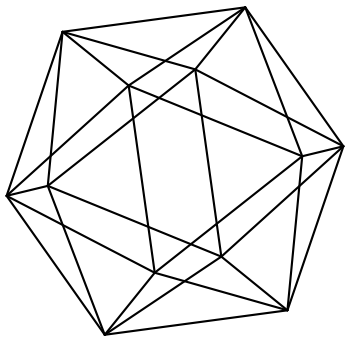
Max-Planck-Institut für Mathematik
Bonn

Supersingular abelian surfaces and Eichler class number formula

by

Jiangwei Xue
Tse-Chung Yang
Chia-Fu Yu



Max-Planck-Institut für Mathematik
Preprint Series 2015 (1)

Supersingular abelian surfaces and Eichler class number formula

Jiangwei Xue
Tse-Chung Yang
Chia-Fu Yu

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Collaborative Innovation Centre
of Mathematics
School of Mathematics and Statistics
Wuhan University
Luojiashan, Wuhan
Hubei 430072
P. R. China

Institute of Mathematics
Academia Sinica
and
NCTS (Taipei Office)
Astronomy-Mathematics Building
No. 1, Sec. 4, Roosevelt Rd.
Taipei 10617
Taiwan

MPIM 15-1

SUPERSINGULAR ABELIAN SURFACES AND EICHLER CLASS NUMBER FORMULA

JIANGWEI XUE,TSE-CHUNG YANG AND CHIA-FU YU

Abstract. Let F be a totally real field with ring of integers O_F, and D be a totally definite quaternion algebra over F. A well-known formula established by Eichler and then extended by Körner computes the class number of any O_F-order in D. In this paper we generalize the Eichler class number formula so that it works for arbitrary $\mathbb{Z}$-orders in D. Our motivation is to count the isomorphism classes of supersingular abelian surfaces in a simple isogeny class over a finite prime field $\mathbb{F}_p$. We give explicit formulas for the number of these isomorphism classes for all primes p.

Contents

Date: January 12, 2015.
2010 *Mathematics Subject Classification.* 11R52, 11G10.
Key words and phrases. supersingular abelian surfaces, class number formula, Brandt matrices, trace formula.

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 the 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 *q-Weil number* if $|\pi| = \sqrt{q}$ for all embeddings of $\mathbb{Q}(\pi)$ into $\mathbb{C}$. The Honda-Tate theory [12, 28] establishes a bijection between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes q-Weil numbers. In [31], Waterhouse developed a theory for studying the isomorphism classes and endomorphism rings of abelian varieties within a fixed simple isogeny class. If π is a q-Weil 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 $\mathbb{F}_{p^2}$ which lies inside the isogeny class $\mathrm{Isog}(X_\pi)$ corresponding to the p^2-Weil 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 [31, 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 containing R_0, where $h(R) := |\mathrm{Pic}(R)|$ denotes the class number of the order R. It is known that the class number $h(R)$ of 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 p-Weil 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 [28, 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 [31, Theorem 6.2] showed 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 p-Weil 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

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

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 by Section 9.2.
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 (6.11).

To obtain Theorem 1.2, it is necessary to compute the class number of D_{∞_1,∞_2}.

Theorem 1.3. *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 $h(D) = H(p)$ and is given by (1.2).

Remark 1.4. By Section 7.10, for all $p \geq 5$ and $j \in \{1, 2, 3\}$, we have $h(K_j) = \nu h(F)h(\Bbbk_j)$, where $\nu \in \{1, 1/2\}$ and $\Bbbk_j := \mathbb{Q}(\sqrt{-pj})$. Hence one may factor out $h(F)$ in the results of Theorem 1.2 and 1.3. For example, we get

$$\frac{h(D)}{h(F)} = \frac{\zeta_F(-1)}{2} + \frac{h(\Bbbk_1)}{8} + \frac{h(\Bbbk_3)}{6} \tag{1.4}$$

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

$$\frac{h(D)}{h(F)} = \frac{\zeta_F(-1)}{2} + \left(\frac{3}{8} + \frac{5}{8}\left(2 - \left(\frac{2}{p}\right)\right)\right)h(\Bbbk_1) + \frac{h(\Bbbk_2)}{4} + \frac{h(\Bbbk_3)}{6} \tag{1.5}$$

for $p > 5$ and $p \equiv 3 \pmod 4$. M. Peters pointed out that the formulas in the right hand sides of (1.4) and (1.5) coincide with formulas for the proper class number $H^+(\mathfrak{d}_F)$ of even definite quaternary quadratic forms of discriminant $\mathfrak{d}_F$ (see [6, p. 85 and p. 95]), where $\mathfrak{d}_F$ is the discriminant of $F = \mathbb{Q}(\sqrt{p})$. That is, we have

$$h(D) = h(F)\, H^+(\mathfrak{d}_F) \quad \text{for all primes } p > 5. \tag{1.6}$$

Particularly, the number $h(D)/h(F)$ is always an integer. The above formula for $H^+(\mathfrak{d}_F)$ is obtained by Kitaoka [16] for primes $p \equiv 1 \pmod 4$ and by Ponomarev [24, 25] for all primes p. Inspired by Peters' comment, we chased the literature and discovered that formula (2) of Theorem 1.3 was obtained in [23].

The calculations for both Theorem 1.2 and 1.3 will be carried out in Section 6.2. The main idea of the proof of Theorem 1.2 is to apply Eichler's class number formula ([9], cf. [29, Chapter V, Corollary 2.5, p. 144]) for totally definite quaternion algebras. Eichler proved the class number formula for Eichler O_F-orders. Based on Eichler's methods, Körner [17] worked out a similar class number formula for any O_F-order. However, the class number formula established in [17] is not readily applicable in our case as the orders arising from the endomorphism rings of supersingular abelian surfaces studied above do not necessarily contain the ring of integers $O_F \subset F$. The first half 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 1.5 (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*

$$h(\mathcal{O}) = \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{w(B)>1} (2 - \delta(B)) h(B) (1 - w(B)^{-1}) \prod_p m_p(B), \tag{1.7}$$

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 causes some confusion as there are possibly more than one choice for defining Brandt matrices and other terms as well at a few places. Thus one needs to examine all details in the original proof in [9] (also [29, Chapter V, Corollary 2.5, p. 144]) until the final formula goes through. Our definition of Brandt matrices is justified by representation theory (Section 4). We remark that the methods of results 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 normalizer 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 second main part (Sections 6–9) of this paper is then devoted to proving the explicit formulas given in Theorems 1.2 and 1.3. In Sections 7–9, we classify

A-orders B in Theorem 1.5 and compute the invariant $w(B)$ and the class number $h(B)$ for each B. These sections are self-contained and can be read independently. The results obtained there will be used in Section 6 for the proof of Theorems 1.2 and 1.3. Based on our explicit formulas, we used Magma to evaluate the numbers $H(p)$ for $p < 10000$ and make the tables for values of related terms for $p < 200$.

We build the formula (1.7) a priori in order to compute the sum of class numbers $H(p)$. A posteriori computing these class numbers becomes helpful for us to understand and examine our formula. There are interesting and concrete proper A-orders B found in the elliptic term due to thse examples. It is also an interesting problem of computing local optimal embeddings of these orders.

In a sequel paper we study the endomorphism rings of abelian varieties X in the isogeny class $\mathrm{Isog}(X_\pi)$. Through analyzing the action of the Picard group $\mathrm{Pic}(O_F)$ on the principal genus in $\mathrm{Isog}(X_\pi)$ (those with maximal endomorphism rings), we obtain a direct proof of the equality (1.6) without computation. Combining the formula for $h(D)$ in this paper, we give a different proof of the results of Kitaoka and Ponomarev as stated in Remark 1.4.

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

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

If Y is also an O_F-module, then Y_p further 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 $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is the ring of finite adeles of $\mathbb{Q}$. We also have that $\widehat{F} = F \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = F \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}} = \prod'_{v:\,\text{finite}} F_v$ 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.

If S is a finite set, 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 all maximal ideals $\mathfrak{m}$ 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 all primes 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 all $\mathfrak{m}|p$. 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 (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 exist $g \in D^\times$ 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 will enable us to define Brandt matrices for arbitrary proper A-orders $\mathcal{O}$ 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. [26, p. 183], [29, p. 22]). We give an example which 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 notations 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. 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. The proposition follows directly from Lemma 2.7 below. □

Lemma 2.7. *Let $R \subseteq S$ be an inclusion of commutative rings with S integral over R. Then $R^\times = S^\times \cap R$.*

Proof. Clearly, $R^\times \subseteq S^\times \cap R$. On the other hand,

$$R^\times = R - \bigcup \mathfrak{m},$$

where the union is over all the maximal ideals $\mathfrak{m} \subset R$. Given an element $u \in S^\times \cap R$, to show that $u \in R^\times$, it is enough to show that $u \notin \mathfrak{m}$ for any maximal ideal $\mathfrak{m} \subset R$. Since S is integral over R, by the going-up theorem [1, Theorem 5.10], any maximal ideal of R can be obtained by intersecting a maximal ideal of S with R. □

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 1.5. We follow closely Eichler's original proof [9]; also see Vignéras's book [29].

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 only depends 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 each $\mathcal{O}_i$ is also closed under the canonical involution. 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 all $x \in \mathcal{O}$. 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 $1 \leq i, j \leq h = h(\mathcal{O})$, 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 the proposition above are finite. This is already known if $A = O_F$ in Körner [17]. 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 $c \in \mathbb{N}_{>0}$, 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 above finite sets. 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 quadratic CM extension of F which can be embedded into D over F. Let B be an A-order in K. Denote by $\mathrm{Emb}(B, \mathcal{O})$ the set of optimal embeddings from B into $\mathcal{O}$. In other words,

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

Equivalently, those are the embeddings of A-orders $\varphi : B \hookrightarrow \mathcal{O}$ so 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 the discrete subset $\mathcal{O}$ and a compact set in $\mathcal{O} \otimes \mathbb{R}$, 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 $|O(\varphi)| = [\mathcal{O}^\times : B^\times] = w(\mathcal{O})/w(B)$, which is independent of φ. This gives (3.4). As a result, one obtains

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

As $\mathcal{O}_p$ and $\mathcal{O}_{i,p}$ are isomorphic, 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 any $i = 1,\dots,h$. 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 [29, Theorem 5.11, p. 92] (also see [32], Lemma 3.2 and below). We provide this proof for the reader's convenience.

Proof. We fix an embedding $\varphi_0 : K \to D$ and let $K_0 := \varphi_0(K)$ and $B_0 := \varphi_0(B)$. Any embedding $f : K \to D$ is of the form $a \mapsto g^{-1}\varphi_0(a)g$ for some $g \in D^\times$. This gives an identification

$$\mathrm{Emb}(B,\mathcal{O}_i)/\mathcal{O}_i^\times \simeq K_0^\times\backslash\mathcal{E}(B,\mathcal{O}_i)/\mathcal{O}_i^\times,$$

where

$$\mathcal{E}(B,\mathcal{O}_i) := \{g \in D^\times \mid g^{-1}K_0 g \cap \mathcal{O}_i = g^{-1}B_0 g\},$$

equipped with the action of $K_0^\times$ (respectively, $\mathcal{O}_i^\times$) by multiplication from the left (respectively, right).

