TAIWANESE JOURNAL OF MATHEMATICS
Vol. 20, No. 4, pp. 723–741, August 2016
DOI: 10.11650/tjm.20.2016.6464
This paper is available online at http://journal.tms.org.tw

Numerical Invariants of Totally Imaginary Quadratic $\mathbb{Z}[\sqrt{p}]$-orders

Jiangwei Xue, Tse-Chung Yang* and Chia-Fu Yu

Abstract. Let A be a real quadratic order of discriminant p or $4p$ with a prime p. In this paper we classify all proper totally imaginary quadratic A-orders B with index $w(B) = [B^\times : A^\times] > 1$. We also calculate numerical invariants of these orders including the class number, the index $w(B)$ and the numbers of local optimal embeddings of these orders into quaternion orders. These numerical invariants are useful for computing the class numbers of totally definite quaternion algebras.

1. Introduction

Let F be a totally real number field with the ring of integers O_F. Let D be a totally definite quaternion algebra over F and $\mathcal{O} \subset D$ an O_F-order in D. A main interest in the arithmetic of quaternion algebras is to compute the class number $h(\mathcal{O})$ of $\mathcal{O}$ (for locally free ideal classes). Eichler's class number formula states that

$$h(\mathcal{O}) = \mathrm{Mass}(\mathcal{O}) + \mathrm{Ell}(\mathcal{O}), \tag{1.1}$$

where $\mathrm{Mass}(\mathcal{O})$ is the mass of $\mathcal{O}$, which is (by definition) a weighted sum over all the ideal classes of $\mathcal{O}$, and $\mathrm{Ell}(\mathcal{O})$ is the elliptic part of $h(\mathcal{O})$, which is expressed as follows:

$$\mathrm{Ell}(\mathcal{O}) = \frac{1}{2} \sum_{w(B)>1} h(B)(1 - w(B)^{-1}) \prod_{\mathfrak{p}} m_{\mathfrak{p}}(B). \tag{1.2}$$

In the summation B runs through all (non-isomorphic) quadratic O_F-orders such that the field K of fractions can be embedded into D and the index $w(B) := [B^\times : O_F^\times] > 1$. The symbol $h(B)$ denotes the class number of B, and for any finite prime $\mathfrak{p}$ of F, $m_{\mathfrak{p}}(B)$ is the number of equivalence classes of optimal embeddings of $B_{\mathfrak{p}} := B \otimes_{O_F} O_{F_{\mathfrak{p}}}$ into $\mathcal{O}_{\mathfrak{p}} := \mathcal{O} \otimes_{O_F} O_{F_{\mathfrak{p}}}$. We refer to Eichler [4], Vigneras [14, Chapter V, Corollary 2.5, p. 144] and Körner [7, Theorem 2]) for more details.

One can use the mass formula (cf. [14, Chapter V, Corollary 2.3] and [16, Section 5]) to compute $\mathrm{Mass}(\mathcal{O})$. When the order $\mathcal{O}$ is not too complicated, for example if $\mathcal{O}$ is

Received June 18, 2015; Accepted February 2, 2016.
Communicated by Yi-Fan Yang.
2010 *Mathematics Subject Classification.* 11R52, 11G10.
Key words and phrases. Class number formula, Arithmetic of quaternion algebras.
*Corresponding author.

an Eichler order, the computation of numbers of local optimal embeddings is known by Eichler (cf. [14, p. 94]) and Hijikata [6, Theorem 2.3, p. 66]. Also see Pizer [12, Sections 3–5] for some extensions. A major difficulty in adapting Eichler's class number formula is to find all the quadratic O_F-orders B with the properties stated below (1.2). It is not hard to see that the fraction field K of B must be totally imaginary over F and the information whether K can be embedded into D is already contained in local optimal embeddings.

In this paper we classify all totally imaginary quadratic O_F-orders B with $w(B) > 1$ in the case where $F = \mathbb{Q}(\sqrt{p})$ is a real quadratic field with a prime number p. We also compute the class number $h(B)$ and the index $w(B)$ of them. As a consequence of our computations we obtain a formula for $h(\mathcal{O})$ for any Eichler order $\mathcal{O}$ of square-free level in an arbitrary totally definite quaternion algebra over $\mathbb{Q}(\sqrt{p})$ (see Section 3.8).

