. We discuss when the multiplicative property $\mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J) = \mathrm{Nr}_A(IJ)$ holds. Clearly $\mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J) \subseteq \mathrm{Nr}_A(IJ)$ as $\mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J)$ is generated by elements $\mathrm{Nr}(x)\,\mathrm{Nr}(y) = \mathrm{Nr}(xy)$ with $x \in I$, $y \in J$ and $xy \in IJ$. Moreover, the equality can be checked locally: the equality $\mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J) = \mathrm{Nr}_A(IJ)$ holds if and only if its local analogue $\mathrm{Nr}_{A_p}(I_p)\,\mathrm{Nr}_{A_p}(J_p) = \mathrm{Nr}_{A_p}(I_pJ_p)$ holds for every prime p. The product IJ of I and J is said to be *coherent* if $\mathcal{O}_r(I) = \mathcal{O}_l(J)$ (cf. [24, p. 183], [27, p. 22]). We give an example that shows that $\mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J) \neq \mathrm{Nr}_A(IJ)$ when the product IJ of I and J is not coherent, even though both I and J are locally principal lattices.

Let $F = \mathbb{Q}$ and D be any quaternion $\mathbb{Q}$-algebra with $D_p = \mathrm{Mat}_2(\mathbb{Q}_p)$. Take any two $\mathbb{Z}$-lattices I and J in D with

$$I_p = \begin{pmatrix} \mathbb{Z}_p & p\,\mathbb{Z}_p \\ p^{-1}\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \quad \text{and} \quad J_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}.$$

Then $\mathrm{Nr}_{\mathbb{Z}_p}(I_p)\,\mathrm{Nr}_{\mathbb{Z}_p}(J_p) = \mathbb{Z}_p$ but $\mathrm{Nr}_{\mathbb{Z}_p}(I_pJ_p) = p^{-1}\mathbb{Z}_p$ as

$$I_pJ_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^{-1}\mathbb{Z}_p & p^{-1}\mathbb{Z}_p \end{pmatrix}.$$

In this example the local product I_pJ_p is not coherent and thus the global product IJ is not coherent.

Due to the above example we are content with the multiplicative properties of the reduced norm for the type of products below.

LEMMA 2.5. *Suppose that the product IJ of I and J is coherent and at least one of I and J is locally principal. Then* $\mathrm{Nr}_A(IJ) = \mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J)$.

Proof. Assume that I is right locally $\mathcal{O}$-principal, where $\mathcal{O} = \mathcal{O}_r(I)$. For any prime p, one has

$$\mathrm{Nr}_{A_p}(I_pJ_p) = \mathrm{Nr}_{A_p}(x_p\mathcal{O}_pJ_p) = \mathrm{Nr}_{A_p}(x_pJ_p) = \mathrm{Nr}(x_p)\,\mathrm{Nr}_{A_p}(J_p).$$

Thus $\mathrm{Nr}_{A_p}(I_pJ_p) = \mathrm{Nr}_{A_p}(I_p)\,\mathrm{Nr}_{A_p}(J_p)$ for all primes p and hence $\mathrm{Nr}_A(IJ) = \mathrm{Nr}_A(I)\,\mathrm{Nr}_A(J)$. The case that J is locally principal can be proved similarly. ∎

PROPOSITION 2.6 (Criterion of units in $\mathcal{O}$). *We keep the notation of Section 2.1, except that F is allowed to be either a number field or a nonarchimedean local field. An element $u \in \mathcal{O}$ is a unit if and only if* $\mathrm{Nr}(u) \in O_F^\times$.

Proof. This is a simple generalization of [27, Lemme 4.12, Chapitre I]. Let $S := O_F[u] \subset D$ be the O_F-algebra generated by $u \in \mathcal{O}$. Since $\mathcal{O}$ is an order, u is integral over O_F, and S is a finite O_F-algebra. Clearly, $u \in S^\times$ if and only if $\mathrm{Nr}(u) \in O_F^\times$. Let $R = S \cap \mathcal{O}$, then $u \in R$ and S is integral over the ring R. By [1, Exercise 5, Chapter 5], we have $R^\times = R \cap S^\times$, and the proposition follows. ∎

3. Traces of Brandt matrices. In this section we define Brandt matrices for arbitrary orders in a totally definite quaternion algebra, and derive a formula for the trace of Brandt matrices. This allows us to obtain the generalized class number formula as stated in Theorem 1.3. We follow closely Eichler's original proof [10]; also see Vignéras's book [27].

3.1. Brandt matrices. Throughout the entire Section 3, F denotes a totally real number field, D a totally definite quaternion F-algebra, $A \subseteq O_F$ a $\mathbb{Z}$-order in F and $\mathcal{O}$ a proper A-order in D. Let $h = h(\mathcal{O})$ be the class number of $\mathcal{O}$.

We fix a complete set of representatives $I_1, \dots, I_h$ for the right ideal classes in $\mathrm{Cl}(\mathcal{O})$, and define

$$\mathcal{O}_i := \mathcal{O}_l(I_i), \qquad w_i := [\mathcal{O}_i^\times : A^\times]. \tag{3.1}$$

The number w_i depends only on the ideal class of I_i. Since $I_i = g_i\mathcal{O}$ for some $g_i \in \widehat{D}^\times$, we have $\mathcal{O}_i = g_i \mathcal{O} g_i^{-1}$ by (2.1). In particular, each $\mathcal{O}_i$ is a proper A-order, and if $\mathcal{O}$ is closed under the canonical involution of D, then so is each $\mathcal{O}_i$. Let

$$\widetilde{A} := \mathrm{Nr}_A(\mathcal{O}) = \left\{ \sum_{i=1}^m a_i \,\mathrm{Nr}(x_i) \text{ for some } m \in \mathbb{N} \,\middle|\, x_i \in \mathcal{O}, a_i \in A \right\} \subset F. \tag{3.2}$$

Then $\widetilde{A}$ is an order in F with $A \subseteq \widetilde{A} \subseteq O_F$. For each $i = 1, \dots, h$, $\mathrm{Nr}_A(I_i) = \mathrm{Nr}(g_i)\widetilde{A}$ is an invertible $\widetilde{A}$-module, and $\mathrm{Nr}_A(\mathcal{O}_i) = \widetilde{A}$.

Lemma 3.1.1. *We have $\widetilde{A} = A$ if and only if $\mathcal{O}$ is closed under the canonical involution $x \mapsto \mathrm{Tr}(x) - x$.*

Proof. Suppose that $\widetilde{A} = A$, then $\mathrm{Nr}(x) \in A$ for every $x \in \mathcal{O}$. Therefore,

$$\mathrm{Tr}(x) - x = \mathrm{Nr}(1 + x) - \mathrm{Nr}(x) - 1 - x \in \mathcal{O}.$$

On the other hand, suppose that $\mathcal{O}$ is closed under the canonical involution. Then for any $x \in \mathcal{O}$, $\mathrm{Nr}(x) = (\mathrm{Tr}(x) - x)x$ lies in $\mathcal{O}$, and hence $\mathrm{Nr}(x) \in \mathcal{O} \cap F = A$. It follows that $\widetilde{A} = \mathrm{Nr}_A(\mathcal{O}) = A$. ∎

In general, $\widetilde{A}$ is not necessarily equal to A. This is the crucial difference in deriving the trace formula for Brandt matrices over non-Dedekind ground rings. For brevity, we write $\mathrm{Nr}(I)$ for $\mathrm{Nr}_A(I)$.

Proposition 3.1.2. *Let $\mathfrak{n}$ be a locally principal integral $\widetilde{A}$-ideal. For any two integers i and j with $1 \le i, j \le h = h(\mathcal{O})$, there are bijections among the following finite sets:*

(a) The set of locally principal right $\mathcal{O}$-ideals $J \subseteq I_i$ such that $J \simeq I_j$ as right $\mathcal{O}$-ideals and $\mathrm{Nr}(J) = \mathfrak{n} \cdot \mathrm{Nr}(I_i)$;

(b) The set of integral locally principal right $\mathcal{O}_i$-ideals $J' \subseteq \mathcal{O}_i$ such that $J' \simeq I_j I_i^{-1}$ as right $\mathcal{O}_i$-ideals and $\mathrm{Nr}(J') = \mathfrak{n}$;

(c) The set of right principal $\mathcal{O}_j$-ideals $J'' \subseteq I_i I_j^{-1}$ such that $\mathrm{Nr}(J'') = \mathfrak{n}\,\mathrm{Nr}(I_i) \cdot \mathrm{Nr}(I_j)^{-1}$;

(d) The set of right $\mathcal{O}_j^\times$-orbits of elements $b \in I_i I_j^{-1}$ such that $\mathrm{Nr}(b\mathcal{O}_j) = \mathfrak{n}\,\mathrm{Nr}(I_i)\,\mathrm{Nr}(I_j)^{-1}$.

Proof. The bijection between (a) and (b) is given by $J \mapsto J' := JI_i^{-1}$. It is easy to see that the product JI_i^{-1} is coherent and hence $\mathrm{Nr}(JI_i^{-1}) = \mathrm{Nr}(J)\,\mathrm{Nr}(I_i)^{-1}$. The bijection between (a) and (c) is given by $J'' := JI_j^{-1}$. The bijection between (c) and (d) is given by $J'' = b\mathcal{O}_j$. ☐

Perhaps it is helpful to indicate why the sets in Proposition 3.1.2 are finite. This is already known if $A = O_F$ by Körner [18]. Consider the set in (b). There are finitely many ideals $J'O_F \subseteq \mathcal{O}_i O_F$ with $\mathrm{Nr}(J'O_F) = \mathfrak{n}O_F$. As $cO_F \subseteq A \subseteq O_F$ for some $c \in \mathbb{Z}_{>0}$, there are also finitely many ideals $J' \subseteq \mathcal{O}_i$ with $cJ'O_F \subseteq J' \subseteq J'O_F$ for each $J'O_F$.

Definition 3.1.3. Let $\mathfrak{B}_{ij}(\mathfrak{n})$ be the cardinality of any of the finite sets in Proposition 3.1.2. The *Brandt matrix associated to* $\mathfrak{n}$ is defined to be the matrix

$$\mathfrak{B}(\mathfrak{n}) := (\mathfrak{B}_{ij}(\mathfrak{n})) \in \mathrm{Mat}_h(\mathbb{Z}).$$

It follows from part (d) of Proposition 3.1.2 that

$$\mathfrak{B}_{ii}(\mathfrak{n}) = \#\left(\{b \in \mathcal{O}_i \,|\, \mathrm{Nr}(b)\widetilde{A} = \mathfrak{n}\}/\mathcal{O}_i^\times\right). \tag{3.3}$$

In particular, $\mathfrak{B}_{ii}(\mathfrak{n}) \neq 0$ only if $\mathfrak{n}$ is principal and generated by a totally positive element.

3.2. Optimal embeddings. Let K be a CM-extension [8, §13] of F that are F-embeddable into D, and B be an A-order in K. Denote by $\mathrm{Emb}(B, \mathcal{O})$ the set of optimal embeddings from B into $\mathcal{O}$, that is,

$$\mathrm{Emb}(B, \mathcal{O}) := \{\varphi \in \mathrm{Hom}_F(K, D) \mid \varphi(K) \cap \mathcal{O} = \varphi(B)\}.$$

Equivalently, these are the embeddings of A-orders $\varphi : B \hookrightarrow \mathcal{O}$ such that $\mathcal{O}/\varphi(B)$ has no torsion. One can show that $\mathrm{Emb}(B, \mathcal{O})$ is a finite set. Indeed, let $x \in B$ be a fixed element generating K over F. Then each map φ is uniquely determined by the image $\varphi(x)$ in $\mathcal{O}$. As the elements $\varphi(x)$, when φ varies, have a fixed norm, these elements land in the intersection of a compact set in $\mathcal{O}\otimes\mathbb{R}$ with the discrete subset $\mathcal{O}$, which is a finite set. Note that $\mathrm{Emb}(B, \mathcal{O})$ is nonempty only if B is a proper A-order. Moreover, if $\mathcal{O}$ is closed under the canonical involution, then $\mathrm{Emb}(B, \mathcal{O})$ is nonempty only if B is closed under the complex conjugation $\iota \in \mathrm{Gal}(K/F)$.