Set

$$\widehat{\mathcal{E}}(B,\mathcal{O}) := \{g \in \widehat{D}^\times \mid K_0 \cap g\widehat{\mathcal{O}}g^{-1} = B_0\}.$$

Let $g_1,...,g_h$ be representatives in $\widehat{D}^\times$ of double cosets in $D^\times\backslash\widehat{D}^\times/\widehat{\mathcal{O}}^\times$. We define a map

$$\begin{array}{rccc} \Phi: & \coprod_{i=1}^{h} K_0^\times\backslash\mathcal{E}(B,\mathcal{O}_i)/\mathcal{O}_i^\times & \longrightarrow & K_0^\times\backslash\widehat{\mathcal{E}}(B,\mathcal{O})/\widehat{\mathcal{O}}^\times \\ & K_0^\times g\mathcal{O}_i^\times & \longmapsto & K_0^\times g g_i\widehat{\mathcal{O}}^\times, \end{array}$$

Note that Φ is well-defined since $\widehat{\mathcal{O}}_i = g_i\widehat{\mathcal{O}}g_i^{-1}$. Now, for each $\hat{g} \in \widehat{\mathcal{E}}(B,\mathcal{O})$, there exist an element $b \in D^\times$, an integer i with $1 \le i \le h$, and an element $\hat{\gamma} \in \widehat{\mathcal{O}}^\times$ such that

$$\hat{g} = b \cdot g_i \cdot \hat{\gamma}.$$

Then b must be in $\mathcal{E}(B,\mathcal{O}_i)$, and the map

$$K_0^\times \hat{g}\widehat{\mathcal{O}}^\times \longmapsto K_0^\times b\mathcal{O}_i^\times \in K_0^\times\backslash\mathcal{E}(B,\mathcal{O}_i)/\mathcal{O}_i^\times$$

gives the inverse map of Φ. This shows

$$\coprod_i \mathrm{Emb}(B,\mathcal{O}_i)/\mathcal{O}_i^\times \simeq K_0^\times\backslash\widehat{\mathcal{E}}(B,\mathcal{O})/\widehat{\mathcal{O}}^\times.$$

Consider the natural surjective map

$$\Psi : K_0^\times\backslash\widehat{\mathcal{E}}(B,\mathcal{O})/\widehat{\mathcal{O}}^\times \twoheadrightarrow \widehat{K}_0^\times\backslash\widehat{\mathcal{E}}(B,\mathcal{O})/\widehat{\mathcal{O}}^\times.$$

The base space $\widehat{K}_0^\times\backslash\widehat{\mathcal{E}}(B,\mathcal{O})/\widehat{\mathcal{O}}^\times$ can be decomposed locally:

$$\widehat{K}_0^\times\backslash\widehat{\mathcal{E}}(B,\mathcal{O})/\widehat{\mathcal{O}}^\times = \prod_p (K_0)_p^\times\backslash\mathcal{E}_p(B_p,\mathcal{O}_p)/\mathcal{O}_p^\times, \tag{3.8}$$

where

$$\mathcal{E}_p(B_p,\mathcal{O}_p) := \{g \in D_p^\times \mid (K_0)_p \cap g\mathcal{O}_p g^{-1} = (B_0)_p\}. \tag{3.9}$$

The fiber of a double coset $\widehat{K}_0^\times g\widehat{\mathcal{O}}^\times$ under the map Ψ is in bijection with the double coset space

$$K_0^\times\backslash\widehat{K}_0^\times/\big(\widehat{K}_0^\times \cap g\widehat{\mathcal{O}}^\times g^{-1}\big) = K_0^\times\backslash\widehat{K}_0^\times/\widehat{B}_0^\times. \tag{3.10}$$

The assertion (3.7) then follows from (3.8) and (3.10). □

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 in $\widetilde{A}^\times$. We define two sets:

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

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

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

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

$$\mathfrak{B}_{ii}(\mathfrak{n}) = |\mathscr{C}_i|/2w_i. \tag{3.11}$$

We define the symbol

$$\delta_{\mathfrak{n}} = \begin{cases} 1 & \text{if } \mathfrak{n} = \widetilde{A}a^2 \text{ for some } a \in A; \\ 0 & \text{otherwise.} \end{cases} \tag{3.12}$$

Note that the center of $\mathcal{O}$ or $\mathcal{O}_i$ is equal to A. It follows that

$$2\delta_{\mathfrak{n}} = |\mathscr{C}_i \cap A|. \tag{3.13}$$

Let $\mathcal{P}_{\mathcal{O},\mathfrak{n}}$ be the set of characteristic polynomials of non-central elements $b \in \mathscr{C}_i$ for some i. This is a finite set in $\widetilde{A}[X]$ as 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 is independent of $\mathcal{O}$ but depends on $\mathfrak{n}$. Let $\mathcal{P}_{D,\mathfrak{n}} \subset \widetilde{A}[X]$ be the set consisting of all irreducible polynomials of the form $X^2 - tX + \varepsilon\beta$ for some $\varepsilon \in S$ such that $t^2 - 4\varepsilon\beta \notin F_v^2$ for all the ramified places v of F for D, including all the archimedean ones. The set $\mathcal{P}_{D,\mathfrak{n}}$ is again finite as the elements t are bounded for all the archimedean norms. 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, and thus 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 $A = \mathbb{Z}[\sqrt{p}]$ with $A^\times \neq O_F^\times$. 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 (Section 9.8). 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 embedding of K_P into D as F-algebras. 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 $1 \leq i \leq h$:

$$\coprod_{P \in \mathcal{P}_{\mathcal{O},\mathfrak{n}}} \coprod_{B_P \subseteq B \subset K_P} \mathrm{Emb}(B, \mathcal{O}_i) = \coprod_{P \in \mathcal{P}_{D,\mathfrak{n}}} \coprod_{B_P \subseteq B \subset K_P} \mathrm{Emb}(B, \mathcal{O}_i), \tag{3.14}$$

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*

$$\mathscr{C}_i - A \simeq \coprod_{P \in \mathcal{P}_{D,\mathfrak{n}}} \coprod_{B_P \subseteq B \subset K_P} \mathrm{Emb}(B, \mathcal{O}_i). \tag{3.15}$$

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. □

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 when 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*

$$\mathrm{Tr}\, \mathfrak{B}(\mathfrak{n}) = \delta_{\mathfrak{n}} \cdot \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{P \in \mathcal{P}_{D,\mathfrak{n}}} \sum_{B_P \subseteq B \subset K_P} M(B), \tag{3.16}$$

where $\delta_{\mathfrak{n}}$ *is defined by (3.12), and*

$$M(B) := \frac{h(B)}{w(B)} \prod_p m_p(B). \tag{3.17}$$

Proof. We have

$$\begin{aligned}\mathfrak{B}_{ii}(\mathfrak{n}) = \frac{|\mathscr{C}_i|}{2w_i} &= \frac{|\mathscr{C}_i - A|}{2w_i} + \frac{2\delta_{\mathfrak{n}}}{2w_i} \\ &= \frac{\delta_{\mathfrak{n}}}{w_i} + \frac{1}{2}\sum_{P\in\mathcal{P}_{D,\mathfrak{n}}}\sum_{B_P\subseteq B\subset K_P}\frac{|\mathrm{Emb}(B,\mathcal{O}_i)|}{w_i} \quad (\text{Lemma 3.3.1}) \\ &= \frac{\delta_{\mathfrak{n}}}{w_i} + \frac{1}{2}\sum_{P\in\mathcal{P}_{D,\mathfrak{n}}}\sum_{B_P\subseteq B\subset K_P}\frac{m(B,\mathcal{O}_i,\mathcal{O}_i^\times)}{w(B)} \quad (\text{by (3.5)}).\end{aligned} \tag{3.18}$$

Summing over $i = 1, \dots, h$ and by Lemma 3.2.1, one obtains (3.16) for the trace of the Brandt matrix $\mathfrak{B}(\mathfrak{n})$. □

3.3.4. We would like to count the right hand side of (3.15) 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,

$$B_P \subseteq \alpha_1^{-1}(B_1) = \alpha_1^{-1}\varphi_1^{-1}(\mathcal{O}_i) = \alpha_2^{-1}\varphi_2^{-1}(\mathcal{O}_i) = \alpha_2^{-1}(B_2) \subset K_P. \tag{3.19}$$

So 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. Suppose that $\alpha_2 = \iota \circ \alpha_1$, 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 (3.19) that $\iota(B) = B$. On the other hand, 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 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

$$T_{B,\mathfrak{n}} := \{x \in B - A \mid N_{K/F}(x) = \varepsilon\beta \ \text{ for some } \varepsilon \in S\}, \tag{3.20}$$

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

$$\mathscr{C}_{B,i} := \{(P, \varphi, \alpha) \mid P \in \mathcal{P}_B, \varphi \in \mathrm{Emb}(B, \mathcal{O}_i), \alpha \in \mathrm{Hom}_A(B_P, B)\}. \tag{3.21}$$

Note that if $P \in \mathcal{P}_B$ but $P \notin \mathcal{P}_{\mathcal{O},\mathfrak{n}}$, then $\mathrm{Emb}(B, \mathcal{O}_i) = \emptyset$ 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

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

The set $\mathscr{E}_{B,P,i}$ is equipped with an action of $\mathrm{Gal}(K/F)$ 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 $\mathrm{Gal}(K/F)$ act on $\mathscr{C}_{B,i}$ fiber-wisely. We have

$$\mathscr{C}_i - A \simeq \coprod_B \mathscr{C}_{B,i}/\operatorname{Gal}(K/F), \tag{3.22}$$

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

$$\mathrm{Emb}(B, \mathcal{O}_i) \simeq \mathscr{E}_{B,P,i}/\operatorname{Gal}(K/F), \qquad \varphi \mapsto (\varphi, \alpha). \tag{3.23}$$

Therefore,

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

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

$$|\mathscr{C}_{B,i}/\operatorname{Gal}(K/F)| = \frac{1}{2}|T_B| \cdot |\mathrm{Emb}(B, \mathcal{O}_i)|. \tag{3.24}$$

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

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

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

$$|\mathscr{C}_{B,i}/\operatorname{Gal}(K/F)| = |T_B| \cdot |\mathrm{Emb}(B, \mathcal{O}_i)|. \tag{3.25}$$

Let $\delta(B)$ be the symbol

$$\delta(B) := \begin{cases} 1 & \text{if } \iota(B) = B; \\ 0 & \text{otherwise.} \end{cases} \tag{3.26}$$

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 (3.20). The trace formula for $\mathfrak{B}(\mathfrak{n})$ is given by*

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

Here in the last summation B runs through all (non-isomorphic) quadratic proper A-orders which can be embedded 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 (3.22), (3.24) and (3.25). □

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 $\mathrm{Emb}(B, \mathcal{O}_i)$ is empty for all $1 \le i \le h$ 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 $\mathrm{Tr}\,\mathfrak{B}(\widetilde{A}) = h(\mathcal{O})$.