Our motivation of computing the class number of quaternion orders comes from the study of supersingular abelian surfaces over finite fields. We are interested in finding an explicit formula for the number $H(p)$ of isomorphism classes of (necessarily superspecial) abelian surfaces in the isogeny class over the prime field $\mathbb{F}_p$ corresponding to the Weil p-number $\sqrt{p}$. The endomorphism algebras of these abelian varieties are isomorphic to the totally definite quaternion algebra D_{∞_1,∞_2} over $F = \mathbb{Q}(\sqrt{p})$ which is ramified only at the two real places. When $p = 2$ or $p \equiv 3 \pmod 4$, the number $H(p)$ is equal to the class number $h(\mathbb{O}_1)$ of a maximal order $\mathbb{O}_1$ in D_{∞_1,∞_2}. When $p \equiv 1 \pmod 4$, we show that $H(p) = h(\mathbb{O}_1)+h(\mathbb{O}_8)+h(\mathbb{O}_{16})$, where $\mathbb{O}_8$ and $\mathbb{O}_{16}$ are certain proper $A = \mathbb{Z}[\sqrt{p}]$-suborders of $\mathbb{O}_1$ of index 8 and 16, respectively. (We say $\mathcal{O}$ is a "proper" A-order if $\mathcal{O} \cap F = A$.) For the non-maximal cases the generalized class number formula [16, Theorem 1.5] requires to find all totally imaginary proper quadratic A-orders B with $w(B) := [B^\times : A^\times] > 1$ and compute the numerical invariants $h(B)$ and $w(B)$ again. These technical issues are dealt within this paper. The results of this paper will be used in [16] to compute the number $H(p)$ of superspecial abelian surfaces. See [16, Theorem 1.2] for the final formula for $H(p)$.

The paper is organized as follows. Section 2 classifies all totally imaginary quadratic fields K over $F = \mathbb{Q}(\sqrt{p})$ with $w_K := [O_K^\times : O_F^\times] > 1$. We express the class numbers $h(K)$ of these fields K in terms of $h(F)$ and compute w_K. Section 3 classifies all O_F-orders B in K with $w(B) > 1$. We also compute the numerical invariants $h(B)$ and $w(B)$ of these orders. Section 4 classifies all proper A-orders B in K with $w(B) > 1$ when $p \equiv 1 \pmod 4$. We compute the same numerical invariants of them and the numbers of related local optimal embeddings mentioned above.

2. 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 $O_{\mathbb{Q}(\sqrt{p})}^\times$. 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. [11, Theorem I.7.4]).

2.1. 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, called the Hasse unit index,

$$Q_{K/F} := [O_K^\times/\boldsymbol{\mu}_K : O_F^\times/\boldsymbol{\mu}_F] = [O_K^\times : \boldsymbol{\mu}_K O_F^\times]. \tag{2.1}$$

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 $\iota\colon x \mapsto \iota(x)$ be the unique nontrivial element of $\mathrm{Gal}(K/F)$. By [15, 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 $\boldsymbol{\mu}_K^2 = \phi_K(\boldsymbol{\mu}_K)$:

$$\phi_K\colon O_K^\times \to \boldsymbol{\mu}_K, \qquad u \mapsto u/\iota(u). \tag{2.2}$$

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

$$z = \iota(z)\zeta_{2n}. \tag{2.3}$$

We note that (2.2) also implies that

$$u^2 \equiv \mathrm{N}_{K/F}(u) \pmod{\boldsymbol{\mu}_K}, \quad \forall\, u \in O_K^\times. \tag{2.4}$$

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

$$O_K^\times/O_F^\times \cong \boldsymbol{\mu}_K/\boldsymbol{\mu}_F = \boldsymbol{\mu}_K/\left\{\pm 1\right\}, \tag{2.5}$$

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

$$1 \to (\boldsymbol{\mu}_K O_F^\times)/O_F^\times \to O_K^\times/O_F^\times \to \boldsymbol{\mu}_K/\boldsymbol{\mu}_K^2 \to 1. \tag{2.6}$$

Let $z \in O_K^\times$ be an element satisfying (2.3). Then

$$z^2 = \mathrm{N}_{K/F}(z)\zeta_{2n}, \tag{2.7}$$

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 $w_K := \left|O_K^\times/O_F^\times\right|$ is given by

$$w_K = \frac{1}{2}\,|\boldsymbol{\mu}_K| \cdot Q_{K/F} = \begin{cases} \frac{1}{2}\,|\boldsymbol{\mu}_K| & \text{if } Q_{K/F} = 1, \\ |\boldsymbol{\mu}_K| & \text{if } Q_{K/F} = 2. \end{cases} \tag{2.8}$$

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

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

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 2.2. *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*

$$z^2 = \epsilon\,\zeta_{2n} \tag{2.9}$$

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 (2.4), $O_F^\times/\boldsymbol{\mu}_F$ 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 (2.6), 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 (2.9). □

2.3. Since $[K:\mathbb{Q}] = 4$, we have $\varphi(2n) \leq 4$. 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 2.4. *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 [3, 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 2.5. *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. [10, Lemma 3, p. 91] or [17, 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 2.6. *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 2.5, $K = \mathbb{Q}(\sqrt{p}, \sqrt{-2})$. 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 $\mathfrak{d}_K = 4p \cdot (-8) \cdot (-8p) = 2^8 p^2$ by Exercise 42(f) of [9, Chapter 2]. On the other hand,

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

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 2.7. *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 Lemmas 2.2 and 2.4, $Q_{K/F} = 1$ 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 2.2 and Proposition 2.5, we see that $Q_{K/F} = 2$ if and only if the equation

$$y^2 = 2\zeta_{2n} \tag{2.10}$$

has a solution in K. By Section 2.3, 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, (2.10) 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 $Q_{K/F} = 2$. $\square$

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 [2, Section 2].