The group $\mathcal{O}^\times$ acts on $\mathrm{Emb}(B, \mathcal{O})$ from the right by $\varphi \mapsto g^{-1}\varphi g$ for all $\varphi \in \mathrm{Emb}(B, \mathcal{O})$ and $g \in \mathcal{O}^\times$. We denote

$$m(B, \mathcal{O}) := |\mathrm{Emb}(B, \mathcal{O})|, \qquad m(B, \mathcal{O}, \mathcal{O}^\times) := |\mathrm{Emb}(B, \mathcal{O})/\mathcal{O}^\times|,$$
$$w(B) := [B^\times : A^\times], \qquad \text{and} \qquad w(\mathcal{O}) := [\mathcal{O}^\times : A^\times].$$

Then one has

$$m(B, \mathcal{O}, \mathcal{O}^\times) = \frac{m(B, \mathcal{O})}{w(\mathcal{O})/w(B)}. \tag{3.4}$$

Indeed, let $\varphi \in \mathrm{Emb}(B, \mathcal{O})$ be an element. The orbit $O(\varphi)$ of φ under the $\mathcal{O}^\times$-action is isomorphic to $\mathcal{O}^\times/\varphi(B)^\times$, and hence $|O(\varphi)| = [\mathcal{O}^\times : \varphi(B)^\times] = w(\mathcal{O})/w(B)$, which is independent of φ. This gives (3.4). As a result, one obtains

$$\frac{m(B, \mathcal{O}_i, \mathcal{O}_i^\times)}{w(B)} = \frac{m(B, \mathcal{O}_i)}{w_i}, \quad \forall\, 1 \le i \le h. \tag{3.5}$$

As $\mathcal{O}_p$ and $\mathcal{O}_{i,p}$ are isomorphic for every $1 \le i \le h$, one has $m(B_p, \mathcal{O}_p, \mathcal{O}_p^\times) = m(B_p, \mathcal{O}_{i,p}, \mathcal{O}_{i,p}^\times)$. For simplicity, we write

$$m_p(B) := m(B_p, \mathcal{O}_p, \mathcal{O}_p^\times). \tag{3.6}$$

LEMMA 3.2.1. *Let $h(B) := |\mathrm{Pic}(B)|$ be the class number of B. We have*

$$\sum_{i=1}^{h} m(B, \mathcal{O}_i, \mathcal{O}_i^\times) = h(B) \prod_p m_p(B). \tag{3.7}$$

The proof is similar to that of [27, Theorem 5.11, p. 92] (also see [29], Lemma 3.2 and below), hence omitted.

3.3. Traces of Brandt matrices. Suppose that $\mathfrak{n} = \widetilde{A}\beta \subseteq \widetilde{A}$ is generated by a totally positive element $\beta \in \widetilde{A}$. Choose a complete set $S = \{\epsilon_1, \dots, \epsilon_s\}$ of representatives for the finite group $\widetilde{A}_+^\times/(A^\times)^2$, where $\widetilde{A}_+^\times$ denotes the subgroup of totally positive elements of $\widetilde{A}^\times$. We define two sets:

$$\begin{aligned}\mathscr{C}_i &:= \{b \in \mathcal{O}_i |\, \mathrm{Nr}(b) = \varepsilon\beta \ \text{ for some } \varepsilon \in S\},\\ \mathscr{B}_i &:= \{b \in \mathcal{O}_i |\, \mathrm{Nr}(b)\widetilde{A} = \mathfrak{n}\}/A^\times.\end{aligned}$$

Since $\ker(A^\times \xrightarrow{\mathrm{Nr}} \widetilde{A}^\times) = \ker(A^\times \xrightarrow{a\mapsto a^2} A^\times) = \{\pm 1\}$,

$$\mathscr{B}_i \simeq \{b \in \mathcal{O}_i |\, \mathrm{Nr}(b) = \varepsilon\beta \ \text{ for some } \varepsilon \in S\}/\{\pm 1\} = \mathscr{C}_i/\{\pm 1\},$$

and $\mathfrak{B}_{ii}(\mathfrak{n}) = |\mathscr{B}_i|/w_i$ by (3.3). Thus,

$$\mathfrak{B}_{ii}(\mathfrak{n}) = |\mathscr{C}_i|/2w_i. \tag{3.8}$$

We first count the number of elements of $\mathscr{C}_i \cap F$. The cardinality is clearly even, so we put

$$|\mathscr{C}_i \cap A| = 2\delta_{\mathfrak{n}}. \tag{3.9}$$

Note that $\mathscr{C}_i \cap F = \mathscr{C}_i \cap A$ since $\mathcal{O}_i \cap F = A$. It follows that $\delta_{\mathfrak{n}} \neq 0$ if and only if $\mathfrak{n} = \widetilde{A}a^2$ for some nonzero $a \in A$. Suppose that this is the case. If $b \in \mathscr{C}_i \cap A$, then $b^2 = a^2\epsilon$ for some $\epsilon \in S$. It follows that $b/a \in O_F^\times$, and hence $\epsilon \in (O_F^\times)^2 \cap \widetilde{A}_+^\times$. Without lose of generality, we further assume that $\{\epsilon_1, \dots, \epsilon_r\} \subseteq S$ forms a complete set of representatives for the quotient group $\big((O_F^\times)^2 \cap \widetilde{A}_+^\times\big)/(A^\times)^2$. Write $\epsilon_j = u_j^2$ for each $1 \le j \le r$. We conclude that

$$\delta_{\mathfrak{n}} = \begin{cases} |\{1 \le j \le r \mid au_j \in A\}| & \text{if } \mathfrak{n} = \widetilde{A}a^2 \text{ for some nonzero } a \in A;\\ 0 & \text{otherwise.}\end{cases} \tag{3.10}$$

In particular, the value of $\delta_{\mathfrak{n}}$ does not depend on $\mathcal{O}_i$. Note that if $\mathfrak{n} = \widetilde{A}$, then $\delta_{\mathfrak{n}} = 1$. Similarly, if $A = O_F$ and $\mathfrak{n} = O_F a^2$, then $\delta_{\mathfrak{n}} = 1$ as well, which recovers the classical case as in [27, Proposition V.2.4].

Next, we count the number of elements of $\mathscr{C}_i - F$. Let $\mathcal{P}_{\mathcal{O},\mathfrak{n}} \subseteq F[X]$ be the set consisting of all characteristic polynomials of non-central elements $b \in \mathscr{C}_i$ for some

$1 \le i \le h$. This is a finite set in $\widetilde{A}[X]$ since for any $x \in \mathcal{O}_i$, the reduced trace $\mathrm{Tr}(x) = \mathrm{Nr}(x+1) - \mathrm{Nr}(x) - 1 \in \widetilde{A}$. It is convenient to introduce a slightly larger finite set which depends only on $\widetilde{A}$ and $\mathfrak{n}$. Let $\mathcal{P}_{D,\mathfrak{n}} \subset \widetilde{A}[X]$ be the set consisting of all irreducible polynomials of the form $X^2 - tX + \varepsilon\beta$ with $\varepsilon \in S$ such that $t^2 - 4\varepsilon\beta \notin F_v^2$ for all the ramified places v of D, including all the archimedean ones. The set $\mathcal{P}_{D,\mathfrak{n}}$ is again finite since all archimedean norms of t are bounded. Clearly $\mathcal{P}_{\mathcal{O},\mathfrak{n}} \subseteq \mathcal{P}_{D,\mathfrak{n}}$.

For each $P \in \mathcal{P}_{D,\mathfrak{n}}$, write $K_P := F[X]/(P)$ and $B_P := A[x] \subset K_P$, where x is the image of X in K_P, hence a root of P in K_P. If x' is the other root of P then $A[x']$ is isomorphic to $A[x]$ as A-orders. However, the order $A[x']$ could be different from $A[x]$ in K_P. For example, let $p \equiv 5 \pmod 8$, $F = \mathbb{Q}(\sqrt{p})$ with fundamental unit $\epsilon \in O_F^\times$, and $A = \mathbb{Z}[\sqrt{p}]$. Suppose that $A^\times \neq O_F^\times$, or equivalently, $\varepsilon \notin A^\times$. Then $A[\epsilon\zeta_6] \neq A[\epsilon\zeta_6^{-1}]$ as $A[\epsilon\zeta_6, \epsilon\zeta_6^{-1}] = O_F[\zeta_6]$ but both orders are proper A-orders. We would like to emphasize that K_P is considered not just as an abstract field, but rather a field with the distinguished element x.

Local conditions imposed in the definition of $\mathcal{P}_{D,\mathfrak{n}}$ ensure the existence of an embedding of $(K_P)_v$ into D_v locally everywhere. Then the local-global principle guarantees the existence of an F-embedding of K_P into D. A priori, one needs to impose a further condition on $\mathcal{P}_{D,\mathfrak{n}}$ so that every order B_P is a proper A-order. However, omission of this condition will not cause any trouble since $\mathrm{Emb}(B, \mathcal{O}_i)$ is empty if B is not a proper A-order. One has the following equality for each $1 \le i \le h$:

$$\coprod_{P \in \mathcal{P}_{\mathcal{O},\mathfrak{n}}} \coprod_{B_P \subseteq B \subset K_P} \mathrm{Emb}(B, \mathcal{O}_i) = \coprod_{P \in \mathcal{P}_{D,\mathfrak{n}}} \coprod_{B_P \subseteq B \subset K_P} \mathrm{Emb}(B, \mathcal{O}_i), \tag{3.11}$$

as $\mathrm{Emb}(B, \mathcal{O}_i)$ is nonempty only when $P \in \mathcal{P}_{\mathcal{O},\mathfrak{n}}$.

Lemma 3.3.1. *There is a natural bijection*

$$\mathscr{C}_i - A \simeq \coprod_{P \in \mathcal{P}_{D,\mathfrak{n}}} \coprod_{B_P \subseteq B \subset K_P} \mathrm{Emb}(B, \mathcal{O}_i). \tag{3.12}$$

Proof. To each element $b \in \mathscr{C}_i - A$, one associates a triple (P, B, φ) in the right hand side as follows: P is the characteristic polynomial of b, $\varphi : K_P \to D$ is the F-embedding determined by $\varphi(x) = b$, where x is the image of X in K_P and $B := \varphi^{-1}(\mathcal{O}_i)$, which ensures that φ is an optimal embedding.

Conversely, to each triple (P, B, φ) in the right hand side, one associates the element $b := \varphi(x)$ in $\mathscr{C}_i - A$. Clearly, the element b and the triple (P, B, φ) determine each other uniquely and this gives a natural bijection between these two sets. $\square$

Definition 3.3.2. The mass of $\mathcal{O}$ is defined as

$$\mathrm{Mass}(\mathcal{O}) := \sum_{i=1}^{h} \frac{1}{[\mathcal{O}_i^\times : A^\times]} = \sum_{i=1}^{h} \frac{1}{w_i}.$$

Theorem 3.3.3 (Eichler Trace Formula, first version). *We have* $\mathrm{Tr}\,\mathfrak{B}(\mathfrak{n}) \neq 0$ *only if the ideal* $\mathfrak{n}$ *is a principal and generated by a totally positive element. When* $\mathfrak{n}$ *is generated by a totally positive element* β*, the trace formula for* $\mathfrak{B}(\mathfrak{n})$ *is given by*

$$\mathrm{Tr}\,\mathfrak{B}(\mathfrak{n}) = \delta_{\mathfrak{n}} \cdot \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{P \in \mathcal{P}_{D,\mathfrak{n}}} \sum_{B_P \subseteq B \subset K_P} M(B), \tag{3.13}$$

where $\delta_{\mathfrak{n}}$ is defined by (3.10), and

$$M(B) := \frac{h(B)}{w(B)} \prod_p m_p(B). \tag{3.14}$$

Proof. We have

$$\begin{aligned}
\mathfrak{B}_{ii}(\mathfrak{n}) &= \frac{|\mathscr{C}_i|}{2w_i} = \frac{|\mathscr{C}_i - A|}{2w_i} + \frac{2\delta_{\mathfrak{n}}}{2w_i} \\
&= \frac{\delta_{\mathfrak{n}}}{w_i} + \frac{1}{2} \sum_{P\in\mathcal{P}_{D,\mathfrak{n}}} \sum_{B_P\subseteq B\subset K_P} \frac{|\mathrm{Emb}(B,\mathcal{O}_i)|}{w_i} \quad (\text{Lemma } 3.3.1) \\
&= \frac{\delta_{\mathfrak{n}}}{w_i} + \frac{1}{2} \sum_{P\in\mathcal{P}_{D,\mathfrak{n}}} \sum_{B_P\subseteq B\subset K_P} \frac{m(B,\mathcal{O}_i,\mathcal{O}_i^\times)}{w(B)} \quad (\text{by } (3.5)).
\end{aligned} \tag{3.15}$$

Summing over $i = 1, \dots, h$ and applying Lemma 3.2.1, one obtains (3.13) for the trace of the Brandt matrix $\mathfrak{B}(\mathfrak{n})$. ∎

3.3.4. We would like to count the right hand side of (3.12) by regrouping the elements according to the orders B. For a fixed $1 \le i \le h$, consider the quadruples (B, P, φ, α) consisting of the following objects:
(a) a quadratic proper A-order B with fraction field K, which is a totally imaginary quadratic extension of F embeddable into D,
(b) a polynomial $P \in \mathcal{P}_{D,\mathfrak{n}}$,
(c) an optimal embedding $\varphi \in \mathrm{Emb}(B, \mathcal{O}_i)$,
(d) an F-isomorphism $\alpha : K_P \to K$ such that $B_P \subseteq \alpha^{-1}(B) \subset K_P$. Equivalently, $\alpha \in \mathrm{Hom}_A(B_P, B)$.
Clearly, each such quadruple defines a unique element $b \in \mathscr{C}_i - A$ given by $b := \varphi(\alpha(x))$. Two quadruples $(B_r, P_r, \varphi_r, \alpha_r)_{r=1,2}$ are identified if $P_1 = P_2$ and there exists an isomorphism $\rho : B_1 \to B_2$ such that $\varphi_1 = \varphi_2 \circ \rho$, $\alpha_2 = \rho \circ \alpha_1$.