Corollary 3.3.8 (Class number formula)**.**

$$\begin{aligned} h(\mathcal{O}) &= \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{P \in \mathcal{P}_{D,(1)}} \sum_{B_P \subseteq B \subset K_P} M(B) \\ &= \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{w(B)>1} (2 - \delta(B)) h(B) (1 - w(B)^{-1}) \prod_p m_p(B). \end{aligned} \tag{3.27}$$

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

$$h(\mathcal{O}) = \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_K \sum_{\substack{B \subset K, \\ w(B)>1}} h(B)(1 - w(B)^{-1}) \prod_p m_p(B), \tag{3.28}$$

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

Proof. The first part of (3.27) 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 (3.27) follows from Theorem 3.3.7. Formula (3.28) is just a more intuitive reformulation of (3.27). Indeed, if $B \neq \iota(B)$, then both B and $\iota(B)$ appears in the right hand side of (3.28), giving us $2h(B)(1 - w(B)^{-1}) \prod_p m_p(B)$ for the isomorphic class of B. □

We call the sum in (3.27) the *elliptic part* (of the class number formula) and denote it by $\mathrm{Ell}(\mathcal{O})$. In other words,

$$\mathrm{Ell}(\mathcal{O}) := \frac{1}{2} \sum_{w(B)>1} (2 - \delta(B)) h(B) (1 - w(B)^{-1}) \prod_p m_p(B). \tag{3.29}$$

3.4. **Local optimal embeddings.** 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-$\mathcal{D}$ ideal, one has the formula [29, p. 94] for all prime ideals $\mathfrak{p} \subset O_F$,

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

Thus, one gets

$$\prod_{\mathfrak{p}} m_{\mathfrak{p}}(B) = \prod_{\mathfrak{p}|\mathcal{D}} \left(1 - \left(\frac{B}{\mathfrak{p}}\right)\right) \prod_{\mathfrak{p}|\mathfrak{N}} \left(1 + \left(\frac{B}{\mathfrak{p}}\right)\right). \tag{3.30}$$

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-$\mathcal{D}$ level $\mathfrak{N}$, Hijikata [11, 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 $\mathcal{E}_p(B_p, \mathcal{O}_p)$ is defined in (3.9). 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 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 all primes p, where the definition of Bass orders for $\mathbb{Z}_p$-orders is given similarly. 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

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

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 action. Using the Cartan decomposition, one easily sees that $U\backslash U(\mathfrak{n})/U$ is a finite set. Let $g_1, \ldots, g_h$ 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 $I_1, \ldots, I_h$ 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 $\{\chi_1, \ldots, \chi_h\}$ 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 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 $j = 1, \ldots, h$. 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

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

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 $\chi_1, \ldots, \chi_h$ 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 normalizer 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 notations and assumptions of Section 3.1. In particular, $\{I_1, \ldots, I_h\}$ 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 [17, Equation (1). p. 190], 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 [29, Chapter V, Corollary 2.3] states that

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

where $\zeta_F(s)$ is the Dedekind zeta-function of F, $\mathcal{D} \subseteq O_F$ is the discriminant ideal of D over F and $\mathfrak{p}$ ranges in the set of prime ideals of O_F that divide $\mathcal{D}$. Using Lemma 5.1.2, one easily derives the relative mass formula

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

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 $\varpi := [O_F^\times : A^\times]$. It is shown in Section 9.2 that $\varpi \in \{1, 3\}$, 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 a inner automorphism of D. Let $\mathfrak{O}_r$ denote the genus consisting of orders in D which are locally isomorphic to $\mathbb{O}_r$ at every prime ℓ.

We will need the following result, which is a special case of [33, 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 [31, 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 [34, 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). □

Remark 6.1.3. Let X be a member in $\mathrm{Isog}(X_\pi)$ with $\mathrm{End}(X) \in \mathfrak{O}_8$. We claim that X does not admit any principal polarization. Suppose otherwise and $\lambda : X \xrightarrow{\simeq} X^\vee$ is a principal polarization, where $X^\vee$ denotes the dual abelian variety. Then λ induces a Rosati involution on $\mathrm{End}(X)$ (not just $\mathrm{End}^0(X)$) by sending $\phi \mapsto \phi' := \lambda^{-1} \circ \phi^\vee \circ \lambda$ for all $\phi \in \mathrm{End}(X)$. The Rosati involution is positive in the sense of [21, Section 21]. By Albert's classification (ibid.), the canonical involution is the unique positive involution for any totally definite quaternion algebra. On the other hand, the orders in $\mathfrak{O}_8$ are not closed under the canonical involution by (5.8). We obtain a contradiction, and hence the claim is verified.

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 $\mathbb{O}_{16}$ are necessary for 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 exclusively for the order $\mathbb{Z}[\sqrt{p}]$ when $p \equiv 1 \pmod 4$. By Section 9.2, $\varpi = [O_F^\times : A^\times] \in \{1, 3\}$, and $\varpi = 1$ if $p \equiv 1 \pmod 8$.

By the class number formula (3.28),

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

The mass part $\mathrm{Mass}(\mathbb{O}_r)$ has already been calculated in Section 5.2. So 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 through 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 (3.26), i.e. it is 1 if B is closed under the complex conjugation, and 0 otherwise.

The detailed classification of all the orders B will be given in the subsequent sections. We only summarize the results below. For this purpose some more notations need to be introduced.

6.2.1. Notations of fields and orders. Let $K_j = \mathbb{Q}(\sqrt{p}, \sqrt{-j})$ with $j \in \{1,2,3\}$[1]. It will be shown that

- for $p > 5$, all quadratic O_F-orders B with $[B^\times : O_F^\times] > 1$ lie in K_j for some $j \in \{1,2,3\}$ (Section 7.8);
- 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 (Lemma 9.4).

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.

6.2.2. 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 [29, p. 94] or Section 3.4). It follows that

$$\mathrm{Ell}(\mathbb{O}_1) = \frac{1}{2}\sum_{w(B)>1} h(B)(1-w(B)^{-1}), \tag{6.3}$$

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

By Section 7.8 and Proposition 8.1, if $p \equiv 1 \pmod 4$ and $p > 5$, then 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

$$h(\mathbb{O}_1) = \frac{1}{2}h(F)\zeta_F(-1) + h(K_1)/4 + h(K_3)/3, \quad \text{if } p \equiv 1 \pmod 4,\ p > 5. \tag{6.4}$$

[1]If we need the 2-adic completion of a number field K, we will have to write $K \otimes_{\mathbb{Q}} \mathbb{Q}_2$ instead of K_2 for the rest of the paper. This is needed only in Section 9.10, so no confusion should arise in general.

On the other hand, if $p \equiv 3 \pmod 4$ and $p \geq 7$, the following table gives a complete list of orders B with $w(B) > 1$ and their class numbers (See Section 7.8 and Section 8):

$p \equiv 3 \pmod 4$	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

$$h(\mathbb{O}_1) = \frac{1}{2}h(F)\zeta_F(-1) + \left(\frac{3}{8} + \frac{5}{8}\left(2-\left(\frac{2}{p}\right)\right)\right)h(K_1) + \frac{1}{4}h(K_2) + \frac{1}{3}h(K_3), \tag{6.5}$$

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

6.2.3. 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

$$\mathrm{Ell}(\mathbb{O}_r) = \frac{1}{2}\sum_{w(B)>1}(2-\delta(B))h(B)(1-w(B)^{-1})m(B_2, (\mathbb{O}_r)_2, (\mathbb{O}_r)_2^\times), \tag{6.6}$$

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 $r = 8, 16$. The following table gives a complete list of mutually non-isomorphic quadratic proper A-orders B with $w(B) > 1$. Here $B_{3,2}$ is a proper A-order only if $p \equiv 5 \pmod 8$ and $\varpi = 3$, in which case $\delta(B_{3,2}) = 0$. All the data in the table below will be calculated in Section 9.

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

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

$$h(\mathbb{O}_8) = \frac{9}{2}\zeta_F(-1)h(F) + \frac{1}{4}h(K_1), \tag{6.7}$$

$$h(\mathbb{O}_{16}) = 3\zeta_F(-1)h(F) + \frac{1}{2}h(K_1) + h(K_3). \tag{6.8}$$

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

$$h(\mathbb{O}_8) = \frac{15}{2\varpi}\zeta_F(-1)h(F) + \frac{3}{4\varpi}h(K_1) + \frac{2\delta_{3,\varpi}}{\varpi}h(K_3), \tag{6.9}$$

$$h(\mathbb{O}_{16}) = \frac{15}{\varpi}\zeta_F(-1)h(F) + \frac{3}{2\varpi}h(K_1) + \frac{1}{\varpi}h(K_3), \tag{6.10}$$

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

6.2.4. Special zeta-values. Let $\mathfrak{d}_F$ be the discriminant of $F = \mathbb{Q}(\sqrt{p})$. By Siegel's formula [35, Table 2, p. 70],

$$\zeta_F(-1) = \frac{1}{60} \sum_{\substack{b^2+4ac=\mathfrak{d}_F \\ a,c>0}} a, \tag{6.11}$$

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 [15]. We list the results here for the sake of completeness.

6.2.5. 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 (6.11) and $h(\mathbb{Q}(\sqrt{2}\,)) = 1$,

$$\begin{aligned} h(\mathbb{O}_1) &= \frac{1}{2} h(\mathbb{Q}(\sqrt{2}\,)) \zeta_{\mathbb{Q}(\sqrt{2}\,)}(-1) + \frac{1}{2}\left(\left(1-\frac{1}{4}\right) + \left(1-\frac{1}{2}\right) + \left(1-\frac{1}{3}\right)\right) \\ &= \frac{1}{24} + \frac{23}{24} = 1 \qquad \text{when } p = 2. \end{aligned} \tag{6.12}$$

6.2.6. 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 6.2.2, 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 (6.11) again, $\zeta_{\mathbb{Q}(\sqrt{3}\,)}(-1) = 1/6$. Since $h(\mathbb{Q}(\sqrt{3}\,)) = 1$,

$$h(\mathbb{O}_1) = \frac{1}{2} h(\mathbb{Q}(\sqrt{3}\,)) \zeta_{\mathbb{Q}(\sqrt{3}\,)}(-1) + \mathrm{Ell}(\mathbb{O}_1) = \frac{1}{12} + \frac{23}{12} = 2 \qquad \text{when } p = 3. \tag{6.13}$$

6.2.7. 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 (6.11) and $h(\mathbb{Q}(\sqrt{5})) = 1$,

$$\begin{aligned} h(\mathbb{O}_1) &= \frac{1}{2} h(\mathbb{Q}(\sqrt{5}))\zeta_{\mathbb{Q}(\sqrt{5})}(-1) + \frac{1}{2}\left(\left(1-\frac{1}{2}\right)+\left(1-\frac{1}{3}\right)+\left(1-\frac{1}{5}\right)\right) \\ &= \frac{1}{60}+\frac{59}{60} = 1 \qquad \text{when } p = 5. \end{aligned} \tag{6.14}$$

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 formulae 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 6.2.7. The fundamental unit $\epsilon = (1+\sqrt{5})/2 \notin \mathbb{Z}[\sqrt{5}]$, so $\varpi = 3$. By (6.9) and (6.10) 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 (6.4), (6.7) and (6.8), we get

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

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 (6.4), (6.9) and (6.10). □

6.3. **Asymptotic behaviors.** We keep the notations 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 $\mathbb{k}_j = \mathbb{Q}(\sqrt{-pj}\,)$, and $\mathfrak{d}_{\mathbb{k}_j}$ be its discriminant. By Section 7.10, $h(K_j) \le h(F)h(\mathbb{k}_j)$ for $p \ge 5$. We have $\lim_{p\to\infty}(\log h(\mathbb{k}_j))/(\log\sqrt{|\mathfrak{d}_{\mathbb{k}_j}|}\,) = 1$ by [14, Theorem 15.4, Chapter 12]. (See also [13, 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 (6.11). Hence

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

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

7. Totally imaginary quadratic extensions K/F

In this section, we classify all the totally imaginary quadratic extensions of $\mathbb{Q}(\sqrt{p}\,)$ that have strictly larger groups of units than $O^\times_{\mathbb{Q}(\sqrt{p}\,)}$. Throughout this section, F denotes a totally real number field with ring of integers O_F and group of units $O_F^\times$, and K always denotes a totally imaginary quadratic extension of F. We write $\boldsymbol{\mu}_K$ for the torsion subgroup of $O_K^\times$. It is a finite cyclic subgroup of $O_K^\times$ consisting of all the roots of unity in K. Clearly, $\boldsymbol{\mu}_F = \{\pm 1\}$. The quotient groups $O_F^\times/\boldsymbol{\mu}_F$ and $O_K^\times/\boldsymbol{\mu}_K$ are free abelian groups of rank $[F:\mathbb{Q}]-1$ by the Dirichlet's Unit Theorem (cf. [22, Theorem I.7.4]).

7.1. Since the free abelian groups $O_F^\times/\boldsymbol{\mu}_F$ and $O_K^\times/\boldsymbol{\mu}_K$ have the same rank, the natural embedding $O_F^\times/\boldsymbol{\mu}_F \hookrightarrow O_K^\times/\boldsymbol{\mu}_K$ realizes $O_F^\times/\boldsymbol{\mu}_F$ as a subgroup of $O_K^\times/\boldsymbol{\mu}_K$ of finite index

$$Q_{K/F} := [O_K^\times/\boldsymbol{\mu}_K : O_F^\times/\boldsymbol{\mu}_F] = [O_K^\times : \boldsymbol{\mu}_K O_F^\times]. \tag{7.1}$$

In particular, $O_F^\times$ has finite index in $O_K^\times$.

Suppose that $\boldsymbol{\mu}_K = \langle \zeta_{2n} \rangle$, where ζ_{2n} is a primitive $2n$-th root of unity. Let $\iota : x \mapsto \iota(x)$ be the unique nontrivial element of $\mathrm{Gal}(K/F)$. By [30, Theorem 4.12], $Q_{K/F}$ is either 1 or 2. This can be seen in the following way. There is a homomorphism ϕ_K whose image contains $\boldsymbol{\mu}_K^2 = \phi_K(\boldsymbol{\mu}_K)$:

$$\phi_K : O_K^\times \to \boldsymbol{\mu}_K, \qquad u \mapsto u/\iota(u). \tag{7.2}$$

One easily checks that $\phi_K(u) \in \boldsymbol{\mu}_K^2$ if and only if $u \in \boldsymbol{\mu}_K O_F^\times$, hence $Q_{K/F} = [\phi_K(O_K^\times) : \boldsymbol{\mu}_K^2] \le 2$. Moreover, $Q_{K/F} = 2$ if and only if ϕ_K is surjective, i.e. there exists $z \in O_K^\times$ such that

$$z = \iota(z)\zeta_{2n}. \tag{7.3}$$

We note that (7.2) also implies that

$$u^2 \equiv \mathrm{N}_{K/F}(u) \pmod{\boldsymbol{\mu}_K}, \quad \forall u \in O_K^\times. \tag{7.4}$$

Consider the quotient group $O_K^\times/O_F^\times$. If $Q_{K/F} = 1$, then $O_K^\times = \boldsymbol{\mu}_K O_F^\times$, and

$$O_K^\times/O_F^\times \cong \boldsymbol{\mu}_K/\boldsymbol{\mu}_F = \boldsymbol{\mu}_K/\{\pm 1\}, \tag{7.5}$$

which is a cyclic group of order n generated by the image of ζ_{2n}. If $Q_{K/F} = 2$, there is an exact sequence

$$1 \to (\boldsymbol{\mu}_K O_F^\times)/O_F^\times \to O_K^\times/O_F^\times \to \boldsymbol{\mu}_K/\boldsymbol{\mu}_K^2 \to 1. \tag{7.6}$$

Let $z \in O_K^\times$ be an element satisfying (7.3). Then

$$z^2 = \mathrm{N}_{K/F}(z)\zeta_{2n}, \tag{7.7}$$

so $\zeta_{2n} \equiv z^2 \pmod{O_F^\times}$. Therefore, $O_K^\times/O_F^\times$ is a cyclic group of order $2n$ generated by the image of z in this case. Either way, $O_K^\times/O_F^\times$ is a cyclic group. Its order $w_K := |O_K^\times/O_F^\times|$ is given by

$$w_K = \frac{1}{2}|\boldsymbol{\mu}_K| \cdot Q_{K/F} = \begin{cases} |\boldsymbol{\mu}_K|/2 & \text{if} \quad Q_{K/F} = 1; \\ |\boldsymbol{\mu}_K| & \text{if} \quad Q_{K/F} = 2. \end{cases} \tag{7.8}$$

For the rest of this section, we assume that $F = \mathbb{Q}(\sqrt{d}\,)$ is a real quadratic field with square free $d \in \mathbb{N}$. We will soon specialize further to the case that $F = \mathbb{Q}(\sqrt{p}\,)$ with a prime $p \in \mathbb{N}$. Recall that

$$O_F = \begin{cases} \mathbb{Z}\left[(1+\sqrt{d}\,)/2\right] & \text{if} \quad d \equiv 1 \pmod 4; \\ \mathbb{Z}[\sqrt{d}\,] & \text{if} \quad d \equiv 2, 3 \pmod 4. \end{cases}$$

The *fundamental unit* by definition is the unit $\epsilon \in O_F^\times$ such that $O_F^\times = \{\pm\epsilon^a \mid a \in \mathbb{Z}\}$ and $\epsilon > 1$. Note that ϵ is totally positive if and only if $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = 1$.

Lemma 7.2. *Let ϵ be the fundamental unit of $F = \mathbb{Q}(\sqrt{d}\,)$, and K a totally imaginary quadratic extension of F with $\boldsymbol{\mu}_K = \langle\zeta_{2n}\rangle$. The index $Q_{K/F} = 2$ if and only if $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = 1$ and the equation*

$$z^2 = \epsilon\,\zeta_{2n} \tag{7.9}$$

has a solution in K. In particular, if $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = -1$, then $Q_{K/F} = 1$.

Proof. Only the first statement needs to be proved, as the second one follows easily. The sufficiency is obvious. We prove the "only if" part. Suppose that $Q_{K/F} = 2$. Let $z \in O_K^\times$ be a representative of a generator of $O_K^\times/\boldsymbol{\mu}_K \cong \mathbb{Z}$. By (7.4), $O_F^\times/\boldsymbol{\mu}_F$ can be generated by a totally positive unit, namely $\mathrm{N}_{K/F}(z)$. Therefore, ϵ must be totally positive, which happens if and only if $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = 1$. Replacing z by $1/z$ if necessary, we may assume $\mathrm{N}_{K/F}(z) = \epsilon$. By (7.6), there exists an odd number $2c+1 \in \mathbb{Z}$ such that $z = \iota(z)\zeta_{2n}^{2c+1}$. We further replace z by $z\zeta_{2n}^{-c}$, then it satisfies equation (7.9). □

7.3. Since $[K : \mathbb{Q}] = 4$, we have $\varphi(2n) \le 4$. The possible n's are $1, 2, 3, 4, 5, 6$. Moreover, the cases $n = 4, 5, 6$ can only happen in the following situations:

- if $n = 4$, then $K = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}\,, \sqrt{2}\,)$ and $F = \mathbb{Q}(\sqrt{2}\,)$;
- if $n = 5$, then $K = \mathbb{Q}(\zeta_{10})$ and $F = \mathbb{Q}(\sqrt{5}\,)$;
- if $n = 6$, then $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{3}\,, \sqrt{-1}\,)$ and $F = \mathbb{Q}(\sqrt{3}\,)$.

Lemma 7.4. *Let ϵ be the fundamental unit of $F = \mathbb{Q}(\sqrt{p}\,)$, where $p \in \mathbb{N}$ is a prime number. Then $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = 1$ if and only if $p \equiv 3 \pmod 4$.*

Proof. If $p = 2$, then $\epsilon = 1 + \sqrt{2}$, so $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = -1$. By [7, Corollary 18.4bis, p. 134], if $p \equiv 1 \pmod 4$, the norm of the fundamental unit is -1. On the other hand, if $p \equiv 3 \pmod 4$, we claim that $\mathrm{N}_{F/\mathbb{Q}}(u) = 1$ for any $u \in O_F^\times$. Indeed, If $u = a + b\sqrt{p}$ has norm -1, then $a^2 - b^2 p = -1$. Modulo p on both sides, we see that -1 is a square in $\mathbb{Z}/p\mathbb{Z}$, contradicting to the assumption $p \equiv 3 \pmod 4$. □

Proposition 7.5. *Suppose that $p \equiv 3 \pmod 4$, and ϵ is the fundamental unit of $F = \mathbb{Q}(\sqrt{p}\,)$. Then $\sqrt{\epsilon/2} \in F$, and $\sqrt{\epsilon/2} \equiv (1+\sqrt{p}\,)/2 \pmod{O_F}$.*

Proof. It is known that $\epsilon = 2x^2$ for some $x \in F$ when $p \equiv 3 \pmod 4$ (cf. [20, Lemma 3, p. 91] or [36, Lemma 3.2(1)]). We have $(2x)^2 = 2\epsilon \equiv 0 \pmod{2O_F}$. Clearly, $2x \in O_F$ but $x \notin O_F$. On the other hand, $1+\sqrt{p}$ is the only nonzero nilpotent element in $O_F/2O_F$. So we must have $2x \equiv 1+\sqrt{p} \pmod{2O_F}$, and the second part of the proposition follows. □

Proposition 7.6. *Suppose that $p \equiv 3 \pmod 4$. Let ϵ be the (totally positive) fundamental unit of $F = \mathbb{Q}(\sqrt{p}\,)$, and $K = F(\sqrt{-\epsilon}\,)$. Then $K = F(\sqrt{-2}\,) = \mathbb{Q}(\sqrt{p}\,,\sqrt{-2}\,)$, and $O_K = \mathbb{Z}[\sqrt{p}\,,\sqrt{-\epsilon}\,]$.*

Proof. By Proposition 7.5, $K = \mathbb{Q}(\sqrt{p}\,,\sqrt{-2}\,)$. Let $B := \mathbb{Z}[\sqrt{p}\,,\sqrt{-\epsilon}\,] = O_F[\sqrt{-\epsilon}\,] \subseteq O_K$, and $\mathfrak{d}_B = \mathfrak{d}_{B/\mathbb{Z}}$ be the discriminant of B with respect to $\mathbb{Z}$. To show that $B = O_K$, it is enough to show that $\mathfrak{d}_B$ coincides with $\mathfrak{d}_{O_K} = \mathfrak{d}_K$, the absolute discriminant of K. We have $\mathfrak{d}_K = 4p \cdot (-8) \cdot (-8p) = 2^8p^2$ by Exercise 42(f) of [19, Chapter 2]. On the other hand,

$$\mathfrak{d}_B = \mathfrak{d}_F^2 \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{d}_{B/O_F}) = (4p)^2 \cdot \mathrm{N}_{F/\mathbb{Q}}(-4\epsilon) = 2^8p^2 = \mathfrak{d}_K.$$

So indeed $O_K = \mathbb{Z}[\sqrt{p}\,,\sqrt{-\epsilon}\,]$. □

The following proposition determines $Q_{K/F}$ for any totally imaginary quadratic extension K of $F = \mathbb{Q}(\sqrt{p}\,)$.

Proposition 7.7. *Suppose $F = \mathbb{Q}(\sqrt{p}\,)$. Then $Q_{K/F} = 2$ if and only if $p \equiv 3 \pmod 4$, and K is either $F(\sqrt{-1}\,) = \mathbb{Q}(\sqrt{p}\,,\sqrt{-1}\,)$ or $F(\sqrt{-\epsilon}\,) = \mathbb{Q}(\sqrt{p}\,,\sqrt{-2}\,)$.*

Proof. By Lemma 7.2 and Lemma 7.4, $Q_{K/F} = 1$ for all K if $p = 2$ or $p \equiv 1 \pmod 4$. Assume that $p \equiv 3 \pmod 4$ for the rest of the proof. Combining Lemma 7.2 and Proposition 7.5, we see that $Q_{K/F} = 2$ if and only if the equation

$$y^2 = 2\zeta_{2n} \tag{7.10}$$

has a solution in K. By Section 7.3, the possible values of n are $6, 3, 2, 1$.

If $n = 6$, then $p = 3$ and $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{3}\,,\sqrt{-1}\,)$. We claim that $\mathbb{Q}(\sqrt{2}\,\zeta_{24}) = K$. Indeed, $\mathbb{Q}(\sqrt{2}\,\zeta_{24}) = \mathbb{Q}(\zeta_3, \sqrt{2}\,\zeta_8)$. Since $\zeta_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{-2}}{2}$, our claim follows. Therefore, (7.10) has a solution in K and $Q_{K/F} = 2$ in this case.

Assume that $p > 3$ for the rest of the proof.

If $n = 3$, then $K = \mathbb{Q}(\sqrt{p}\,,\sqrt{-3}\,)$. If $\sqrt{2}\,\zeta_{12} \in K$, then it implies that $\sqrt{-2} = \sqrt{2}\,\zeta_4 \in K$, which is clearly false. Therefore, $Q_{K/F} = 1$ if $K = \mathbb{Q}(\sqrt{p}\,,\sqrt{-3}\,)$ with $p > 3$.