Suppose that two quadruples $(B_r, P_r, \varphi_r, \alpha_r)_{r=1,2}$ give rise to the same $b \in \mathscr{C}_i - A$. Then necessarily $P_1 = P_2$ since both are the characteristic polynomial of b. Denote this polynomial by P. An F-embedding $K_P \hookrightarrow D$ is uniquely determined by the image of x. So $\varphi_1 \circ \alpha_1 = \varphi_2 \circ \alpha_2$. In particular,

$$B_P \subseteq \alpha_1^{-1}(B_1) = \alpha_1^{-1}\varphi_1^{-1}(\mathcal{O}_i) = \alpha_2^{-1}\varphi_2^{-1}(\mathcal{O}_i) = \alpha_2^{-1}(B_2) \subset K_P. \tag{3.16}$$

Thus B_1 and B_2 are isomorphic. Without lose of generality, we may assume that $B := B_1 = B_2$ from the very beginning. Note that $\varphi_1 = \varphi_2$ implies that $\alpha_1 = \alpha_2$ and vice versa. If on the other hand $\alpha_2 = \iota \circ \alpha_1$, where $\iota \in \mathrm{Gal}(K/F)$ is the unique nontrivial isomorphism (i.e. the complex conjugation), then $\varphi_1 = \varphi_2 \circ \iota$, and it follows from (3.16) that $\iota(B) = B$. Conversely, if (B, P, φ, α) satisfies conditions (a)–(d) and $\iota(B) = B$, then $(B, P, \varphi \circ \iota, \iota \circ \alpha)$ again satisfies these conditions, and the two quadruples need to be identified since they give rise to the same element in $\mathscr{C}_i - A$.

Recall that $\mathfrak{n} = \widetilde{A}\beta$. For each quadratic proper A-order B, let $T_{B,\mathfrak{n}} \subset B$ be the finite set

$$T_{B,\mathfrak{n}} := \{ b \in B - A \mid N_{K/F}(b) = \varepsilon\beta \ \text{ for some } \varepsilon \in S \}, \tag{3.17}$$

and $\mathcal{P}_{B,\mathfrak{n}}$ be the set of characteristic polynomials of elements in $T_{B,\mathfrak{n}}$. In general $\mathfrak{n}$ should be clear from the context, so we drop it from the subscript and write T_B and

$\mathcal{P}_B$ instead. We define

$$\mathscr{C}_{B,i} := \{(P, \varphi, \alpha) \mid P \in \mathcal{P}_B, \varphi \in \operatorname{Emb}(B, \mathcal{O}_i), \alpha \in \operatorname{Hom}_A(B_P, B)\}. \tag{3.18}$$

Note that if $P \in \mathcal{P}_B$ but $P \notin \mathcal{P}_{\mathcal{O},\mathfrak{n}}$, then $\operatorname{Emb}(B, \mathcal{O}_i) = \emptyset$ for all $1 \le i \le h$. The fiber of the projection map $\mathscr{C}_{B,i} \to \mathcal{P}_B$ over each $P \in \mathcal{P}_B$ is

$$\mathscr{E}_{B,P,i} := \operatorname{Emb}(B, \mathcal{O}_i) \times \operatorname{Hom}_A(B_P, B).$$

The set $\mathscr{E}_{B,P,i}$ is equipped with an action of $\operatorname{Gal}(K/F)$ in the following way: if $\iota(B) = B$, then ι acts by sending $(\varphi, \alpha) \mapsto (\varphi \circ \iota, \iota \circ \alpha)$; otherwise ι acts trivially. It is clear that this action is independent of P and i. Let $\operatorname{Gal}(K/F)$ act on $\mathscr{C}_{B,i}$ fiber-wisely. We have

$$\mathscr{C}_i - A \simeq \coprod_B \mathscr{C}_{B,i}/\operatorname{Gal}(K/F), \tag{3.19}$$

where the disjoint union is taken over all the non-isomorphic quadratic proper A-orders B. In the next two subsections, we calculate the cardinality of $\mathscr{C}_{B,i}/\operatorname{Gal}(K/F)$. There are two cases to consider, depending on whether $\iota(B) = B$ or not.

3.3.5. Suppose that $\iota(B) = B$. We have

$$\mathscr{C}_{B,i}/\operatorname{Gal}(K/F) = \coprod_{P \in \mathcal{P}_B} \mathscr{E}_{B,P,i}/\operatorname{Gal}(K/F).$$

Note that $\operatorname{Hom}_A(B_P, B) = \operatorname{Hom}_F(K_P, K)$ for all $P \in \mathcal{P}_B$ in this case. Any choice of a fixed element $\alpha \in \operatorname{Hom}_F(K_P, K)$ induces a bijection

$$\operatorname{Emb}(B, \mathcal{O}_i) \simeq \mathscr{E}_{B,P,i}/\operatorname{Gal}(K/F), \qquad \varphi \mapsto (\varphi, \alpha). \tag{3.20}$$

Therefore,

$$|\mathscr{C}_{B,i}/\operatorname{Gal}(K/F)| = |\mathcal{P}_B| \cdot |\operatorname{Emb}(B, \mathcal{O}_i)|.$$

Since $\iota(B) = B$, an element $b \in T_B$ if and only if $\iota(b) \in T_B$. We have a surjective 2-to-1 map $T_B \to \mathcal{P}_B$. It follows that

$$|\mathscr{C}_{B,i}/\operatorname{Gal}(K/F)| = \frac{1}{2}|T_B| \cdot |\operatorname{Emb}(B, \mathcal{O}_i)|. \tag{3.21}$$

3.3.6. Suppose that $\iota(B) \neq B$. Let $\mathcal{Q}_B$ be the set of pairs $\{(P, \alpha) \mid P \in \mathcal{P}_B, \alpha \in \operatorname{Hom}_A(B_P, B)\}$. Since $\operatorname{Gal}(K/F)$ acts trivially, we have

$$\mathscr{C}_{B,i}/\operatorname{Gal}(K/F) = \mathscr{C}_{B,i} = \coprod_{(P,\alpha) \in \mathcal{Q}_B} \operatorname{Emb}(B, \mathcal{O}_i).$$

We claim that there is a canonical bijection between T_B and $\mathcal{Q}_B$. Indeed, each pair $(P, \alpha) \in \mathcal{Q}_B$ determines a unique element $b := \alpha(x) \in T_B$, where x is the distinguished element in K_P. On the other hand, given any element $b \in T_B$, we just set P to be the characteristic polynomial of b, and $\alpha : B_P \to B$ to be the canonical homomorphism sending x to b. Therefore, if $\iota(B) \neq B$, then

$$|\mathscr{C}_{B,i}/\operatorname{Gal}(K/F)| = |T_B| \cdot |\operatorname{Emb}(B, \mathcal{O}_i)|. \tag{3.22}$$

Let $\delta(B)$ be the symbol

$$\delta(B) := \begin{cases} 1 & \text{if } \iota(B) = B; \\ 0 & \text{otherwise.} \end{cases} \tag{3.23}$$

THEOREM 3.3.7 (Eichler Trace Formula, second version). *Suppose that* $\mathfrak{n} = \widetilde{A}\beta$ *is generated by a totally positive element* $\beta \in \widetilde{A}$. *Let* $|T_{B,\mathfrak{n}}|$ *be the cardinality of the set* $T_{B,\mathfrak{n}}$ *defined in (3.17). The trace formula for* $\mathfrak{B}(\mathfrak{n})$ *is given by*

$$\operatorname{Tr}\mathfrak{B}(\mathfrak{n}) = \delta_{\mathfrak{n}} \cdot \operatorname{Mass}(\mathcal{O}) + \frac{1}{4}\sum_{B}(2 - \delta(B))M(B)|T_{B,\mathfrak{n}}|.$$

Here in the last summation B *runs over all (non-isomorphic) quadratic proper* A*-orders embeddable into* D.

Proof. The proof employs the same line of arguments as Theorem 3.3.3, except that instead of applying Lemma 3.3.1, one combines (3.19), (3.21) and (3.22). □

Note that if $\mathcal{O}$ is closed under the canonical involution of D, then $\widetilde{A} = A$ by Lemma 3.1.1. In this case, only those quadratic proper A-orders B closed under the complex conjugation need to be considered in the trace formula, as $\operatorname{Emb}(B, \mathcal{O}_i)$ is empty for all $1 \leq i \leq h$ if $\delta(B) = 0$. This observation applies to the class number formula below as well.

When $\mathfrak{n} = (1) = \widetilde{A}$, the Brandt matrix $\mathfrak{B}(\widetilde{A})$ is the identity and $\operatorname{Tr}\mathfrak{B}(\widetilde{A}) = h(\mathcal{O})$.

COROLLARY 3.3.8 (Class number formula).

$$\begin{aligned} h(\mathcal{O}) &= \operatorname{Mass}(\mathcal{O}) + \frac{1}{2}\sum_{P \in \mathcal{P}_{D,(1)}} \sum_{B_P \subseteq B \subset K_P} M(B) \\ &= \operatorname{Mass}(\mathcal{O}) + \frac{1}{2}\sum_{w(B)>1} (2 - \delta(B))h(B)(1 - w(B)^{-1})\prod_p m_p(B). \end{aligned} \tag{3.24}$$

Here in the last summation B *runs over all (non-isomorphic) quadratic proper* A*-orders with* $w(B) = [B^\times : A^\times] > 1$. *Equivalently,*

$$h(\mathcal{O}) = \operatorname{Mass}(\mathcal{O}) + \frac{1}{2}\sum_{K}\sum_{\substack{B \subset K, \\ w(B)>1}} h(B)(1 - w(B)^{-1})\prod_p m_p(B), \tag{3.25}$$

where K *runs over all (non-isomorphic) totally imaginary quadratic extensions of* F *embeddable into* D, *and* B *runs over all the distinct quadratic proper* A*-orders in* O_K *with* $w(B) > 1$.

Proof. The first part of (3.24) follows directly from Theorem 3.3.3. For each quadratic proper A-order B, let $q = w(B)$, and $B^\times/A^\times = \{\bar{1}, \bar{x}_2, \ldots, \bar{x}_q\}$. As the map $T_{B,(1)} \to \{\bar{x}_2, \ldots, \bar{x}_q\}$ is surjective and two-to-one, sending $\pm x \mapsto \bar{x}$, one gets $\#T_{B,(1)} = 2(q-1)$. So the second part of (3.24) follows from Theorem 3.3.7. Formula (3.25) is just a more intuitive reformulation of (3.24). Indeed, if $B \neq \iota(B)$, then both B and $\iota(B)$ appears in the right hand side of (3.25), giving us $2h(B)(1 - w(B)^{-1})\prod_p m_p(B)$ for the isomorphic class of B. □

We call the sum in (3.24) the *elliptic part* (of the class number formula) and denote it by $\mathrm{Ell}(\mathcal{O})$, that is,

$$\mathrm{Ell}(\mathcal{O}) := \frac{1}{2}\sum_{w(B)>1}(2-\delta(B))h(B)(1-w(B)^{-1})\prod_p m_p(B). \tag{3.26}$$

REMARK 3.3.9. For the reader's convenience, we explain the definitions of some of the terms occurring in the proof of Theorem 3.3.3. In the definition of Brandt matrices, one should take $\mathfrak{n}$ as an ideal in $\widetilde{A}$, rather than in A. This is justified in Section 4. One should consider the representative set S for $\widetilde{A}_+^\times/(A^\times)^2$, rather than for $\widetilde{A}_+^\times/(\widetilde{A}^\times)^2$, since the norm of groups $\mathcal{O}_i^\times/A^\times$ land in the first group. In (3.10), one should take a in A, rather than in $\widetilde{A}$. This is because the central contribution has norm in this form. While $P\in\mathcal{P}_{D,\mathfrak{n}}$ is a polynomial in $\widetilde{A}[X]$, one should take $B_P=A[x]$, rather than the naive one $\widetilde{A}[X]/(P)$. Otherwise there would be no optimal embedding of B_P into any order $\mathcal{O}_i$.

3.4. Local optimal embeddings. Let $\mathfrak{D}$ be the reduced discriminant of D, that is, the product of all finite primes of F that are ramified in D. When $A=O_F$ and $\mathcal{O}$ is an Eichler O_F-order of level $\mathfrak{N}$, where $\mathfrak{N}\subseteq O_F$ is a square-free prime-to-$\mathfrak{D}$ ideal, one has the formula [27, p. 94] for all prime ideals $\mathfrak{p}\subset O_F$,

$$m_\mathfrak{p}(B) := m(B_\mathfrak{p},\mathcal{O}_\mathfrak{p},\mathcal{O}_\mathfrak{p}^\times) = \begin{cases} 1-\left(\frac{B}{\mathfrak{p}}\right) & \text{if } \mathfrak{p}|\mathfrak{D};\\ 1+\left(\frac{B}{\mathfrak{p}}\right) & \text{if } \mathfrak{p}|\mathfrak{N};\\ 1 & \text{otherwise.}\end{cases}$$

Thus, one gets

$$\prod_\mathfrak{p} m_\mathfrak{p}(B) = \prod_{\mathfrak{p}|\mathfrak{D}}\left(1-\left(\frac{B}{\mathfrak{p}}\right)\right)\prod_{\mathfrak{p}|\mathfrak{N}}\left(1+\left(\frac{B}{\mathfrak{p}}\right)\right). \tag{3.27}$$

Here $(B/\mathfrak{p})$ is the Eichler symbol, defined as follows:

$$\left(\frac{B}{\mathfrak{p}}\right) := \begin{cases}\left(\frac{K}{\mathfrak{p}}\right) & \text{if } \mathfrak{p}\nmid\mathfrak{f}(B);\\ 1 & \text{otherwise;}\end{cases}$$

where $\mathfrak{f}(B)\subseteq O_F$ is the conductor of B and $(K/\mathfrak{p})$ is the Artin symbol

$$\left(\frac{K}{\mathfrak{p}}\right) := \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } K;\\ -1 & \text{if } \mathfrak{p} \text{ is inert in } K;\\ 0 & \text{if } \mathfrak{p} \text{ is ramified in } K.\end{cases}$$

When $\mathcal{O}$ is an Eichler O_F-order with arbitrary prime-to-$\mathfrak{D}$ level $\mathfrak{N}$, Hijikata [12, Theorem 2.3, p. 66] computed the numbers of equivalence classes of the local optimal embeddings from $B_\mathfrak{p}$ into $\mathcal{O}_\mathfrak{p}$.