If $n = 2$, then $K = \mathbb{Q}(\sqrt{p}\,,\sqrt{-1}\,)$. We have $(1+\sqrt{-1}\,)^2 = 2\sqrt{-1} = 2\zeta_4$. Therefore, $Q_{K/F} = 2$ in this case.

Lastly, suppose that $n = 1$. Then $Q_{K/F} = 2$ implies that $K = F(\sqrt{-2}\,) = \mathbb{Q}(\sqrt{p}\,,\sqrt{-2}\,)$. One easily checks that $\boldsymbol{\mu}_K$ is indeed $\{\pm 1\}$ so this is also sufficient for $Q_{K/F} = 2$. □

In the case where $F = \mathbb{Q}(\sqrt{d}\,)$ is an arbitrary real quadratic field and K is an imaginary bicyclic biquadratic field containing F, the calculation of $Q_{K/F}$ is discussed in [5, Section 2].

7.8. The following table gives a complete list of the extensions $K/\mathbb{Q}(\sqrt{p}\,)$ with $w_K = [O_K^\times : O_{\mathbb{Q}(\sqrt{p}\,)}^\times] > 1$ for all primes p.

p	K	w_K	p	K	w_K	$p>5$	K	w_K
2	$\mathbb{Q}(\sqrt{2},\sqrt{-1})$	4	5	$\mathbb{Q}(\sqrt{5},\sqrt{-1})$	2	$p\equiv 1\ (4)$	$\mathbb{Q}(\sqrt{p},\sqrt{-1})$	2
	$\mathbb{Q}(\sqrt{2},\sqrt{-3})$	3		$\mathbb{Q}(\sqrt{5},\sqrt{-3})$	3		$\mathbb{Q}(\sqrt{p},\sqrt{-3})$	3
3	$\mathbb{Q}(\sqrt{3},\sqrt{-1})$	12		$\mathbb{Q}(\zeta_{10})$	5	$p\equiv 3\ (4)$	$\mathbb{Q}(\sqrt{p},\sqrt{-1})$	4
	$\mathbb{Q}(\sqrt{3},\sqrt{-2})$	2					$\mathbb{Q}(\sqrt{p},\sqrt{-2})$	2
							$\mathbb{Q}(\sqrt{p},\sqrt{-3})$	3

It is well known that the class numbers (cf. [30, Theorem 11.1])

$$h(\mathbb{Q}(\zeta_8)) = h(\mathbb{Q}(\zeta_{10})) = h(\mathbb{Q}(\zeta_{12})) = 1. \tag{7.11}$$

Using Magma, one easily calculates that

$$h(\mathbb{Q}(\sqrt{2},\sqrt{-3})) = h(\mathbb{Q}(\sqrt{5},\sqrt{-1})) = h(\mathbb{Q}(\sqrt{5},\sqrt{-3})) = 1, \tag{7.12}$$

$$h(\mathbb{Q}(\sqrt{3},\sqrt{-2})) = 2. \tag{7.13}$$

7.9. Let $E_j = \mathbb{Q}(\sqrt{-j})$ for $j = 1, 2, 3$, and $\mathfrak{d}_{E_j}$ be the discriminant of E_j. Suppose that p is *odd*, and $\mathfrak{d}_F$ is the discriminant of $F = \mathbb{Q}(\sqrt{p})$. Consider the biquadratic field $K_j := \mathbb{Q}(\sqrt{p},\sqrt{-j})$, which is the compositum of F with E_j. If $p = 3$, we only take K_1 and K_2. Proposition 7.7 shows the following simple but mysterious criterion:

$$Q_{K_j/F} = 1 \qquad \Longleftrightarrow \qquad \gcd(\mathfrak{d}_F, \mathfrak{d}_{E_j}) = 1. \tag{7.14}$$

7.10. Suppose for the moment that $F = \mathbb{Q}(\sqrt{d})$ is an arbitrary real quadratic field, and K is the compositum of F with an imaginary quadratic field E. By the work of Herglotz [10], if $K \neq \mathbb{Q}(\sqrt{2},\sqrt{-1})$, then

$$h(K) = Q_{K/F} h(F) h(E) h(E')/2, \tag{7.15}$$

where E' is the only other imaginary quadratic subfield of K distinct from E. In particular, if $F = \mathbb{Q}(\sqrt{p})$, $K_j = \mathbb{Q}(\sqrt{p},\sqrt{-j})$ and $\Bbbk_j = \mathbb{Q}(\sqrt{-pj})$ with $j = 1, 2, 3$ and $p \geq 5$, then

$$h(K_j) = \begin{cases} h(F)h(\Bbbk_j) & \text{if } j = 1,2 \text{ and } p \equiv 3 \pmod 4; \\ h(F)h(\Bbbk_j)/2 & \text{otherwise.} \end{cases} \tag{7.16}$$

Here we used the facts that $h(\mathbb{Q}(\sqrt{-j})) = 1$ for all $j \in \{1, 2, 3\}$ and $Q_{K_j/F}$ is calculated in Proposition 7.7.

7.11. Suppose that p is odd, and $K = K_1 = \mathbb{Q}(\sqrt{p},\sqrt{-1})$. Let $L = \mathbb{Q}(\sqrt{p^*}) \subset K$, where $p^* := \left(\frac{-1}{p}\right) p$, and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Then $O_L = \mathbb{Z} \oplus \mathbb{Z}\omega_p$, with $\omega_p := (1+\sqrt{p^*})/2 \in O_L$. Since $\gcd(\mathfrak{d}_L, \mathfrak{d}_{\mathbb{Q}(\sqrt{-1})}) = 1$, we have $O_K = O_L[\sqrt{-1}]$ and a $\mathbb{Z}$-basis of O_K is given by

$$\left\{1, \quad \frac{1+\sqrt{p^*}}{2}, \quad \sqrt{-1}, \quad \frac{\sqrt{-1}+\sqrt{-p^*}}{2}\right\}. \tag{7.17}$$

We claim that $|(O_K/2O_K)^\times| = 4\left(2 - \left(\frac{2}{p}\right)\right)$. Indeed, we have

$$O_K/2O_K \cong (O_L/2O_L)[t]/(t^2+1) = (O_L/2O_L)[t]/((t+1)^2), \tag{7.18}$$

with the isomorphism sending $\sqrt{-1} \mapsto \bar{t}$, which denotes the image of t in the quotient. The isomorphism (7.18) gives rise to an exact sequence

$$0 \to (O_L/2O_L) \to (O_K/2O_K)^\times \to (O_L/2O_L)^\times \to 1. \tag{7.19}$$

Note that 2 is unramified in L, and

$$O_L/2O_L \simeq \begin{cases} \mathbb{F}_2 \oplus \mathbb{F}_2 & \text{if } \left(\frac{2}{p}\right) = 1; \\ \mathbb{F}_4 & \text{if } \left(\frac{2}{p}\right) = -1. \end{cases} \tag{7.20}$$

Hence the exact sequence (7.19) splits. More precisely,

$$(O_K/2O_K)^\times \simeq \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } \left(\frac{2}{p}\right) = 1; \\ (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } \left(\frac{2}{p}\right) = -1. \end{cases} \tag{7.21}$$

7.12. Consider the order $B_{1,4} := \mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,] = \mathbb{Z}[\sqrt{p^*}\,, \sqrt{-1}\,]$ in $K = \mathbb{Q}(\sqrt{p}\,, \sqrt{-1}\,)$ with p odd. Since $\mathbb{Z}[\sqrt{p^*}\,]/2O_L \cong \mathbb{F}_2$, we have $2O_K \subset B_{1,4}$, and

$$O_K/2O_K \supset B_{1,4}/2O_K \cong (\mathbb{Z}[\sqrt{p^*}\,]/2O_L)[t]/((t+1)^2) \cong \mathbb{F}_2[t]/((t+1)^2) \tag{7.22}$$

under the isomorphism (7.18). In particular, $(B_{1,4}/2O_K)^\times \cong \mathbb{Z}/2\mathbb{Z}$.

Note that $O_L/2O_L$ is spanned by the image of 1 and ω_p over $\mathbb{F}_2$. One easily checks that the only other ring intermediate to

$$\mathbb{F}_2[t]/((t+1)^2) \subset (O_L/2O_L)[t]/((t+1)^2) = (O_L/2O_L) \oplus (O_L/2O_L)(1+\bar{t}\,) \tag{7.23}$$

is $\mathbb{F}_2 \oplus (O_L/2O_L)(1+\bar{t}\,)$. It follows that $B_{1,2} := \mathbb{Z} + \mathbb{Z}_{\sqrt{p}} + \mathbb{Z}\sqrt{-1} + \mathbb{Z}y_p^*$ is the only nontrivial suborder intermediate to $B_{1,4} \subset O_K$, where

$$y_p^* := \omega_p(1+\sqrt{-1}\,) = (1+\sqrt{p^*}\,)(1+\sqrt{-1}\,)/2.$$

However, it is more convenient to define $y_p := (1+\sqrt{-1}\,)(1+\sqrt{p}\,)/2$, then $B_{1,2} = \mathbb{Z} + \mathbb{Z}_{\sqrt{p}} + \mathbb{Z}\sqrt{-1} + \mathbb{Z}y_p$ as well. Note that $y_p^2 = (1+p)\sqrt{-1}\,/2 + \sqrt{-p}$, so $B_{1,2} = \mathbb{Z}[\sqrt{-1}\,, y_p]$. Since $B_{1,2}/2O_K \cong \mathbb{F}_2 \oplus (O_L/2O_L)(1+\bar{t}\,)$, we have

$$(B_{1,2}/2O_K)^\times \cong O_L/2O_L \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

8. O_F-orders in K

We keep the notations of Section 7. In particular, $F = \mathbb{Q}(\sqrt{p}\,)$ and its ring of integers is denoted by O_F. We will classify all the quadratic O_F-orders B satisfying the following two conditions:

(i) the fraction field of B is a totally imaginary quadratic extension K of F;
(ii) $w(B) = [B^\times : O_F^\times] > 1$.

Unless specified otherwise, the notation B will be reserved for such orders throughout this section. The quotient group $B^\times/O_F^\times$ is a subgroup of the finite cyclic group $O_K^\times/O_F^\times$, hence $w(B)$ divides $w_K = [O_K^\times : O_F^\times]$. Therefore, K must be one of the fields given in the table of Section 7.8.

Proposition 8.1. *Suppose that w_K is a prime. Then $B = O_K$ is the unique O_F-order in K such that $w(B) > 1$.*

Proof. By the table of Section 7.8, w_K is a prime only when $w_K = 2, 3, 5$. Then $O_K^\times/O_F^\times$ is a cyclic group of prime order with a nontrivial subgroup $B^\times/O_F^\times$. Therefore, $B^\times/O_F^\times = O_K^\times/O_F^\times$, so $B^\times = O_K^\times$. Then $B \supseteq O_F[u]$ for any $u \in O_K^\times$.

If $w_K = 5$, then $F = \mathbb{Q}(\sqrt{5}\,)$ and $K = \mathbb{Q}(\zeta_{10})$. We have $B \supseteq O_F[\zeta_{10}] \supseteq \mathbb{Z}[\zeta_{10}]$. But $\mathbb{Z}[\zeta_{10}]$ is the maximal order in K. So $B = O_K = \mathbb{Z}[\zeta_{10}]$.

If $Q_{K/F} = 2$ and $w_K = 2$, then $p \equiv 3 \pmod 4$ and $K = F(\sqrt{-\epsilon}\,) = \mathbb{Q}(\sqrt{p}\,, \sqrt{-2}\,)$. Proposition 7.6 shows that $O_F[\sqrt{-\epsilon}\,] = O_K$ is the maximal order in K. So $B = O_K = O_F[\sqrt{-\epsilon}\,]$.