However, the situation is more delicate when $Z(\mathcal{O})=A\subsetneq O_F$. Let $B\subset K$ and $\mathcal{O}\subset D$ be proper A-orders. Suppose that $D_p\simeq \mathrm{Mat}_2(F_p)=\mathrm{End}_{F_p}(V_p)$, where V_p is a free F_p-module of rank two, and $\mathcal{O}_p=\mathrm{End}_{A_p}(L_p)$, where L_p is a full A_p-lattice in V_p.

Fix an embedding $\varphi_0 : K_p \to D_p$ of F_p-algebras. We view V_p as a free K_p-module of rank one through φ_0. A lattice $M_p \subset V_p$ is said to be a *proper B_p-lattice* if $\{x \in K_p \mid \varphi_0(x)M_p \subseteq M_p\} = B_p$. Let $\mathcal{L}(B_p, L_p, V_p)$ denote the set of isomorphism classes of proper B_p-lattices $M_p \subset V_p$ such that there is an isomorphism $M_p \simeq L_p$ of A_p-lattices. We claim that the number $m(B_p, \mathcal{O}_p, \mathcal{O}_p^\times)$ is equal to $|\mathcal{L}(B_p, L_p, V_p)|$. Notice that $m(B_p, \mathcal{O}_p, \mathcal{O}_p^\times)$ is the cardinality of $\varphi_0(K_p)^\times \backslash \mathcal{E}_p(B_p, \mathcal{O}_p)/\mathcal{O}_p^\times$, where $\mathcal{E}_p(B_p, \mathcal{O}_p) = \{g \in D_p^\times | \varphi_0(K_p) \cap g\mathcal{O}_p g^{-1} = \varphi_0(B_p)\}$. It is straightforward to check that the map $g \mapsto gL_p$ induces a bijection between the set $\varphi_0(K_p)^\times \backslash \mathcal{E}_p(B_p, \mathcal{O}_p)/\mathcal{O}_p^\times$ and $\mathcal{L}(B_p, L_p, V_p)$. This proves our claim.

We will need some structural theorems for modules over Bass orders. A standard reference for Bass orders is the original work [2] of Bass. Recall that a $\mathbb{Z}$-order (or a $\mathbb{Z}_p$-order) B is a *Bass order* if B is Gorenstein and any order B' containing B is also Gorenstein. Bass orders share the following local property: B is Bass if and only if the completion B_p is Bass for every prime p. If a $\mathbb{Z}_p$-order B_p is Bass, then any proper B_p-module of rank one is isomorphic to B_p. Using this and our claim, we obtain the following lemma.

LEMMA 3.4.1. *Suppose that $\mathcal{O}_p = \mathrm{End}_{A_p}(L_p)$. If B_p is a Bass order, then $m(B_p, \mathcal{O}_p, \mathcal{O}_p^\times)$ is either 0 or 1, and $m(B_p, \mathcal{O}_p, \mathcal{O}_p^\times) = 1$ if and only if $B_p \simeq L_p$ as A_p-modules.*

4. Representation-theoretic interpretation of Brandt matrices.

4.1. A general formulation. Let G be a unimodular locally compact topological group. Assume there is a discrete and co-compact subgroup $\Gamma \subset G$. Then the quotient $\Gamma\backslash G$ is a compact topological space with right translation action by G. Let $U \subset G$ be an open compact subgroup. Choose a Haar measure dg on G with volume one on U and use the counting measure on Γ. Since $\Gamma\backslash G$ is compact and U is open, the double coset space $\Gamma\backslash G/U$ is a finite set. Let $L^2(\Gamma\backslash G)$ be the Hilbert space of square-integrable $\mathbb{C}$-valued functions on the compact topological space $\Gamma\backslash G$. The group G acts on $L^2(\Gamma\backslash G)$ by right translation, and we denote this action by R. The subspace $L^2(\Gamma\backslash G)^U$ of U-invariant functions equals $L^2(\Gamma\backslash G/U)$, which is a finite-dimensional vector space. Let $\mathcal{H}(G) := C_c^\infty(G)$ denote the Hecke algebra of G, which consists of all smooth $\mathbb{C}$-valued functions on G with compact support, together with the convolution. The action of $\mathcal{H}(G)$ on $L^2(\Gamma\backslash G)$ is as follows:

$$(R(f)\phi)(x) = \int_G f(g)\phi(xg)dg, \quad f \in \mathcal{H}(G),\ \phi \in L^2(\Gamma\backslash G).$$

Let $\mathcal{H}(G, U) = C_c^\infty(U\backslash G/U)$ denote the subspace of U-bi-invariant functions. For any $f \in \mathcal{H}(G, U)$, the Hecke operator $R(f)$ sends the finite-dimensional vector space $L^2(\Gamma\backslash G/U)$ into itself.

4.2. Quaternion algebras, Brandt matrices and Hecke operators. Let D, F, A and $\mathcal{O}$ be as in Section 3.1. Note that $D^\times \subset \widehat{D}^\times$ is not a discrete subgroup when $[F : \mathbb{Q}] > 1$ because the unit group $O_F^\times$ is not finite. We consider the following groups:

$$G := \widehat{D}^\times/\widehat{A}^\times, \quad \Gamma := D^\times/A^\times, \quad \text{and} \quad U := \widehat{\mathcal{O}}^\times/\widehat{A}^\times.$$

Then $\Gamma \subset G$ is a discrete and co-compact subgroup. This allows us to consider Hecke operators on the space $L^2(\Gamma\backslash G)$ of functions. The group G operates transitively on the set of right locally principal $\mathcal{O}$-ideals. This gives natural bijections

$$D^\times \backslash \widehat{D}^\times / \widehat{\mathcal{O}}^\times \simeq \Gamma \backslash G / U \simeq \mathrm{Cl}(\mathcal{O}). \tag{4.1}$$

Therefore, $h(\mathcal{O}) = \dim L^2(\Gamma\backslash G/U)$. If $\mathbf{1}_U$ denotes the characteristic function of U, then the map $R(\mathbf{1}_U)$ is the identity on $L^2(\Gamma\backslash G/U)$ and $\mathrm{Tr}\, R(\mathbf{1}_U) = h(\mathcal{O})$.

Let $\mathfrak{n} \subseteq \widetilde{A}$ be a locally principal integral $\widetilde{A}$-ideal. The finite idele group $\widehat{F}^\times$ operates on the set of $\widetilde{A}$-ideals. Set

$$U(\mathfrak{n}) := \{x \in G \,|\, x\widehat{\mathcal{O}} \subseteq \widehat{\mathcal{O}},\ \mathrm{Nr}(x)\widetilde{A} = \mathfrak{n}\,\}.$$

This is an open compact subset in G which is stable under U by left and right actions. Using the Cartan decomposition, one easily sees that $U\backslash U(\mathfrak{n})/U$ is a finite set. Let $g_1, \dots, g_h$ be a complete set of representatives for $D^\times\backslash \widehat{D}^\times/\widehat{\mathcal{O}}^\times$, one has

$$\widehat{D}^\times = \coprod_{i=1}^h D^\times g_i \widehat{\mathcal{O}}^\times, \quad \text{and} \quad G = \coprod_{i=1}^h \Gamma \bar{g}_i U,$$

where $\bar{g}_i$ are the images of g_i in G. Set $I_i := g_i\mathcal{O}$, then $I_1, \dots, I_h$ form a complete set of representatives for ideal classes in $\mathrm{Cl}(\mathcal{O})$.

Let χ_i be the characteristic function for the open compact subset $\Gamma\backslash\Gamma\bar{g}_i U \subset \Gamma\backslash G$. The set $\{\chi_1, \dots, \chi_h\}$ forms a basis for the vector space $L^2(\Gamma\backslash G/U)$. Let f be the characteristic function of $U(\mathfrak{n})$, which is an element in $\mathcal{H}(G, U)$, and hence $R(f)$ is a linear operator on $L^2(\Gamma\backslash G/U)$. Write

$$R(f) \sim (a_{ij})$$

for the representing matrix with respect to the basis $\{\chi_i\}$. One has

$$R(f)(\chi_j) = \sum_{i=1}^h a_{ij}\chi_i.$$

One computes

$$R(f)(\chi_j)(x) = \int_G f(g)\chi_j(xg)dg = \int_{U(\mathfrak{n})} \chi_j(xg)dg.$$

Thus,

$$a_{ij} = R(f)(\chi_j)(\bar{g}_i) = \int_{U(\mathfrak{n})} \chi_j(\bar{g}_i g)dg = \int_{U_{ij}} dg = \mathrm{vol}(U_{ij}),$$

where

$$U_{ij} := \{g \in U(\mathfrak{n}) \,|\, \bar{g}_i g \in \Gamma\bar{g}_j U\}.$$

Each U_{ij} is invariant under the right translation of U. For each fixed i with $1 \le i \le h$, the set $U(\mathfrak{n})$ is the disjoint union of U_{ij} for $j = 1, \dots, h$. For $g \in U_{ij}$, one has

$$\bar{g}_i g\mathcal{O} \simeq \bar{g}_j\mathcal{O} = I_j, \quad \text{and} \quad \bar{g}_i g\mathcal{O} \subseteq \bar{g}_i\mathcal{O} = I_i.$$

If one puts $J := \bar{g}_i g\mathcal{O}$, then $\mathrm{Nr}(J) = \mathfrak{n}\,\mathrm{Nr}(I_i)$. As a result we get a bijection

$$U_{ij}/U \simeq \{J \subseteq I_i \,|\, J \simeq I_j,\ \mathrm{Nr}(J) = \mathfrak{n}\,\mathrm{Nr}(I_i)\}, \quad \text{by } g \mapsto \bar{g}_i g\mathcal{O}.$$

Therefore, we get

$$a_{ij} = |U_{ij}/U| = \mathfrak{B}_{ij}(\mathfrak{n}).$$

THEOREM 4.2.1. *Let f be the characteristic function of $U(\mathfrak{n})$ as above. Then the Brandt matrix is the representing matrix of the Hecke operator $R(f)$ with respect to the basis $\chi_1, \dots, \chi_h$ for the vector space $L^2(\Gamma\backslash G/U)$.*

REMARK 4.2.2. In the function field setting where

- F is a global function field with constant field $\mathbb{F}_q$,
- A an S-order (whose normalization is the S-ring of integers), where S is a nonempty finite set of places of F,
- D a definite quaternion F-algebra relative to S, and
- $\mathcal{O}$ a proper A-order in D,

all results in Sections 3-4 make sense and remain valid, possibly except for Theorems 3.3.3 and 3.3.7 and Corollary 3.3.8 in characteristic 2.

5. Mass of Orders.

5.1. Mass formula. We keep the notation and assumptions of Section 3.1. In particular, $\{I_1, \dots, I_h\}$ is a complete set of representatives for the right ideal classes in $\mathrm{Cl}(\mathcal{O})$, and $\mathcal{O}_i = \mathcal{O}_l(I_i)$. Recall that the *mass* of $\mathcal{O}$ is defined by

$$\mathrm{Mass}(\mathcal{O}) = \sum_{i=1}^{h} \frac{1}{w_i}, \qquad w_i = [\mathcal{O}_i^\times : A^\times]. \tag{5.1}$$

The mass of $\mathcal{O}$ is independent of the choices of representatives for $\mathrm{Cl}(\mathcal{O})$.

LEMMA 5.1.1. *Let $G := \widehat{D}^\times/\widehat{A}^\times$, $\Gamma := D^\times/A^\times$ and $U := \widehat{\mathcal{O}}^\times/\widehat{A}^\times$. Then Γ is a discrete cocompact subgroup of G, and for the counting measure on Γ and any Haar measure on G, we have*

$$\mathrm{vol}(\Gamma\backslash G) = \mathrm{vol}(U) \cdot \mathrm{Mass}(\mathcal{O}). \tag{5.2}$$

Proof. By (4.1), one has $h = |\Gamma\backslash G/U|$. Write $G = \coprod_{i=1}^{h} \Gamma g_i U$. Then

$$\mathrm{vol}(\Gamma\backslash G) = \sum_{i=1}^{h} \mathrm{vol}(\Gamma\backslash\Gamma g_i U) = \sum_{i=1}^{h} \frac{\mathrm{vol}(U)}{|\Gamma \cap g_i U g_i^{-1}|}. \tag{5.3}$$

The statement then follows from $[\mathcal{O}_i^\times : A^\times] = |\Gamma \cap g_i U g_i^{-1}|$. ☐

LEMMA 5.1.2. *Let $\mathscr{R} \subseteq \mathcal{O}$ be two $\mathbb{Z}$-orders in D with centers R and A, respectively. Then*

$$\mathrm{Mass}(\mathscr{R}) = \mathrm{Mass}(\mathcal{O}) \frac{[\widehat{\mathcal{O}}^\times : \widehat{\mathscr{R}}^\times]}{[A^\times : R^\times]}. \tag{5.4}$$

Proof. Let $G_1 := \widehat{D}^\times/\widehat{A}^\times$, $\Gamma_1 := D^\times/A^\times$, $U_1 := \widehat{\mathcal{O}}^\times/\widehat{A}^\times$. We define G_2, Γ_2 and U_2 for the order $\mathscr{R}$ similarly. The map $G_2 \to G_1$ is a finite cover with degree $[\widehat{A}^\times : \widehat{R}^\times]$ and $\Gamma_2 \to \Gamma_1$ is a finite cover of degree $[A^\times : R^\times]$. Therefore, one gets

$$\mathrm{vol}(\Gamma_2\backslash G_2) = \mathrm{vol}(\Gamma_1\backslash G_1) \frac{[\widehat{A}^\times : \widehat{R}^\times]}{[A^\times : R^\times]}.$$

On the other hand, $\mathrm{vol}(U_1)/\mathrm{vol}(U_2) = [\widehat{\mathcal{O}}^\times : \widehat{\mathscr{R}}^\times]/[\widehat{A}^\times : \widehat{R}^\times]$. The lemma now follows from Lemma 5.1.1. □

Let $\mathcal{O}_{\max}$ be a maximal order in D containing $\mathcal{O}$. The mass formula [27, Chapter V, Corollary 2.3] states that

$$\mathrm{Mass}(\mathcal{O}_{\max}) = \frac{1}{2^{n-1}}|\zeta_F(-1)|h(F)\prod_{\mathfrak{p}|\mathfrak{D}}(N(\mathfrak{p})-1), \tag{5.5}$$

where $\zeta_F(s)$ is the Dedekind zeta-function of F, $\mathfrak{D} \subseteq O_F$ is the reduced discriminant of D over F, and $\mathfrak{p}$ ranges over all finite primes of F dividing $\mathfrak{D}$. Using Lemma 5.1.2, one easily derives the relative mass formula

$$\begin{aligned}\mathrm{Mass}(\mathcal{O}) &= \mathrm{Mass}(\mathcal{O}_{\max})\cdot\frac{[\widehat{\mathcal{O}}_{\max}^\times : \widehat{\mathcal{O}}^\times]}{[O_F^\times : A^\times]}\\ &= \frac{1}{2^{n-1}}|\zeta_F(-1)|h(F)\prod_{\mathfrak{p}|\mathfrak{D}}(N(\mathfrak{p})-1)\cdot\frac{[\widehat{\mathcal{O}}_{\max}^\times : \widehat{\mathcal{O}}^\times]}{[O_F^\times : A^\times]}.\end{aligned} \tag{5.6}$$

5.2. Special cases. Let $F = \mathbb{Q}(\sqrt{p})$, where p is a prime number, and $D = D_{\infty_1,\infty_2}$, the totally definite quaternion F-algebra ramified only at the archimedean places $\{\infty_1, \infty_2\}$. Let $\mathbb{O}_1$ be a maximal O_F-order in D and $A = \mathbb{Z}[\sqrt{p}] \subseteq O_F$. By (5.5), the mass of $\mathbb{O}_1$ is

$$\mathrm{Mass}(\mathbb{O}_1) = \frac{1}{2}\zeta_F(-1)\,h(F). \tag{5.7}$$

5.2.1. **Mass of $\mathbb{O}_r$, $r = 8, 16$.** Assume that $p \equiv 1 \pmod 4$ for the rest of this subsection. In this case $A \neq O_F$, and $A/2O_F \cong \mathbb{F}_2$. Let $\mathbb{O}_8, \mathbb{O}_{16} \subset \mathbb{O}_1$ be the proper A-orders such that

$$(\mathbb{O}_8)_2 := \mathbb{O}_8 \otimes_{\mathbb{Z}} \mathbb{Z}_2 = \begin{pmatrix} A_2 & 2O_{F_2} \\ O_{F_2} & O_{F_2}\end{pmatrix}, \qquad (\mathbb{O}_{16})_2 = \mathrm{Mat}_2(A_2), \tag{5.8}$$

$$(\mathbb{O}_r)_\ell = (\mathbb{O}_1)_\ell \qquad \forall\,\text{prime } \ell \neq 2, \quad r \in \{8, 16\}. \tag{5.9}$$

The order $\mathbb{O}_r \subset \mathbb{O}_1$ is of index r.

We claim that $\mathrm{Nr}_A(\mathbb{O}_8) = O_F \neq A$. It is enough to show that $\mathrm{Nr}_{A_\ell}((\mathbb{O}_8)_\ell) = (O_F)_\ell$ for all primes ℓ, which follows from (5.8) for $\ell = 2$, and (5.9) for the rest of the primes.

Put $\varpi := [O_F^\times : A^\times]$. By [32, Section 4.2], we have $\varpi \in \{1, 3\}$, and $\varpi = 1$ if $p \equiv 1 \pmod 8$. By formula (5.6), one has

$$\mathrm{Mass}(\mathbb{O}_r) = \mathrm{Mass}(\mathbb{O}_1)\frac{[(\mathbb{O}_1/2\mathbb{O}_1)^\times : (\mathbb{O}_r/2\mathbb{O}_1)^\times]}{\varpi}, \quad r = 8, 16. \tag{5.10}$$

The group $(\mathbb{O}_{16}/2\mathbb{O}_1)^\times \simeq \mathrm{GL}_2(\mathbb{F}_2)$ and hence $|(\mathbb{O}_{16}/2\mathbb{O}_1)^\times| = 6$.

Suppose that $p \equiv 1 \pmod 8$. The group $(\mathbb{O}_1/2\mathbb{O}_1)^\times \simeq \mathrm{GL}_2(\mathbb{F}_2) \times \mathrm{GL}_2(\mathbb{F}_2)$ is of order 36. By (5.10) we have $\mathrm{Mass}(\mathbb{O}_{16}) = 6\,\mathrm{Mass}(\mathbb{O}_1)$. For the order $\mathbb{O}_8$ one has

$$\mathbb{O}_8/2\mathbb{O}_1 \simeq \begin{pmatrix} \mathbb{F}_2 & 0 \\ \mathbb{F}_2\times\mathbb{F}_2 & \mathbb{F}_2\times\mathbb{F}_2\end{pmatrix},$$

and hence $|(\mathbb{O}_8/2\mathbb{O}_1)^\times| = 4$. Therefore by (5.10) we have $\mathrm{Mass}(\mathbb{O}_8) = 9\ \mathrm{Mass}(\mathbb{O}_1)$.

Suppose now that $p \equiv 5 \pmod 8$. The group $(\mathbb{O}_1/2\mathbb{O}_1)^\times \simeq \mathrm{GL}_2(\mathbb{F}_4)$ is of order 180. Thus, $\mathrm{Mass}(\mathbb{O}_{16}) = 30/\varpi \cdot \mathrm{Mass}(\mathbb{O}_1)$. Since

$$\mathbb{O}_8/2\mathbb{O}_1 \simeq \begin{pmatrix} \mathbb{F}_2 & 0 \\ \mathbb{F}_4 & \mathbb{F}_4 \end{pmatrix},$$

we have $|(\mathbb{O}_8/2\mathbb{O}_1)^\times| = 12$. Thus, $\mathrm{Mass}(\mathbb{O}_8) = 15/\varpi \cdot \mathrm{Mass}(\mathbb{O}_1)$ by (5.10).

In summary,

$$\begin{aligned} \mathrm{Mass}(\mathbb{O}_8) &= \begin{cases} 9/2 \cdot \zeta_F(-1)\, h(F) & \text{for } p \equiv 1 \pmod 8; \\ (15/2\varpi) \cdot \zeta_F(-1)\, h(F) & \text{for } p \equiv 5 \pmod 8; \end{cases} \\ \mathrm{Mass}(\mathbb{O}_{16}) &= \begin{cases} 3\,\zeta_F(-1)\, h(F) & \text{for } p \equiv 1 \pmod 8; \\ (15/\varpi) \cdot \zeta_F(-1)\, h(F) & \text{for } p \equiv 5 \pmod 8. \end{cases} \end{aligned} \tag{5.11}$$

6. Supersingular abelian surfaces.

6.1. Isomorphism classes. Let $\pi = \sqrt{p}$ and X_π an abelian variety over $\mathbb{F}_p$ corresponding to the Weil number π. Let $\mathrm{Isog}(X_\pi)$ denote the set of $\mathbb{F}_p$-isomorphism classes of abelian varieties in the isogeny class of X_π over $\mathbb{F}_p$. It is known that the endomorphism algebra D of X_π over $\mathbb{F}_p$ is isomorphic to the totally definite quaternion algebra $D = D_{\infty_1,\infty_2}$ over $F = \mathbb{Q}(\sqrt{p}\,)$ defined in Section 5.2. We also recall the orders $\mathbb{O}_1, \mathbb{O}_8, \mathbb{O}_{16}$ introduced there. The endomorphism ring of each member X in $\mathrm{Isog}(X_\pi)$ may be regarded as an order in D, uniquely determined up to an inner automorphism of D. Let $\mathfrak{O}_r$ denote the genus consisting of the orders in D that are locally isomorphic to $\mathbb{O}_r$ at every prime ℓ. If $p \equiv 1 \pmod 4$, then $A = \mathbb{Z}[\sqrt{p}\,] \subset O_F$ is a suborder of index 2 in O_F.

We will need the following result, which is a special case of [35, Theorem 2.2].

PROPOSITION 6.1.1. *Let X_0 be an abelian variety over a finite field $\mathbb{F}_q$ and $\mathcal{R} := \mathrm{End}_{\mathbb{F}_q}(X_0)$ the endomorphism ring of X_0. Then there is a natural bijection from the set $\mathrm{Cl}(\mathcal{R})$ to the set of $\mathbb{F}_q$-isomorphism classes of abelian varieties X satisfying the following three conditions*

(a) *X is isogenous to X_0 over $\mathbb{F}_q$,*

(b) *the Tate module $T_\ell(X)$ is isomorphic to $T_\ell(X_0)$ as $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-modules for all primes $\ell \neq p$,*

(c) *the Dieudonné module $M(X)$ of X is isomorphic to $M(X_0)$.*

THEOREM 6.1.2.

(a) *Suppose that $p \not\equiv 1 \pmod 4$. The endomorphism ring of any member X in $\mathrm{Isog}(X_\pi)$ is a maximal order in D. Moreover, there is a bijection between the set $\mathrm{Isog}(X_\pi)$ with the set $\mathrm{Cl}(\mathbb{O}_1)$ of ideal classes.*

(b) *Suppose that $p \equiv 1 \pmod 4$. The endomorphism ring $\mathrm{End}(X)$ of any member X in $\mathrm{Isog}(X_\pi)$ belongs to $\mathfrak{O}_r$ for some $r = 1, 8, 16$. Moreover, for each $r \in \{1, 8, 16\}$ the set of members X in $\mathrm{Isog}(X_\pi)$ with $\mathrm{End}(X) \in \mathfrak{O}_r$ is in bijection with the set $\mathrm{Cl}(\mathbb{O}_r)$ of ideal classes. In particular, there is a bijection $\mathrm{Isog}(X_\pi) \simeq \coprod_{r=1,8,16} \mathrm{Cl}(\mathbb{O}_r)$.*

Proof. Part (a) has been proven in [28, Theorem 6.2]. We prove part (b) where $p \equiv 1 \pmod 4$. By Proposition 6.1.1, one is reduced to classify the Tate modules and Dieudonné modules of members X in $\mathrm{Isog}(X_\pi)$. Since the ground field is $\mathbb{F}_p$, the

Dieudonné module $M(X)$ of X is simply an A_p-module in F_p^2. As A_p is the maximal order in F_p, there is only one such isomorphism class and its endomorphism ring is a maximal order in $\mathrm{Mat}_2(F_p)$. The Tate module $T_\ell(X)$ of X is simply an A_ℓ-module. Therefore, when $\ell \neq 2$, there is only one such isomorphism class and its endomorphism ring is again a maximal order in $\mathrm{Mat}_2(F_\ell)$. Now we consider the case where $\ell = 2$. Since $2O_{F_2} \subset A_2 \subset O_{F_2}$, the order A_2 is Bass and hence the classification of A_2-modules is known; see [2]. It follows that the Tate module $T_2(X)$ of X is isomorphic to one of the following three A_2-lattices in F_2^2:

$$L_1 = O_{F_2}^2, \quad L_2 = A_2 \oplus O_{F_2}, \quad L_4 = A_2^2, \tag{6.1}$$

(also see [36, Corollary 5.2] for a direct classification). One easily computes that $\mathrm{End}_{A_2}(L_1) = (\mathbb{O}_1)_2$, $\mathrm{End}_{A_2}(L_2) = (\mathbb{O}_8)_2$ and $\mathrm{End}_{A_2}(L_4) = (\mathbb{O}_{16})_2$. If we let X_1, X_8, X_{16} be members in $\mathrm{Isog}(X_\pi)$ representing these three classes respectively and let $\mathcal{R}_r := \mathrm{End}(X_r)$, then each $\mathcal{R}_r \in \mathfrak{O}_r$ and the set of members X in $\mathrm{Isog}(X_\pi)$ defined as in Proposition 6.1.1 is isomorphic to $\mathrm{Cl}(\mathcal{R}_r) \simeq \mathrm{Cl}(\mathbb{O}_r)$. This proves part (b). □

6.2. Computation of class numbers. In this subsection, we give explicit class number formulas for the orders $\mathbb{O}_1$, $\mathbb{O}_8$ and $\mathbb{O}_{16}$ arising from the study of supersingular abelian surfaces in the isogeny class corresponding to $\pi = \sqrt{p}$. Recall that $\mathbb{O}_8$ and $\mathbb{O}_{16}$ come into consideration only when $p \equiv 1 \pmod 4$. Let $Z(\mathbb{O}_r)$ be the center of $\mathbb{O}_r$. We have $Z(\mathbb{O}_1) = O_F$, and $Z(\mathbb{O}_r) = \mathbb{Z}[\sqrt{p}] \neq O_F$ for $r = 8, 16$ when $p \equiv 1 \pmod 4$. For the rest of this subsection we write A for the order $\mathbb{Z}[\sqrt{p}]$ when $p \equiv 1 \pmod 4$. Recall (Section 5.2.1) that $\varpi = [O_F^\times : A^\times] \in \{1, 3\}$, and $\varpi = 1$ if $p \equiv 1 \pmod 8$. As mentioned at the start of Section 2, *quadratic orders* refer exclusively to those whose fractional fields are CM-extensions of F.