Suppose that $Q_{K/F} = 1$, p is odd and $K \neq \mathbb{Q}(\zeta_{10})$. In other words, we assume one of the following holds:

- $p \equiv 1 \pmod 4$, and $K \neq \mathbb{Q}(\zeta_{10})$;
- $p \equiv 3 \pmod 4$, $p \neq 3$, and $K = F(\zeta_6) = \mathbb{Q}(\sqrt{p}\,, \sqrt{-3}\,)$.

Then we have $K = \mathbb{Q}(\sqrt{p}\,, \sqrt{-j}\,)$ with $j \in \{1, 3\}$, which depends on p. By Section 7.9, the assumption $Q_{K/F} = 1$ guarantees that the discriminants of $\mathbb{Q}(\sqrt{p}\,)$ and $\mathbb{Q}(\sqrt{-j}\,)$ are relatively prime. Let $\zeta = \zeta_4$ if $j = 1$ and $\zeta = \zeta_6$ if $j = 3$. Then $B \supseteq O_F[\zeta]$. By [18, Proposition III.17], $O_F[\zeta]$ is the maximal order in K. Therefore $B = O_K$.

The only remaining case to consider is $F = \mathbb{Q}(\sqrt{2}\,)$ and $K = F(\zeta_6) = \mathbb{Q}(\sqrt{2}\,, \sqrt{-3}\,)$. We note that the discriminants of $\mathbb{Q}(\sqrt{2}\,)$ and $\mathbb{Q}(\sqrt{-3}\,)$ are again relatively prime. So the same argument as above shows that $B = O_K$. □

Lemma 8.2. *Suppose that $p \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{p}\,, \sqrt{-1}\,)$. Let $B \subseteq O_K$ be a quadratic O_F-order with $2 \mid w(B)$. Then $B_{1,4} = \mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,] \subseteq B$. Moreover, $4 \mid w(B)$ if and only if $y_p = (1 + \sqrt{-1}\,)(1 + \sqrt{p}\,)/2 \in B$.*

Proof. If $p = 3$, then $O_K^\times/O_F^\times$ is a cyclic group of order 12, generated by the image of $z = \sqrt{\epsilon\zeta_{12}} \in O_K^\times$. Since $2 \mid w(B)$, we have $B \ni z^6 = \epsilon^3\sqrt{-1}\,$. Then $\sqrt{-1} \in B^\times$ as $\epsilon \in O_F^\times \subset B^\times$. We have $4 \mid w(B)$ if and only if $B \ni z^3 = \epsilon\sqrt{\epsilon}\,\zeta_8$, or equivalently, $B \ni \sqrt{\epsilon}\,\zeta_8$.

If $p > 3$ and $p \equiv 3 \pmod 4$, then $O_K^\times/O_F^\times$ is a cyclic group of order 4 generated by $z = \sqrt{\epsilon\zeta_4}\,$. If $2 \mid w(B)$, then $B \ni z^2 = \epsilon\sqrt{-1}\,$, so $\sqrt{-1} \in B$. Moreover, $w(B) = 4$ if and only if $B \ni z = \sqrt{\epsilon}\,\zeta_8$.

It remains to show that $\sqrt{\epsilon}\,\zeta_8 \in B$ if and only if $y_p \in B$. By Proposition 7.5, there exists $m, n \in \mathbb{Z}$ such that $\sqrt{\epsilon/2} = m + n\sqrt{p} + (1 + \sqrt{p}\,)/2$. We then have

$$\sqrt{\epsilon}\,\zeta_8 = \sqrt{\epsilon/2}\,\cdot(\sqrt{2}\,\zeta_8) = \left(m + n\sqrt{p} + \frac{1+\sqrt{p}}{2}\right)(1 + \sqrt{-1}\,).$$

But B already contains $\mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,]$ by the above arguments, so $\sqrt{\epsilon}\,\zeta_8 \in B$ if and only if $y_p = (1 + \sqrt{-1}\,)(1 + \sqrt{p}\,)/2 \in B$. □

Proposition 8.3. *Suppose that $p \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{p}\,, \sqrt{-1}\,)$. The O_F-orders $B \subseteq O_K$ with $2 \mid w(B)$ are:*

$$\begin{aligned} O_K, &\qquad w(O_K) = 4\gcd(p, 3); \\ B_{1,2} = \mathbb{Z}[\sqrt{-1}\,, y_p], &\qquad w(B_{1,2}) = 4; \\ B_{1,4} = \mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,], &\qquad w(B_{1,4}) = 2. \end{aligned}$$

If $p > 3$, the above is a complete list of O_F-orders in K with $w(B) > 1$. If $p = 3$, there is an extra order $B_{1,3} = \mathbb{Z}[\sqrt{3}\,, \zeta_6]$ with $w(B_{1,3}) = 3$.

Proof. Recall that $w_K = 4$ or 12. Given any $B \subseteq O_K$ with $w(B) > 1$, we have either $2 \mid w(B)$ or $w(B) = 3$, with the latter case possible only if $p = 3$.

Suppose that $2 \mid w(B)$. Then $B \supseteq B_{1,4} := \mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,]$ by Lemma 8.2. By Section 7.12, $B_{1,2}$ is the only O_F-order of index 2 intermediate to $B_{1,4} \subset O_K$. Since $y_p \notin B_{1,4}$, we have $w(B_{1,4}) = 2$ by Lemma 8.2. On the other hand, $4 \mid w(B_{1,2})$. So $w(B_{1,2}) = 4$ if $p > 3$. Note that $\zeta_{12} = (\sqrt{3} + \sqrt{-1}\,)/2 \notin B_{1,2}$ if $p = 3$. Hence $w(B_{1,2}) = 4$ in this case as well.

Suppose that $p = 3$, $z = \sqrt{\epsilon\zeta_{12}}$ and $3 \mid w(B)$. Then $B \ni z^4 = \epsilon^2\zeta_6$ and hence $B \supseteq \mathbb{Z}[\sqrt{3}\,, \zeta_6]$. A $\mathbb{Z}$-basis of $B_{1,3} := \mathbb{Z}[\sqrt{3}\,, \zeta_6]$ is given by

$$\left\{1, \quad \sqrt{3}\,, \quad \zeta_6 = \frac{1+\sqrt{-3}}{2}, \quad \sqrt{3}\,\zeta_6 = \frac{\sqrt{3}+3\sqrt{-1}}{2}\right\}.$$

One easily checks that $[O_K : B_{1,3}] = 3$. Hence the only other O_F-order containing $B_{1,3}$ is O_K itself. Since $\sqrt{-1} \notin B_{1,3}$, we have $w(B_{1,3}) = 3$. □

For the rest of this section, we study the class numbers $h(B)$ of those non-maximal orders B with $w(B) > 1$.

8.4. For the moment let us assume that K is an arbitrary number field, and $B \subseteq O_K$ is an order in K with conductor $\mathfrak{f}$. The class number of B is given by [22, Theorem I.12.12]

$$h(B) = \frac{h(O_K)[(O_K/\mathfrak{f})^\times : (B/\mathfrak{f})^\times]}{[O_K^\times : B^\times]}. \tag{8.1}$$

We leave it as an exercise to show that $[(O_K/\mathfrak{a})^\times : (B/\mathfrak{a})^\times] = [(O_K/\mathfrak{f})^\times : (B/\mathfrak{f})^\times]$ for any nonzero ideal $\mathfrak{a}$ of O_K contained in $\mathfrak{f}$. Therefore,

$$h(B) = \frac{h(O_K)[(O_K/\mathfrak{a})^\times : (B/\mathfrak{a})^\times]}{[O_K^\times : B^\times]}. \tag{8.2}$$

Lemma 8.5. *Suppose that $p \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{p}\,, \sqrt{-1}\,)$. Let $B_{1,2}$ and $B_{1,4}$ be the orders in Proposition 8.3. We have*

$$h(B_{1,2}) = h(B_{1,4}) = \left(2 - \left(\frac{2}{p}\right)\right) h(O_K) \tag{8.3}$$

if $p > 3$ and $p \equiv 3 \pmod 4$. If $p = 3$, then $h(B_{1,2}) = h(B_{1,4}) = h(O_K)$.

Proof. By Section 7.12, we have $O_K \supset B_{1,2} \supset B_{1,4} \supset 2O_K$. So take $\mathfrak{a} = 2O_K$ in (8.2). It has been shown in Sections 7.11 and 7.12 that

$$|(O_K/2O_K)^\times| = 4\left(2 - \left(\frac{2}{p}\right)\right), \quad |(B_{1,2}/2O_K)^\times| = 4 \quad \text{and} \quad |(B_{1,4}/2O_K)^\times| = 2.$$

On the other hand, $[O_K^\times : B^\times] = w_K/w(B)$ for $B = B_{1,2}$ or $B_{1,4}$. Recall that $w_K = 4$ if $p > 3$ and $w_K = 12$ if $p = 3$. The lemma now follows from Proposition 8.3, where it has been shown that $w(B_{1,2}) = 4$ and $w(B_{1,4}) = 2$. □

8.6. Assume that $F = \mathbb{Q}(\sqrt{2}\,)$ and $K = F(\zeta_8) = \mathbb{Q}(\sqrt{2}\,, \sqrt{-1}\,)$. Then $w_K = 4$, and $O_K^\times/O_F^\times \cong \mathbb{Z}/4\mathbb{Z}$. Any $B \subseteq O_K$ with $w(B) > 1$ must contain $O_F[\zeta_8^2] = \mathbb{Z}[\sqrt{2}\,, \sqrt{-1}\,]$. By Exercise 42(b) of [19, Chapter 2], a $\mathbb{Z}$-basis of O_K is given by $\{1, \quad \sqrt{-1}\,, \quad \sqrt{2}\,, \quad (\sqrt{2} + \sqrt{-2}\,)/2\}$. Let $B = \mathbb{Z}[\sqrt{2}\,, \sqrt{-1}\,]$, which is a sublattice

of O_K of index 2. Therefore, there are no other quadratic O_F-orders B' in K with $w(B') > 1$ and $B' \neq O_K$. We have

$$w(O_K) = 4 \quad \text{and} \quad w(B) = 2. \tag{8.4}$$

Note that $\sqrt{2}\,O_K \subseteq B$. The ideal $\mathfrak{p} = (1+\zeta_8)O_K$ is the unique prime ideal above 2. Therefore, $O_K/\sqrt{2}\,O_K$ is a two-dimensional $\mathbb{F}_2$-algebra whose unit group $(O_K/\sqrt{2}\,O_K)^\times = (O_K/\mathfrak{p}^2)^\times \cong \mathbb{Z}/2\mathbb{Z}$. Since $[O_K : B] = 2$, we have $B/\sqrt{2}\,O_K \cong \mathbb{F}_2$. It follows that $h(B) = h(O_K) = 1$.

8.7. Let $K = \mathbb{Q}(\sqrt{3}\,,\sqrt{-1}\,)$ and $B_{1,3} = \mathbb{Z}[\sqrt{3}\,,\zeta_6]$. We have $\sqrt{-3}\,O_K \subset B_{1,3}$. On the other hand, $\sqrt{-3}\,O_K$ is a prime ideal in O_K with residue field $\mathbb{F}_9$. Since $[O_K : B_{1,3}] = 3$, we have $B_{1,3}/\sqrt{3}\,O_K \cong \mathbb{F}_3$. Therefore, $h(B_{1,3}) = h(O_K) = 1$.

9. Quadratic proper $\mathbb{Z}[\sqrt{p}\,]$-orders in K

Throughout this section, we assume that $p \equiv 1 \pmod 4$ and let $A = \mathbb{Z}[\sqrt{p}\,]$. It is an order of index 2 in $O_F = \mathbb{Z} + \mathbb{Z}(1+\sqrt{p}\,)/2$ with $A/2O_F \cong \mathbb{F}_2$. We will classify all the quadratic proper A-orders B satisfying the following two conditions:

(i) the fraction field of B is a totally imaginary quadratic extension K of F;
(ii) $w(B) := [B^\times : A^\times] > 1$.

First we need some knowledge about the group $A^\times$.