By the class number formula (3.25),

$$h(\mathbb{O}_r) = \mathrm{Mass}(\mathbb{O}_r) + \mathrm{Ell}(\mathbb{O}_r) \qquad \text{for } r = 1, 8, 16.$$

The mass part $\mathrm{Mass}(\mathbb{O}_r)$ has already been calculated in Section 5.2. We focus on the elliptic part

$$\mathrm{Ell}(\mathbb{O}_r) = \frac{1}{2} \sum_B (2 - \delta(B)) h(B)(1 - w(B)^{-1}) \prod_\ell m(B_\ell, (\mathbb{O}_r)_\ell, (\mathbb{O}_r)_\ell^\times),$$

where B runs over all the (non-isomorphic) quadratic proper $Z(\mathbb{O}_r)$-orders with

$$w(B) = [B^\times : Z(\mathbb{O}_r)^\times] > 1, \tag{6.2}$$

and $\delta(B)$ is given by (3.23), i.e. it is 1 if B is closed under the complex conjugation, and 0 otherwise.

The detailed classification of all the orders B is given in a separate paper [32], and we only summarize its results below. For this purpose some more notation needs to be introduced.

6.2.1. **Notations of fields[1] and orders**. Let $K_j = \mathbb{Q}(\sqrt{p}, \sqrt{-j})$ with $j \in \{1, 2, 3\}$. One can show that

- for $p > 5$, all quadratic O_F-orders B with $[B^\times : O_F^\times] > 1$ lie in K_j for some $j \in \{1, 2, 3\}$;

[1]If we need the 2-adic completion of a number field K, we will write $K \otimes_{\mathbb{Q}} \mathbb{Q}_2$ instead of K_2 for the rest of the paper. Similarly for 3-adic completions.

- for $p \equiv 1 \pmod 4$, all quadratic proper A-orders B with $[B^\times : A^\times] > 1$ lie in either K_1 or K_3;

see [32] for more details.

We adopt the convention that $B_{j,k}$ is an order in K_j with index k in O_{K_j}. The non-maximal suborders of O_{K_j} that we will consider are:

$$B_{1,2} := \mathbb{Z} + \mathbb{Z}\sqrt{p} + \mathbb{Z}\sqrt{-1} + \mathbb{Z}(1+\sqrt{-1})(1+\sqrt{p})/2, \qquad B_{1,4} := \mathbb{Z}[\sqrt{p}, \sqrt{-1}],$$
$$B_{3,4} := \mathbb{Z}[\sqrt{p}, \zeta_6] \qquad \text{if } p \equiv 1 \pmod 4;$$
$$B_{3,2} := A[\epsilon\zeta_6] \qquad \text{if } p \equiv 5 \pmod 8 \quad \text{and} \quad \varpi = 3.$$

Here $B_{3,2}$ is the suborder of O_{K_3} generated by $\epsilon\zeta_6$ over A, where $\epsilon \in O_F^\times$ is the fundamental unit of F. With the exception of $B_{3,2}$, all the other orders above are closed under the complex conjugation.

Given a number field K, the class number of an arbitrary order $B \subseteq O_K$ of conductor $\mathfrak{f}$ can be computed by the following formula [20, Theorem I.12.12]

$$h(B) = \frac{h(O_K)[(O_K/\mathfrak{f})^\times : (B/\mathfrak{f})^\times]}{[O_K^\times : B^\times]}. \tag{6.3}$$

Lemma 6.2.2. *Assume that $p \equiv 1 \pmod 4$. If $B \in \{B_{1,2}, B_{1,4}, B_{3,4}, B_{3,2}\}$, then B is a Bass order.*

Proof. By a theorem of Borevich and Faddeev [3] (cf. Curtis-Reiner [9, Section 37, p. 789]), B is Bass if and only if the B-module O_K/B is generated by one element. In particular, if B is of prime index in O_K then B is Bass. This shows that $B_{1,2}$ and $B_{3,2}$ are Bass orders. Since $O_{K_1} = \mathbb{Z}[\sqrt{-1}, (1+\sqrt{p})/2]$, the quotient $O_{K_1}/B_{1,4}$ is generated by $(1+\sqrt{p})/2$ as a $B_{1,4}$-module. Hence $B_{1,4}$ is a Bass order. Since 2 is inert in $\mathbb{Z}[\zeta_6]$, one has $O_{K_3}/B_{3,4} \simeq \mathbb{F}_4$ as $\mathbb{Z}[\zeta_6]/(2) \simeq \mathbb{F}_4$-modules. This proves that $B_{3,4}$ is also a Bass order. □

6.2.3. **Class number formula for $\mathbb{O}_1$ when $p > 5$.** Since $\mathbb{O}_1$ is a maximal order and D_{∞_1,∞_2} splits at all the finite places, we have $m(B_\ell, (\mathbb{O}_1)_\ell, (\mathbb{O}_1)_\ell^\times) = 1$ for all ℓ (see [27, p. 94] or Section 3.4). It follows that

$$\mathrm{Ell}(\mathbb{O}_1) = \frac{1}{2} \sum_{w(B)>1} h(B)(1 - w(B)^{-1}), \tag{6.4}$$

where $w(B) = [B^\times : O_F^\times]$, and the summation is over all isomorphism classes of quadratic O_F-orders B with $w(B) > 1$.

When $p \equiv 1 \pmod 4$ and $p > 5$, the only orders with nonzero contributions to the elliptic part $\mathrm{Ell}(\mathbb{O}_1)$ are O_{K_1} and O_{K_3}, with $w(O_{K_1}) = 2$ and $w(O_{K_3}) = 3$ respectively. We have

$$h(\mathbb{O}_1) = \frac{1}{2} h(F)\zeta_F(-1) + h(K_1)/4 + h(K_3)/3 \quad \text{if } p \equiv 1 \pmod 4,\ p > 5. \tag{6.5}$$

When $p \equiv 3 \pmod 4$ and $p \geq 7$, we compute the following numerical invariants of all orders B in some K_j with $w(B) > 1$:

$p \equiv 3 \pmod 4$	O_{K_1}	$B_{1,2}$	$B_{1,4}$	O_{K_2}	O_{K_3}
$h(B)$	$h(K_1)$	$\left(2-\left(\frac{2}{p}\right)\right)h(K_1)$	$\left(2-\left(\frac{2}{p}\right)\right)h(K_1)$	$h(K_2)$	$h(K_3)$
$w(B)$	4	4	2	2	3

Therefore, we have

$$h(\mathbb{O}_1) = \frac{1}{2}h(F)\zeta_F(-1) + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(K_1)}{8} + \frac{1}{4}h(K_2) + \frac{1}{3}h(K_3) \tag{6.6}$$

if $p \equiv 3 \pmod 4$ and $p \geq 7$.

6.2.4. **Class number formula for $\mathbb{O}_8$ and $\mathbb{O}_{16}$ when $p \equiv 1 \pmod 4$.** Since $(\mathbb{O}_r)_\ell$ is maximal for all $\ell \neq 2$ and $r \in \{8, 16\}$, we have

$$\mathrm{Ell}(\mathbb{O}_r) = \frac{1}{2}\sum_{w(B)>1}(2-\delta(B))h(B)(1-w(B)^{-1})m(B_2,(\mathbb{O}_r)_2,(\mathbb{O}_r)_2^\times), \tag{6.7}$$

where $w(B) = [B^\times : A^\times]$ and the summation is over all isomorphism classes of quadratic proper A-orders B with $w(B) > 1$. For simplicity, we will write $m_{2,r}(B) := m(B_2,(\mathbb{O}_r)_2,(\mathbb{O}_r)_2^\times)$ for $r = 8, 16$, where $(\mathbb{O}_r)_2 = \mathbb{O}_r \otimes_{\mathbb{Z}} \mathbb{Z}_2$ and $B_2 = B \otimes_{\mathbb{Z}} \mathbb{Z}_2$. The numerical invariants of all proper A-orders B with $w(B) > 1$ are given by the following table:

$p \equiv 1 \pmod 4$	$B_{1,2}$	$B_{1,4}$	$B_{3,4}$	$B_{3,2}$
$h(B)$	$\frac{1}{\varpi}\left(2-\left(\frac{2}{p}\right)\right)h(K_1)$	$\frac{2}{\varpi}\left(2-\left(\frac{2}{p}\right)\right)h(K_1)$	$3h(K_3)/\varpi$	$h(K_3)$
$w(B)$	2	2	3	3
$m_{2,8}(B)$	1	0	0	1
$m_{2,16}(B)$	0	1	1	0
$\delta(B)$	1	1	1	0

Here $B_{3,2}$ is a proper A-order only if $p \equiv 5 \pmod 8$ and $\varpi = 3$, in which case $\delta(B_{3,2}) = 0$. The numbers of conjugacy classes of 2-adic optimal embeddings $m_{2,r}(B)$ will be calculated in the next subsection.

For the explicit class number formulas of $\mathbb{O}_8$ and $\mathbb{O}_{16}$, it is more convenient to separate into cases. If $p \equiv 1 \pmod 8$, then

$$h(\mathbb{O}_8) = \frac{9}{2}\zeta_F(-1)h(F) + \frac{1}{4}h(K_1), \tag{6.8}$$

$$h(\mathbb{O}_{16}) = 3\zeta_F(-1)h(F) + \frac{1}{2}h(K_1) + h(K_3). \tag{6.9}$$

If $p \equiv 5 \pmod 8$, then

$$h(\mathbb{O}_8) = \frac{15}{2\varpi}\zeta_F(-1)h(F) + \frac{3}{4\varpi}h(K_1) + \frac{2\delta_{3,\varpi}}{\varpi}h(K_3), \tag{6.10}$$

$$h(\mathbb{O}_{16}) = \frac{15}{\varpi}\zeta_F(-1)h(F) + \frac{3}{2\varpi}h(K_1) + \frac{1}{\varpi}h(K_3), \tag{6.11}$$

where $\delta_{3,\varpi}$ is the Kronecker δ-symbol.

6.2.5. **Numbers of conjugacy classes of 2-adic optimal embeddings.** Assume that $p \equiv 1 \pmod 4$, and B is an order in the list $\{B_{1,2}, B_{1,4}, B_{3,4}, B_{3,2}\}$. According to Lemma 6.2.2, B is a Bass order. Recall that

$$(\mathbb{O}_8)_2 = \mathrm{End}_{A_2}(A_2 \oplus O_{F_2}), \qquad (\mathbb{O}_{16})_2 = \mathrm{End}_{A_2}(A_2^2)$$

by the proof of Theorem 6.1.2. It follows from Lemma 3.4.1 that $m_{2,r}(B) \in \{0, 1\}$ for $r = 8, 16$, and

$$\begin{aligned} m_{2,8}(B) = 1 &\iff B_2 \simeq A_2 \oplus O_{F_2}, \\ m_{2,16}(B) = 1 &\iff B_2 \simeq A_2 \oplus A_2. \end{aligned}$$

Since A_2 is a Bass order, B_2 is isomorphic to one of the lattices given in (6.1). However, $B_2 \not\simeq O_{F_2} \oplus O_{F_2}$ as B_2 is a proper A_2-order. Note that $O_F B = O_K$, where the product is taken inside the fraction field K of B. Hence $B_2 \otimes_{A_2} (A_2/2O_{F_2}) \cong B_2/2(O_K \otimes_{\mathbb{Z}} \mathbb{Z}_2) \cong B/2O_K$. By looking at the tensor product of B_2 with $(A_2/2O_{F_2})$ for each B, we get the following isomorphisms of A_2-modules

$$(B_{1,2})_2 \simeq (B_{3,2})_2 \simeq A_2 \oplus O_{F_2}, \quad (B_{1,4})_2 \simeq (B_{3,4})_2 \simeq A_2 \oplus A_2.$$

As a result, we have

$$m_{2,8}(B_{1,2}) = 1,\ m_{2,16}(B_{1,2}) = 0,\ m_{2,8}(B_{1,4}) = 0,\ m_{2,16}(B_{1,4}) = 1,$$

$$m_{2,8}(B_{3,4}) = 0,\ m_{2,16}(B_{3,4}) = 1,\ m_{2,8}(B_{3,2}) = 1,\ m_{2,16}(B_{3,2}) = 0.$$

6.2.6. **Special zeta-values.** Let $\mathfrak{d}_F$ be the discriminant of $F = \mathbb{Q}(\sqrt{p})$. By Siegel's formula [37, Table 2, p. 70],

$$\zeta_F(-1) = \frac{1}{60} \sum_{\substack{b^2+4ac=\mathfrak{d}_F \\ a,c>0}} a, \tag{6.12}$$

where $b \in \mathbb{Z}$ and $a, c \in \mathbb{N}_{>0}$.

It remains to calculate the class numbers of $\mathbb{O}_1$ when $p = 2, 3, 5$. This has already been done in [16] by computer. We list the results here for the sake of completeness.

6.2.7. **Class number of $\mathbb{O}_1$ for $p = 2$.** In this case $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{-1}) = \mathbb{Q}(\zeta_8)$. Besides O_{K_1} and O_{K_3}, we also need to consider the order $\mathbb{Z}[\sqrt{2}, \sqrt{-1}]$, which is of index 2 in O_{K_1}. The orders with nonzero contributions to $\mathrm{Ell}(\mathbb{O}_1)$ are

$p=2$	$\mathbb{Z}[\zeta_8]$	$\mathbb{Z}[\sqrt{2}, \sqrt{-1}]$	$\mathbb{Z}[\sqrt{2}, \zeta_6]$
$h(B)$	1	1	1
$w(B)$	4	2	3

Since $\zeta_{\mathbb{Q}(\sqrt{2})}(-1) = 1/12$ by (6.12) and $h(\mathbb{Q}(\sqrt{2})) = 1$,

$$\begin{aligned} h(\mathbb{O}_1) &= \frac{1}{2} h(\mathbb{Q}(\sqrt{2}))\zeta_{\mathbb{Q}(\sqrt{2})}(-1) + \frac{1}{2}\left(\left(1 - \frac{1}{4}\right) + \left(1 - \frac{1}{2}\right) + \left(1 - \frac{1}{3}\right)\right) \\ &= \frac{1}{24} + \frac{23}{24} = 1 \qquad \text{when } p = 2. \end{aligned} \tag{6.13}$$

6.2.8. **Class number of $\mathbb{O}_1$ for $p=3$.** In this case, we have $K_1 = K_3 = \mathbb{Q}(\zeta_{12})$. Besides the orders listed in the table of Section 6.2.3, we also need to consider the order $B_{1,3} := \mathbb{Z}[\sqrt{3}, \zeta_6]$. The table becomes

$p=3$	O_{K_1}	$B_{1,2}$	$B_{1,4}$	$B_{1,3}$	O_{K_2}
$h(B)$	1	1	1	1	2
$w(B)$	12	4	2	3	2

Hence

$$\mathrm{Ell}(\mathbb{O}_1) = \frac{1}{2}\left(\left(1-\frac{1}{12}\right)+\left(1-\frac{1}{4}\right)+\left(1-\frac{1}{2}\right)+\left(1-\frac{1}{3}\right)+2\left(1-\frac{1}{2}\right)\right) = \frac{23}{12}.$$

Using (6.12) again, $\zeta_{\mathbb{Q}(\sqrt{3})}(-1) = 1/6$. Since $h(\mathbb{Q}(\sqrt{3}))=1$,

$$h(\mathbb{O}_1) = \frac{1}{2}h(\mathbb{Q}(\sqrt{3}))\zeta_{\mathbb{Q}(\sqrt{3})}(-1) + \mathrm{Ell}(\mathbb{O}_1) = \frac{1}{12}+\frac{23}{12} = 2 \qquad \text{when } p=3. \quad (6.14)$$

6.2.9. **Class number of $\mathbb{O}_1$ for $p=5$.** In this case we also need to consider the field $\mathbb{Q}(\zeta_{10})$. The maximal order $\mathbb{Z}[\zeta_{10}] \subset \mathbb{Q}(\zeta_{10})$ is the only order whose unit group is strictly larger than $O_F^\times$. The orders needed for the calculation of $\mathrm{Ell}(\mathbb{O}_1)$ are

$p=5$	O_{K_1}	O_{K_3}	$\mathbb{Z}[\zeta_{10}]$
$h(B)$	1	1	1
$w(B)$	2	3	5

Since $\zeta_{\mathbb{Q}(\sqrt{5})}(-1) = 1/30$ by (6.12) and $h(\mathbb{Q}(\sqrt{5}))=1$,

$$\begin{aligned} h(\mathbb{O}_1) &= \frac{1}{2}h(\mathbb{Q}(\sqrt{5}))\zeta_{\mathbb{Q}(\sqrt{5})}(-1) + \frac{1}{2}\left(\left(1-\frac{1}{2}\right)+\left(1-\frac{1}{3}\right)+\left(1-\frac{1}{5}\right)\right) \\ &= \frac{1}{60}+\frac{59}{60} = 1 \qquad \text{when } p=5. \end{aligned} \quad (6.15)$$

The results on the class number of $\mathbb{O}_1$ can be summarized as follows.

Proposition 6.2.10. *Let $D = D_{\infty_1,\infty_2}$ be the quaternion algebra over $F = \mathbb{Q}(\sqrt{p})$ ramified only at the two real places of F. The class number $h(D)$ (i.e. the class number of any maximal order in D) is given below:*

(1) $h(D) = 1, 2, 1$ for $p = 2, 3, 5$, respectively;
(2) if $p \equiv 1 \pmod 4$ and $p \neq 5$, $h(D) = h(F)\zeta_F(-1)/2 + h(K_1)/4 + h(K_3)/3$;
(3) if $p \equiv 3 \pmod 4$ and $p \neq 3$, then

$$h(D) = \frac{1}{2}h(F)\zeta_F(-1) + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(K_1)}{8} + \frac{1}{4}h(K_2) + \frac{1}{3}h(K_3).$$

Proof of Theorem 1.2. By definition, $H(p) = |\mathrm{Isog}(X_\pi)|$, so it follows from Theorem 6.1.2 that

$$H(p) = \begin{cases} h(\mathbb{O}_1) + h(\mathbb{O}_8) + h(\mathbb{O}_{16}) & \text{if } p \equiv 1 \pmod 4; \\ h(\mathbb{O}_1) & \text{if } p \equiv 3 \pmod 4 \quad \text{or} \quad p=2. \end{cases}$$

The explicit formulas for $h(\mathbb{O}_1)$ when $p=2$ and $p \equiv 3 \pmod 4$ have already been given above.

Suppose that $p = 5$. We have $h(\mathbb{O}_1) = 1$ by Section 6.2.9. The fundamental unit $\epsilon = (1+\sqrt{5})/2 \notin \mathbb{Z}[\sqrt{5}]$, so $\varpi = 3$. By (6.10) and (6.11) respectively, $h(\mathbb{O}_8) = h(\mathbb{O}_{16}) = 1$. Hence $H(p) = 3$ if $p = 5$.

Suppose that $p \equiv 1 \pmod 8$. Combining (6.5), (6.8) and (6.9), we get

$$H(p) = h(\mathbb{O}_1) + h(\mathbb{O}_8) + h(\mathbb{O}_{16}) = 8\zeta_F(-1)h(F) + h(K_1) + \frac{4}{3}h(K_3).$$

Lastly, suppose that $p \equiv 5 \pmod 8$ and $p > 5$. Note that $2\delta_{3,\varpi}/\varpi + 1/\varpi = 1$ for $\varpi = 1, 3$. We obtain

$$\begin{aligned} H(p) &= \left(\frac{1}{2} + \frac{15}{2\varpi} + \frac{15}{\varpi}\right)\zeta_F(-1)h(F) + \left(\frac{1}{4} + \frac{3}{4\varpi} + \frac{3}{2\varpi}\right)h(K_1) + \frac{4}{3}h(K_3) \\ &= \left(\frac{45+\varpi}{2\varpi}\right)\zeta_F(-1)h(F) + \frac{9+\varpi}{4\varpi}h(K_1) + \frac{4}{3}h(K_3) \end{aligned}$$

by combining (6.5), (6.10) and (6.11). □

REMARK 6.2.11. For every square-free integer $m \in \mathbb{Z}$, let us write $h(m)$ for the class number of $\mathbb{Q}(\sqrt{m})$. It follows from the work of Herglotz [11] that for every $p \geq 5$ and $j \in \{1, 2, 3\}$, we have $h(K_j) = \nu h(F)h(-pj)$ with $\nu \in \{1, 1/2\}$ (see [32, Section 2.10]). Hence one may factor out $h(F)$ in the results of Theorem 1.2 and Proposition 6.2.10. For example, we get

$$\frac{h(D)}{h(F)} = \frac{\zeta_F(-1)}{2} + \frac{h(-p)}{8} + \frac{h(-3p)}{6} \tag{6.16}$$

for $p > 5$ and $p \equiv 1 \pmod 4$, and

$$\frac{h(D)}{h(F)} = \frac{\zeta_F(-1)}{2} + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-2p)}{4} + \frac{h(-3p)}{6} \tag{6.17}$$

for $p > 5$ and $p \equiv 3 \pmod 4$.

After the first version of this paper appeared on the web, M. Peters kindly informed us that the formulas in the right hand sides of (6.16) and (6.17) coincide with formulas for the proper class number $H^+(\mathfrak{d}_F)$ of even definite quaternary quadratic forms of discriminant $\mathfrak{d}_F$ (see [7, p. 85 and p. 95]), where $\mathfrak{d}_F$ is the discriminant of $F = \mathbb{Q}(\sqrt{p})$. That is, we have

$$h(D) = h(F)\,H^+(\mathfrak{d}_F) \quad \text{for all primes } p > 5. \tag{6.18}$$

Particularly, the number $h(D)/h(F)$ is always an integer. The above formula for $H^+(\mathfrak{d}_F)$ is obtained by Kitaoka [17] for primes $p \equiv 1 \pmod 4$ and by Ponomarev [22, 23] for all primes p.

Inspired by Peters' comment, we chased the literature and discovered that formula (2) of Proposition 6.2.10 was already obtained in [21], and later that Vignéras [26] has given explicit formulas for the class number of the totally definite quaternion algebra D_m over any real quadratic $\mathbb{Q}(\sqrt{m})$ unramified at all the finite places, where $m > 1$ is a square-free integer. To see that formula (3) of Proposition 6.2.10 follows from [26, Theorem 3.1] when $m = p \equiv 3 \pmod 4$, one would need to know that $\mathbb{Q}(\sqrt{p}, \sqrt{-\epsilon}) = \mathbb{Q}(\sqrt{p}, \sqrt{-2})$ and that $O_F[\sqrt{-\epsilon}]$ is the maximal order. But it is not difficult to prove them (for example, see a proof in [32]). Thus, Proposition 6.2.10

is known due to [26]. Nevertheless, for the sake of completeness and the reader's convenience, we keep the presentation for Proposition 6.2.10 as an exposition.

We should point out that the proof for [26, Prop. 2.2] given in the original paper is incomplete. This proposition is proved based on the author's computation of class numbers ([26, Theorem 3.1]) and the remark below Corollary 1.1 loc. cit. p. 82, which states that if the degree of the totally real field k is even, then $H_{1,1} = h_k T_{1,1}$ and hence $H_{1,1}/h_k$ is an integer (in the notation of [26]). However, the number $H_{1,1}/h_k$ is not always equal to the type number $T_{1,1}$. Nevertheless, it is shown [30] by the first and third named authors of the present paper that $H_{1,1}/h_k$ indeed is always integral, thus completing the proof of [26, Prop. 2.2].

6.3. Asymptotic behavior. We keep the notation and assumptions of Section 3.1. In particular, $\{I_1, \dots, I_h\}$ is a complete set of representatives of the right ideal classes $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O} \subset D$ with center $Z(\mathcal{O}) = A$. The automorphism group $\mathrm{Aut}_{\mathcal{O}}(I_i)$ of each I_i as a right $\mathcal{O}$-module is $\mathcal{O}_i^\times$, where $\mathcal{O}_i = \mathcal{O}_l(I_i)$. For an order $\mathcal{O}$ with a large number of ideal classes, it is generally expected that $w_i = [\mathcal{O}_i^\times : A^\times] = 1$ for most $1 \le i \le h$. Equivalently, we expect $\mathrm{Mass}(\mathcal{O}) = \sum_{i=1}^h 1/w_i$ to be the dominant term in the class number formula $h(\mathcal{O}) = \mathrm{Mass}(\mathcal{O}) + \mathrm{Ell}(\mathcal{O})$. This is indeed the case for the orders $\mathbb{O}_r \subset D_{\infty_1,\infty_2}$ with $r = 1, 8, 16$.

THEOREM 6.3.1. *Assume that that $p \equiv 1 \pmod 4$ if $r = 8, 16$. For all $r \in \{1, 8, 16\}$, we have* $\lim_{p\to\infty} \mathrm{Mass}(\mathbb{O}_r)/h(\mathbb{O}_r) = 1$.