Lemma 9.1. *If $p \equiv 1 \pmod 8$, then $A^\times = O_F^\times$. In particular, the fundamental unit $\epsilon \in A^\times$.*

Proof. By our assumption on p, $2O_F = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal ideals of O_F with residue fields $O_F/\mathfrak{p}_1 = O_F/\mathfrak{p}_2 = \mathbb{F}_2$. Therefore,

$$(O_F/2O_F)^\times \cong (O_F/\mathfrak{p}_1)^\times \times (O_F/\mathfrak{p}_2)^\times$$

is a trivial group. We have $u \equiv 1 \pmod{2O_F}$ for any $u \in O_F^\times$. Hence $u \in A \cap O_F^\times = A^\times$. □

9.2. If $p \equiv 5 \pmod 8$, 2 is inert in O_F, and we have $(O_F/2O_F)^\times \simeq \mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$. Let $U^{(1)}$ be the kernel of the map $O_F^\times \to (O_F/2O_F)^\times$. Since $(A/2O_F)^\times$ is the trivial subgroup of $(O_F/2O_F)^\times$, we have $A^\times = U^{(1)}$. If $\epsilon \in A$, then $O_F^\times = A^\times = U^{(1)}$; otherwise, $O_F^\times/A^\times \simeq \mathbb{Z}/3\mathbb{Z}$, and $O_F^\times \to (O_F/2O_F)^\times$ is surjective. Here we are in a more complicated situation since both cases may occur, and whether $\epsilon \in A^\times$ or not can no longer be determined by a simple congruence condition on p. The list of $p \equiv 5 \pmod 8$ and $p < 1000$ such that $\epsilon \in A^\times$ are given bellow:

37, 101, 197, 269, 349, 373, 389, 557, 677, 701, 709, 757, 829, 877, 997.

This is the sequence A130229 in the OEIS [27]. For any $p \equiv 1 \pmod 4$, we define

$$\varpi := [O_F^\times : A^\times] \in \{1, 3\}. \tag{9.1}$$

By Lemma 9.1, $\varpi = 1$ if $p \equiv 1 \pmod 8$.

9.3. Let $A_+^\times \subset A^\times$ be the subgroup consisting of all the totally positive elements of $A^\times$. We claim that

$$A_+^\times = (A^\times)^2. \tag{9.2}$$

If $\epsilon \in A$, then $A^\times = O_F^\times = \langle\epsilon\rangle \times \{\pm 1\}$. Since ϵ is not totally positive by Lemma 7.4, we have $A_+^\times = \langle\epsilon^2\rangle = (A^\times)^2$. If $\epsilon \notin A$, then $A^\times = \langle\epsilon^3\rangle \times \{\pm 1\}$ by Section 9.2. It follows that $A_+^\times = \langle\epsilon^6\rangle = (A^\times)^2$. So either way, (9.2) holds.

Lemma 9.4. *Let K be a totally imaginary quadratic extension of F such that there exists a quadratic proper A-order $B \subset K$ with $w(B) > 1$. Then K is necessarily one of the following*

$$K_1 = \mathbb{Q}(\sqrt{p}\,, \sqrt{-1}\,), \qquad K_3 = \mathbb{Q}(\sqrt{p}\,, \sqrt{-3}\,).$$

Moreover, if $K = K_1$, then $B \supseteq \mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,]$.

Proof. By Section 7.3, it is enough to show that $\boldsymbol{\mu}_K \neq \{\pm 1\}$, and $K \neq \mathbb{Q}(\zeta_{10})$ if $p = 5$.

First, if $p = 5$, the fundamental unit $\epsilon = (1 + \sqrt{5}\,)/2 \notin A$, and by Section 9.2, $O_F^\times / A^\times \cong \mathbb{Z}/3\mathbb{Z}$. Assume $K = \mathbb{Q}(\zeta_{10})$, then

$$\{1\} \subsetneq B^\times / A^\times \subseteq O_K^\times / A^\times = \langle \bar{\epsilon} \rangle \oplus \left\langle \bar{\zeta}_{10} \right\rangle \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z},$$

where $\bar{\epsilon}$ and $\bar{\zeta}_{10}$ denote the image of ϵ and ζ_{10} respectively in the quotient $O_K^\times / A^\times$. Note that $B^\times / A^\times$ can not contain the subgroup $\langle \bar{\epsilon} \rangle \cong \mathbb{Z}/3\mathbb{Z}$. Otherwise, $B \ni \epsilon$, which implies that $B \supset \mathbb{Z}[\epsilon] = O_F$, contradicting to the assumption that B is a proper A-order. On the other hand, if $B^\times / A^\times \supseteq \left\langle \bar{\zeta}_{10} \right\rangle \cong \mathbb{Z}/5\mathbb{Z}$, then $B \ni \zeta_{10}$. Hence $B \supseteq \mathbb{Z}[\zeta_{10}]$, which is the maximal order in $K = \mathbb{Q}(\zeta_{10})$. Again this leads to a contradiction to the assumption on B. We conclude that $K \neq \mathbb{Q}(\zeta_{10})$ if $p = 5$.

Recall that $\boldsymbol{\mu}_K \supseteq \phi_K(B^\times)$, where $\phi_K : u \mapsto u/\iota(u)$ is the map given in (7.2). Clearly, $\phi_K(B^\times) \neq \{1\}$. Otherwise, $B^\times \subseteq O_F^\times \cap B = A^\times$, contradicting to the assumption that $w(B) > 1$.

Suppose that $-1 = \phi_K(u)$ for some $u \in B^\times$. We have $-u^2 = \mathrm{N}_{K/F}(u) \in A_+^\times$, the group of totally positive units of A. Since $A_+^\times = (A^\times)^2$ by (9.2), multiplying u by a suitable element of $A^\times$, we may assume that $u^2 = -1$. Therefore, $K = K_1 = F(\sqrt{-1}\,)$. On the other hand, if $K = K_1$, then by Section 7.1, $\phi_K(O_K^\times) = \boldsymbol{\mu}_K^2 = \{\pm 1\}$ since $Q_{K/F} = 1$. Therefore, $\phi_K(u) = -1$ for all $u \in B^\times - A^\times$. We have in fact shown that $B \ni \sqrt{-1}$ for all proper A-orders in K_1 with $w(B) > 1$.

Lastly, if $-1 \notin \phi_K(B^\times)$, then $\phi_K(B^\times)$ contains a root of unity which is not in F. In particular, $\boldsymbol{\mu}_K \neq \{\pm 1\}$ and $w_K > 1$. By Section 7.3, we must have $K = K_3 = F(\sqrt{-3}\,)$ since all other possibilities have been exhausted. □

9.5. Suppose that $K = K_1$. It has been shown in Lemma 9.4 that $B \supseteq B_{1,4} = \mathbb{Z}[\sqrt{p}\,, \sqrt{-1}\,]$. By Section 7.12,

$$B_{1,2} = \mathbb{Z} + \mathbb{Z}\sqrt{p} + \mathbb{Z}\sqrt{-1} + \mathbb{Z}(1 + \sqrt{-1}\,)(1 + \sqrt{p}\,)/2$$

is the only other proper A-order that contains $B_{1,4}$. The class numbers of $B_{1,2}$ and $B_{1,4}$ can be calculated exactly in the same way as in Lemma 8.5. Let B be either $B_{1,2}$ or $B_{1,4}$. If $\epsilon \in A$, then $O_K^\times / A^\times = O_K^\times / O_F^\times \cong \mathbb{Z}/2\mathbb{Z}$. Hence $B^\times = O_K^\times$. If $\epsilon \notin A^\times$, $O_K^\times / A^\times \cong \mathbb{Z}/6\mathbb{Z}$, with the cyclic subgroup of order 3 generated by $\bar{\epsilon}$. Since $\epsilon \notin B$, we must have $B^\times / A^\times \cong \mathbb{Z}/2\mathbb{Z}$ in this case as well. Therefore,

$$w(B_{1,2}) = w(B_{1,4}) = 2. \tag{9.3}$$

Using $[O_K^\times : A^\times] = 2\varpi$, we obtain

$$h(B_{1,2}) = \frac{1}{\varpi}\left(2 - \left(\frac{2}{p}\right)\right) h(O_{K_1}) \text{ and } h(B_{1,4}) = \frac{2}{\varpi}\left(2 - \left(\frac{2}{p}\right)\right) h(O_{K_1}). \tag{9.4}$$

9.6. Suppose that $K = K_3$. By Exercise 42 of [19, Chapter 2], a $\mathbb{Z}$-basis of $\mathcal{O}_{K_3}$ is

$$\left\{1, \quad \omega_p = \frac{1+\sqrt{p}}{2}, \quad \zeta_6 = \frac{1+\sqrt{-3}}{2}, \quad \omega_p\zeta_6 = \frac{(1+\sqrt{p}\,)(1+\sqrt{-3}\,)}{4}\right\}. \tag{9.5}$$

Note that 2 is inert in $L := \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3}\,) \subset K$. There are two primes $\mathfrak{p}_1, \mathfrak{p}_2$ above $2O_L$ in K. Both have residue fields $O_K/\mathfrak{p}_1 \simeq O_K/\mathfrak{p}_2 \simeq \mathbb{F}_4$. Therefore, $O_L/2O_L \simeq \mathbb{F}_4$ embeds diagonally[2] into

$$O_K/2O_K \cong (O_K/\mathfrak{p}_1) \times (O_K/\mathfrak{p}_2) \simeq \mathbb{F}_4 \times \mathbb{F}_4. \tag{9.6}$$

Suppose that $B \supseteq B_{3,4} := \mathbb{Z}[\sqrt{p}\,, \zeta_6]$. Since $B_{3,4}/2O_K$ is a 2-dimensional $\mathbb{F}_2$-vector space spanned by the images of 1 and ζ_6, we have a canonical isomorphism $B_{3,4}/2O_K \cong O_L/2O_L$. The only other subring of $\mathbb{F}_4 \times \mathbb{F}_4$ containing the diagonal is $\mathbb{F}_4 \times \mathbb{F}_4$ itself. It follows that $B_{3,4}$ is the only proper A-order in K containing ζ_6.

We calculate the class number of $B_{3,4}$ using (8.2) with $\mathfrak{a} = 2O_K$. It has already been shown that $(B_{3,4}/2O_K)^\times \simeq \mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, and

$$(O_K/2O_K)^\times \cong (O_K/\mathfrak{p}_1)^\times \times (O_K/\mathfrak{p}_2)^\times \simeq (\mathbb{Z}/3\mathbb{Z})^2. \tag{9.7}$$

If $\epsilon \in A$, then $O_K^\times = B_{3,4}^\times$; otherwise, $O_K^\times/B_{3,4}^\times$ is a cyclic group of order 3, generated by the image of ϵ. It follows that

$$w(B_{3,4}) = 3, \qquad h(B_{3,4}) = \frac{3h(O_{K_3})}{\varpi} = \begin{cases} 3h(O_{K_3}) & \text{if } \epsilon \in A; \\ h(O_{K_3}) & \text{if } \epsilon \notin A. \end{cases} \tag{9.8}$$

9.7. Suppose that $K = K_3 = \mathbb{Q}(\sqrt{p}\,, \sqrt{-3}\,)$, and $\varpi = 1$. In other words, we assume $\epsilon \in A^\times$ and $O_F^\times = A^\times$. For example, this is the case if $p \equiv 1 \pmod 8$ by Lemma 9.1. For any quadratic proper A-order B with $w(B) > 1$, we have

$$\{1\} \subsetneq B^\times/A^\times \subseteq O_K^\times/A^\times \simeq \mathbb{Z}/3\mathbb{Z}.$$

Hence, $B^\times = O_K^\times$, and $B \supseteq \mathbb{Z}[\sqrt{p}\,, \zeta_6]$. It follows that $B_{3,4}$ is the only proper A-order with $w(B) > 1$ in this case.