Proof. It is enough to prove that $\lim_{p\to\infty} \mathrm{Ell}(\mathbb{O}_r)/\mathrm{Mass}(\mathbb{O}_r) = 0$ for each r. Recall that $\mathrm{Mass}(\mathbb{O}_r) = c_r \zeta_F(-1) h(F)$, and $\mathrm{Ell}(\mathbb{O}_r) = \sum_{j=1}^3 d_{r,j}\, h(K_j)$ for some constants $c_r > 0$ and $d_{r,j}$ in each case. It reduces to prove that $\lim_{p\to\infty} h(K_j)/(\zeta_F(-1)h(F)) = 0$ for each $j \in \{1,2,3\}$. Let $\mathfrak{d}(-pj)$ be the discriminant of $\mathbb{Q}(\sqrt{-pj}\,)$. It follows from the work of Herglotz [11] that $h(K_j) \le h(F)h(-pj)$ for $p \ge 5$ (see also Remark 6.2.11). We have $\lim_{p\to\infty}(\log h(-pj))/(\log\sqrt{|\mathfrak{d}(-pj)|}\,) = 1$ by [15, Theorem 15.4, Chapter 12]. (See also [14, Lemma 4] for a similar result on the asymptotic behavior of relative class numbers of arbitrary CM-fields.) On the other hand, $\zeta_F(-1) > (p-1)/240$ by (6.12). Hence

$$0 \le \lim_{p\to\infty} \frac{h(K_j)}{h(F)\zeta_F(-1)} \le \lim_{p\to\infty} \frac{h(-pj)}{\zeta_F(-1)} = 0,$$

which shows that $\lim_{p\to\infty} h(K_j)/(h(F)\zeta_F(-1)) = 0$ for all $j \in \{1,2,3\}$. ∎

7. Tables. In this section, we list the class numbers $h(\mathbb{O}_r)$ and related data for $r = 1, 8, 16$ (separated into 3 tables) and all primes $5 < p < 200$. Here $F = \mathbb{Q}(\sqrt{p}\,)$, and $K_j = \mathbb{Q}(\sqrt{p}, \sqrt{-j}\,)$ for $j = 1, 2, 3$. Recall that $\mathbb{O}_8$ and $\mathbb{O}_{16}$ are defined only for the primes $p \equiv 1 \pmod 4$. Moreover, for these p the values of $h(K_2)$ are not needed in the calculation and are left blank. By [4, footnote to table 3, p. 424], out of the 303 primes $p < 2000$, $h(\mathbb{Q}(\sqrt{p}\,)) = 1$ for 264 of them. So it is not surprising that most $h(F) = 1$ in Table 1.

Table 1: Class numbers of $\mathbb{O}_1$ for all primes $7 \le p < 200$.

p	$h(\mathbb{O}_1)$	$\mathrm{Mass}(\mathbb{O}_1)$	$\mathrm{Ell}(\mathbb{O}_1)$	$\zeta_F(-1)$	$h(F)$	$h(K_1)$	$h(K_2)$	$h(K_3)$
7	3	1/3	8/3	2/3	1	1	4	2
11	4	7/12	41/12	7/6	1	1	2	2

Continued on next page

Table 1: Class numbers of $\mathbb{O}_1$ for all primes $7 \le p < 200$.

p	$h(\mathbb{O}_1)$	$\mathrm{Mass}(\mathbb{O}_1)$	$\mathrm{Ell}(\mathbb{O}_1)$	$\zeta_F(-1)$	$h(F)$	$h(K_1)$	$h(K_2)$	$h(K_3)$
13	1	1/12	11/12	1/6	1	1		2
17	1	1/6	5/6	1/3	1	2		1
19	6	19/12	53/12	19/6	1	1	6	2
23	7	5/3	16/3	10/3	1	3	4	4
29	2	1/4	7/4	1/2	1	3		3
31	9	10/3	17/3	20/3	1	3	8	2
37	2	5/12	19/12	5/6	1	1		4
41	2	2/3	4/3	4/3	1	4		1
43	12	21/4	27/4	21/2	1	1	10	6
47	13	14/3	25/3	28/3	1	5	8	4
53	3	7/12	29/12	7/6	1	3		5
59	16	85/12	107/12	85/6	1	3	6	2
61	3	11/12	25/12	11/6	1	3		4
67	18	41/4	31/4	41/2	1	1	14	6
71	19	29/3	28/3	58/3	1	7	4	4
73	3	11/6	7/6	11/3	1	2		2
79	69	42	27	28	3	15	24	18
83	22	43/4	45/4	43/2	1	3	10	6
89	4	13/6	11/6	13/3	1	6		1
97	4	17/6	7/6	17/3	1	2		2
101	5	19/12	41/12	19/6	1	7		5
103	31	19	12	38	1	5	20	6
107	28	197/12	139/12	197/6	1	3	6	10
109	5	9/4	11/4	9/2	1	3		6
113	5	3	2	6	1	4		3
127	39	80/3	37/3	160/3	1	5	16	10
131	38	93/4	59/4	93/2	1	5	6	6
137	6	4	2	8	1	4		3
139	44	127/4	49/4	127/2	1	3	14	6
149	7	35/12	49/12	35/6	1	7		7
151	49	37	12	74	1	7	12	6
157	7	43/12	41/12	43/6	1	3		8
163	50	467/12	133/12	467/6	1	1	22	10
167	47	91/3	50/3	182/3	1	11	12	8
173	8	13/4	19/4	13/2	1	7		9
179	54	157/4	59/4	157/2	1	5	6	6
181	8	19/4	13/4	19/2	1	5		6
191	61	130/3	53/3	260/3	1	13	8	8
193	10	49/6	11/6	49/3	1	2		4
197	9	49/12	59/12	49/6	1	5		11
199	71	55	16	110	1	9	20	6

Acknowledgements. The project grew from J. Xue and CF Yu's participation in the Shimura curves seminar organized by Yifan Yang at the the National Center for Theoretical Science (NCTS). They also wish to thank NCTS for provid-

TABLE 2
Class numbers of $\mathbb{O}_8$ for all primes $5 < p < 200$ and $p \equiv 1 \pmod 4$.

p	$h(\mathbb{O}_8)$	Mass($\mathbb{O}_8$)	Ell($\mathbb{O}_8$)	p	$h(\mathbb{O}_8)$	Mass($\mathbb{O}_8$)	Ell($\mathbb{O}_8$)
13	2	5/12	19/12	101	29	95/4	21/4
17	2	3/2	1/2	109	16	45/4	19/4
29	4	5/4	11/4	113	28	27	1
37	7	25/4	3/4	137	37	36	1
41	7	6	1	149	21	175/12	77/12
53	7	35/12	49/12	157	24	215/12	73/12
61	8	55/12	41/12	173	24	65/4	31/4
73	17	33/2	1/2	181	29	95/4	21/4
89	21	39/2	3/2	193	74	147/2	1/2
97	26	51/2	1/2	197	65	245/4	15/4

TABLE 3
Class numbers of $\mathbb{O}_{16}$ for all primes $5 < p < 200$ and $p \equiv 1 \pmod 4$.

p	$h(\mathbb{O}_{16})$	Mass($\mathbb{O}_{16}$)	Ell($\mathbb{O}_{16}$)	p	$h(\mathbb{O}_{16})$	Mass($\mathbb{O}_{16}$)	Ell($\mathbb{O}_{16}$)
13	2	5/6	7/6	101	63	95/2	31/2
17	3	1	2	109	26	45/2	7/2
29	5	5/2	5/2	113	23	18	5
37	18	25/2	11/2	137	29	24	5
41	7	4	3	149	35	175/6	35/6
53	9	35/6	19/6	157	40	215/6	25/6
61	12	55/6	17/6	173	39	65/2	13/2
73	14	11	3	181	52	95/2	9/2
89	17	13	4	193	54	49	5
97	20	17	3	197	141	245/2	37/2

ing Magma software that they use to compute the class numbers. Discussions with Markus Kirschmer, Meinhard Peters, Paul Ponomarev, John Voight, and Yifan Yang are very helpful and greatly appreciated. J. Xue is partially supported by Natural Science Foundation of China grant #11601395, and the grant NSC 102-2811-M-001-090. TC Yang and CF Yu are partially supported by the grants NSC 100-2628-M-001-006-MY4 and AS-98-CDA-M01.

REFERENCES

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] H. Bass, *Torsion free and projective modules*, Trans. Amer. Math. Soc., 102 (1962), pp. 319–327.

[3] Z. I. Borevič and D. K. Faddeev, *Representations of orders with cyclic index*, Trudy Mat. Inst. Steklov, 80 (1965), pp. 51–65.

[4] A. I. Borevich and I. R. Shafarevich, *Number theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24(3-4) (1997), pp. 235–265. Computational algebra and number theory (London, 1993).

[6] J. Brzezinski, *A generalization of Eichler's trace formula*, Collect. Math., 48(1-2) (1997), pp. 53–61. Journées Arithmétiques (Barcelona, 1995).

[7] W. K. Chan and M. Peters, *Quaternary quadratic forms and Hilbert modular surfaces*, in "Algebraic and arithmetic theory of quadratic forms", volume 344 of Contemp. Math., pp. 85–97. Amer. Math. Soc., Providence, RI, 2004.

[8] P. E. Conner and J. Hurrelbrink, *Class number parity*, volume 8 of *Series in Pure Mathematics*, World Scientific Publishing Co., Singapore, 1988.

[9] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library. John Wiley & Sons, Inc., New York, 1990. With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.

[10] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math., 195 (1955), pp. 127–151.

[11] G. Herglotz, *Über einen Dirichletschen Satz*, Math. Z., 12:1 (1922), pp. 255–261.

[12] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan, 26 (1974), pp. 56–82.

[13] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan, 20 (1968), pp. 83–95.

[14] K. Horie and M. Horie, *CM-fields and exponents of their ideal class groups*, Acta Arith., 55:2 (1990), pp. 157–170.

[15] L. K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982. Translated from the Chinese by Peter Shiu.

[16] M. Kirschmer and J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput., 39:5 (2010), pp. 1714–1747.

[17] Y. Kitaoka, *Quaternary even positive definite quadratic forms of prime discriminant*, Nagoya Math. J., 52 (1973), pp. 147–161.

[18] O. Körner, *Traces of Eichler-Brandt matrices and type numbers of quaternion orders*, Proc. Indian Acad. Sci. Math. Sci., 97(1-3) (1988), pp. 189–199.

[19] Q. Li, J. Xue, and C.-F. Yu, *Unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields*, `http://arxiv.org/abs/1807.04736v2`, 54 pp., to appear in Trans. Amer. Math. Soc.

[20] J. Neukirch, *Algebraic number theory*, volume 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[21] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionenalgebren*, Acta Arith., 15 (1968/1969), pp. 329–365.

[22] P. Ponomarev, *Arithmetic of quaternary quadratic forms*, Acta Arith., 29:1 (1976), pp.1–48.

[23] P. Ponomarev, *Class number formulas for quaternary quadratic forms*, Acta Arith., 39:1 (1981), pp. 95–104.

[24] I. Reiner, *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*, The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[25] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, in "Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, volume 175 of Lecture Notes in Math., pages Exp. No. 352, 95–110. Springer, Berlin, 1971.

[26] M.-F. Vignéras, *Nombre de classes d'un ordre d'Eichler et valeur au point* -1 *de la fonction zêta d'un corps quadratique réel*, Enseignement Math. (2), 21:1 (1975), pp. 69–105.

[27] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, volume 800 of Lecture Notes in Mathematics, Springer, Berlin, 1980.

[28] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4), 2 (1969), pp. 521–560.

[29] F.-T. Wei and C.-F. Yu, *Class numbers of central simple algebras over global function fields*, Int. Math. Res. Not. IMRN, 11 (2015), pp. 3525–3575.

[30] J. Xue and C.-F. Yu, *On superspecial abelian surfaces and type numbers of totally definite quaternion algebras*, ArXiv e-prints, September 2018, `https://arxiv.org/abs/1809.04316`, `arXiv:1809.04316`, to appear in the Indiana Univ. Math. J.

[31] J. Xue and C.-F. Yu, *On counting certain abelian varieties over finite fields*, `http://arxiv.org/abs/1801.00229v2`, 25 pp., to appear in Acta Math. Sin. (Engl. Ser.).

[32] J. Xue, T.-Ch. Yang, and C.-F. Yu, *Numerical invariants of totally imaginary quadratic* $\mathbb{Z}[\sqrt{p}]$*-orders*, Taiwanese J. Math., 20:4 (2016), pp. 723–741.

[33] J. Xue, T.-Ch. Yang, and C.-F. Yu, *On superspecial abelian surfaces over finite fields*, Doc. Math., 21 (2016), pp. 1607–1643.

[34] J. Xue, T.-Ch. Yang, and C.-F. Yu, *On superspecial abelian surfaces over finite fields II*, `http://arxiv.org/abs/1801.09374v2`, 26 pp., to appear in J. Math. Soc. Japan.

[35] C.-F. Yu, *Simple mass formulas on Shimura varieties of PEL-type*, Forum Math., 22:3 (2010), pp. 565–582.
[36] C.-F. Yu, *Superspecial abelian varieties over finite prime fields*, J. Pure Appl. Algebra, 216:6 (2012), pp. 1418–1427.
[37] D. Zagier, *On the values at negative integers of the zeta-function of a real quadratic field*, Enseignement Math. (2), 22(1-2) (1976), pp. 55–95.