9.8. Suppose that $K = K_3 = \mathbb{Q}(\sqrt{p}\,, \sqrt{-3}\,)$, and $\varpi = 3$. By an abuse of notation, we still write ϵ and ζ_6 for their images in $O_K^\times/A^\times$. Then

$$\{1\} \subsetneq B^\times/A^\times \subseteq O_K^\times/A^\times = \langle \epsilon, \zeta_6 \rangle \simeq (\mathbb{Z}/3\mathbb{Z})^2.$$

Since $\epsilon \notin B$, $B^\times/A^\times$ is one of the following cyclic subgroup of order 3 in $O_K^\times/A^\times$: $\langle \epsilon\zeta_6 \rangle, \langle \epsilon\zeta_6^{-1} \rangle, \langle \zeta_6 \rangle$. The case $B \ni \zeta_6$ has already been treated in the previous subsections. So we focus on the orders

$$B_{3,2} := A[\epsilon\zeta_6] = \mathbb{Z}[\sqrt{p}\,, \epsilon\zeta_6], \qquad B'_{3,2} := A[\epsilon\zeta_6^{-1}] = \mathbb{Z}[\sqrt{p}\,, \epsilon\zeta_6^{-1}].$$

Clearly $B'_{3,2}$ coincides with the complex conjugation of $B_{3,2}$.

Since $(\epsilon\zeta_6)^3 = -\epsilon^3 \in A$, the order $B_{3,2}$ is generated as a A-module by the set $\{1, \epsilon\zeta_6, \epsilon^2\zeta_6^2\}$. We claim that $B_{3,2} \supset 2O_K$. A $\mathbb{Z}$-basis of O_K is given in (9.5). Clearly, $2 \in A$ and $2\omega_p \in A$ with $\omega_p = (1+\sqrt{p}\,)/2$. Let $a = \mathrm{Tr}_{F/\mathbb{Q}}(\epsilon)$ and recall that $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = -1$, we have $\epsilon^2 = a\epsilon + 1$. Therefore,

$$\epsilon^2\zeta_6^2 = (a\epsilon + 1)(\zeta_6 - 1) = a\epsilon\zeta_6 + \zeta_6 - a\epsilon - 1.$$

[2]Since the isomorphisms $O_K/\mathfrak{p}_i \simeq \mathbb{F}_4$ is *not* canonical, the diagonal of $(O_K/\mathfrak{p}_1) \times (O_K/\mathfrak{p}_2)$ depends on the choice of $(O_K/\mathfrak{p}_1) \simeq (O_K/\mathfrak{p}_2)$. Here both of them are identified naturally with $O_L/2O_L$. In Section 9.8, we have a different diagonal. However, whichever diagonal we choose, the prime field $A/2O_F \cong \mathbb{F}_2$ embeds canonically in it.

It follows that $B_{3,2}$ is also generated over A by $\{1, \epsilon\zeta_6, \zeta_6 - a\epsilon\}$. Since $2a\epsilon \in A$, we have $2\zeta_6 = 2(\zeta_6 - a\epsilon) + 2a\epsilon \in B_{3,2}$. Lastly, we need to show that $2\omega_p\zeta_6 \in B_{3,2}$. Since $\epsilon \notin A$, there exists $x \in A$ such that $\epsilon = x + \omega_p$. Note that $2x\zeta_6 \in B_{3,2}$ because $2\zeta_6 \in B_{3,2}$, so $2\omega_p\zeta_6 = 2(\epsilon - x)\zeta_6 = 2\epsilon\zeta_6 - 2x\zeta_6 \in B_{3,2}$. This finishes the proof of our claim.

Next, we show that $B_{3,2}$ and $B'_{3,2}$ are indeed proper A-orders and calculate their class numbers. Since $p \equiv 5 \pmod 8$, we have $O_F/2O_F \simeq \mathbb{F}_4$, which is generated by the image of ϵ over $A/2O_F \cong \mathbb{F}_2$. Denote this image by $\bar{\epsilon}$. Recall that $O_K = O_F[\zeta_6]$, so

$$O_K/2O_K \simeq \mathbb{F}_4[t]/(t^2 - t + 1) \simeq \mathbb{F}_4 \times \mathbb{F}_4,$$

sending $t \mapsto (\bar{\epsilon}, \bar{\epsilon} + 1)$. One checks that $B_{3,2}/2O_K = \mathbb{F}_4 \times \mathbb{F}_2$, and $B'_{3,2} = \mathbb{F}_2 \times \mathbb{F}_4$. In particular, they do not contain the diagonal of $\mathbb{F}_4 \times \mathbb{F}_4$, which is identified with $O_F/2O_F$. Thus both $B_{3,2}$ and $B'_{3,2}$ are proper A-orders of index 2 in $O_K = O_{K_3}$, conforming with the convention of our notations. In particular,

$$w(B_{3,2}) = w(B'_{3,2}) = 3. \tag{9.9}$$

Using (8.2), one sees that

$$h(B_{3,2}) = h(B'_{3,2}) = h(O_{K_3}). \tag{9.10}$$

Lemma 9.9. *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 [8, 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. By (7.23), we have

$$O_{K_1}/B_{1,4} = \langle (1 + \sqrt{p}\,)/2 \rangle \simeq \mathbb{F}_2[1 + \sqrt{-1}\,]/(1 + \sqrt{-1}\,)^2$$

as $\mathbb{Z}[\sqrt{-1}\,]$-modules. Therefore, $B_{1,4}$ 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. □

9.10. In this subsection, we calculate the number of conjugacy classes of local optimal embeddings of B into $\mathbb{O}_8$ or $\mathbb{O}_{16}$ at $\ell = 2$. For $r = 8$ or 16, we write $m_{2,r}(B) = m(B_2, (\mathbb{O}_r)_2, (\mathbb{O}_r)_2^\times)$, where $(\mathbb{O}_r)_2 = \mathbb{O}_r \otimes_{\mathbb{Z}} \mathbb{Z}_2$ and $B_2 = B \otimes_{\mathbb{Z}} \mathbb{Z}_2$. 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 for any A-order $B \in \{B_{1,2}, B_{1,4}, B_{3,4}, B_{3,2}\}$, one has $m_{2,r}(B) \in \{0, 1\}$, and

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

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. We have $O_F B = O_K$ for all $B \in \{B_{1,2}, B_{1,4}, B_{3,4}, B_{3,2}\}$, 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

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

10. 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	$h(\mathbb{O}_1)$	Mass($\mathbb{O}_1$)	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
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

Continued on next page

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

p	$h(\mathbb{O}_1)$	Mass($\mathbb{O}_1$)	Ell($\mathbb{O}_1$)	$\zeta_F(-1)$	$h(F)$	$h(K_1)$	$h(K_2)$	$h(K_3)$
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

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

Acknowledgements

The project grew from Xue and 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 providing 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. The first named author is partially supported by the grant NSC 102-2811-M-001-090. The second and third named authors 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] Hyman Bass.
Torsion free and projective modules.
Trans. Amer. Math. Soc., 102:319–327, 1962.

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

[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] D. A. Buell, H. C. Williams, and K. S. Williams.
On the imaginary bicyclic biquadratic fields with class-number 2.
Math. Comp., 31(140):1034–1042, 1977.

[6] Wai Kiu Chan and Meinhard Peters.
Quaternary quadratic forms and Hilbert modular surfaces.
In *Algebraic and arithmetic theory of quadratic forms*, volume 344 of *Contemp. Math.*, pages 85–97. Amer. Math. Soc., Providence, RI, 2004.

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

[8] Charles W. Curtis and Irving 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.

[9] Martin Eichler.
Zur Zahlentheorie der Quaternionen-Algebren.
J. Reine Angew. Math., 195:127–151 (1956), 1955.

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

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

[12] Taira Honda.
Isogeny classes of abelian varieties over finite fields.
J. Math. Soc. Japan, 20:83–95, 1968.

[13] Kuniaki Horie and Mitsuko Horie.

CM-fields and exponents of their ideal class groups.
Acta Arith., 55(2):157–170, 1990.

[14] Loo Keng Hua.
Introduction to number theory.
Springer-Verlag, Berlin-New York, 1982.
Translated from the Chinese by Peter Shiu.

[15] Markus Kirschmer and John Voight.
Algorithmic enumeration of ideal classes for quaternion orders.
SIAM J. Comput., 39(5):1714–1747, 2010.

[16] Yoshiyuki Kitaoka.
Quaternary even positive definite quadratic forms of prime discriminant.
Nagoya Math. J., 52:147–161, 1973.

[17] Otto Körner.
Traces of Eichler-Brandt matrices and type numbers of quaternion orders.
Proc. Indian Acad. Sci. Math. Sci., 97(1-3):189–199 (1988), 1987.

[18] Serge Lang.
Algebraic number theory, volume 110 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, second edition, 1994.

[19] Daniel A. Marcus.
Number fields.
Springer-Verlag, New York, 1977.
Universitext.

[20] Thomas M. McCall, Charles J. Parry, and Ramona Ranalli.
Imaginary bicyclic biquadratic fields with cyclic 2-class group.
J. Number Theory, 53(1):88–99, 1995.

[21] David Mumford.
Abelian varieties, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*.
Published for the Tata Institute of Fundamental Research, Bombay, 2008.
With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[22] Jürgen 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.

[23] M. Peters.
Ternäre und quaternäre quadratische Formen und Quaternionenalgebren.
Acta Arith., 15:329–365, 1968/1969.

[24] Paul Ponomarev.
Arithmetic of quaternary quadratic forms.
Acta Arith., 29(1):1–48, 1976.

[25] Paul Ponomarev.
Class number formulas for quaternary quadratic forms.
Acta Arith., 39(1):95–104, 1981.

[26] 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.
[27] Warut Roonguthai.
The On-Line Encyclopedia of Integer Sequences.
Published electronically at `http://oeis.org/A130229`, Aug. 2007.
Primes $p \equiv 5 \pmod 8$ such that the Diophantine equation $x^2 - py^2 = -4$ has no solution in odd integers x, y.
[28] John 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.
[29] Marie-France Vignéras.
Arithmétique des algèbres de quaternions, volume 800 of *Lecture Notes in Mathematics*.
Springer, Berlin, 1980.
[30] Lawrence C. Washington.
Introduction to cyclotomic fields, volume 83 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, second edition, 1997.
[31] William C. Waterhouse.
Abelian varieties over finite fields.
Ann. Sci. École Norm. Sup. (4), 2:521–560, 1969.
[32] Fu-Tsun Wei and Chia-Fu Yu.
Class numbers of definite central simple algebras over global function functions.
Int. Math. Res. Not.
(2014) rnu038, 51 pp.
[33] Chia-Fu Yu.
Simple mass formulas on Shimura varieties of PEL-type.
Forum Math., 22(3):565–582, 2010.
[34] Chia-Fu Yu.
Superspecial abelian varieties over finite prime fields.
J. Pure Appl. Algebra, 216(6):1418–1427, 2012.
[35] Don Zagier.
On the values at negative integers of the zeta-function of a real quadratic field.
Enseignement Math. (2), 22(1-2):55–95, 1976.
[36] Zhe Zhang and Qin Yue.
Fundamental units of real quadratic fields of odd class number.
J. Number Theory, 137:122–129, 2014.

(Xue) Collaborative Innovation Centre of Mathematics, School of Mathematics and Statistics, Wuhan University, Luojiashan, Wuhan, Hubei, 430072, P.R. China.
E-mail address: `xue_j@whu.edu.cn`

(Yang) Institute of Mathematics, Academia Sinica, Astronomy-Mathematics Building, 6F, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN.
E-mail address: `tsechung@math.sinica.edu.tw`

(Yu) Institute of Mathematics, Academia Sinica and NCTS (Taipei Office), Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN.
E-mail address: `chiafu@math.sinica.edu.tw`

The Max-Planck-Institut für Mathematik, Vivatsgasse 7, Bonn, Germany 53111
E-mail address: `chiafu@mpim-bonn.mpg.de`