2.8. 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. [15, Theorem 11.1])

$$h(\mathbb{Q}(\zeta_8)) = h(\mathbb{Q}(\zeta_{10})) = h(\mathbb{Q}(\zeta_{12})) = 1. \tag{2.11}$$

Using Magma [1], one easily calculates that

$$h(\mathbb{Q}(\sqrt{2}, \sqrt{-3})) = h(\mathbb{Q}(\sqrt{5}, \sqrt{-1})) = h(\mathbb{Q}(\sqrt{5}, \sqrt{-3})) = 1, \tag{2.12}$$

$$h(\mathbb{Q}(\sqrt{3}, \sqrt{-2})) = 2. \tag{2.13}$$

2.9. 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 2.7 shows the following simple but mysterious criterion:

$$Q_{K_j/F} = 1 \iff \gcd(\mathfrak{d}_F, \mathfrak{d}_{E_j}) = 1. \tag{2.14}$$

2.10. 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 [5], if $K \neq \mathbb{Q}(\sqrt{2}, \sqrt{-1})$, then

$$h(K) = Q_{K/F} h(F) h(E) h(E')/2, \tag{2.15}$$

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

$$h(K_j) = \begin{cases} h(F)h(\Bbbk_j) & \text{if } j = 1, 2 \text{ and } p \equiv 3 \pmod 4, \\ h(F)h(\Bbbk_j)/2 & \text{otherwise.} \end{cases} \tag{2.16}$$

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 2.7.

2.11. 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

$$\left\{1, \ \frac{1 + \sqrt{p^*}}{2}, \ \sqrt{-1}, \ \frac{\sqrt{-1} + \sqrt{-p^*}}{2}\right\}. \tag{2.17}$$

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

$$O_K/2O_K \cong (O_L/2O_L)[t]/(t^2 + 1) = (O_L/2O_L)[t]/((t + 1)^2), \tag{2.18}$$

with the isomorphism sending $\sqrt{-1} \mapsto \bar{t}$, which denotes the image of t in the quotient. The isomorphism (2.18) gives rise to an exact sequence

$$0 \to (O_L/2O_L) \to (O_K/2O_K)^\times \to (O_L/2O_L)^\times \to 1. \tag{2.19}$$

Note that 2 is unramified in L, and

$$O_L/2O_L \cong \begin{cases} \mathbb{F}_2 \oplus \mathbb{F}_2 & \text{if } \left(\frac{2}{p}\right) = 1, \\ \mathbb{F}_4 & \text{if } \left(\frac{2}{p}\right) = -1. \end{cases} \tag{2.20}$$

Hence the exact sequence (2.19) splits. More precisely,

$$(O_K/2O_K)^\times \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } \left(\frac{2}{p}\right) = 1, \\ (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } \left(\frac{2}{p}\right) = -1. \end{cases} \tag{2.21}$$

2.12. 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

$$O_K/2O_K \supset B_{1,4}/2O_K \cong (\mathbb{Z}[\sqrt{p^*}]/2O_L)[t]/((t+1)^2) \cong \mathbb{F}_2[t]/((t+1)^2) \tag{2.22}$$

under the isomorphism (2.18). 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

$$\mathbb{F}_2[t]/((t+1)^2) \subset (O_L/2O_L)[t]/((t+1)^2) = (O_L/2O_L) \oplus (O_L/2O_L)(1+\bar{t}) \tag{2.23}$$

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

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

3. O_F-orders in K

We keep the notations of Section 2. 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 2.8.

Proposition 3.1. *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 2.8, 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 2.6 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 2.9, 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 [8, 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 3.2. *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 2.5, 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 3.3. *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:*

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

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 3.2. By Section 2.12, $B_{1,2}$ 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 3.2. 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

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

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 $w(B) > 1$.

3.4. 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 [11, Theorem I.12.12]

$$h(B) = \frac{h(O_K)[(O_K/\mathfrak{f})^\times : (B/\mathfrak{f})^\times]}{[O_K^\times : B^\times]}. \tag{3.1}$$

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,

$$h(B) = \frac{h(O_K)[(O_K/\mathfrak{a})^\times : (B/\mathfrak{a})^\times]}{[O_K^\times : B^\times]}. \tag{3.2}$$

Lemma 3.5. *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 3.3. We have*

$$h(B_{1,2}) = h(B_{1,4}) = \left(2 - \left(\frac{2}{p}\right)\right) h(O_K) \tag{3.3}$$

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 2.12, we have $O_K \supset B_{1,2} \supset B_{1,4} \supset 2O_K$. So take $\mathfrak{a} = 2O_K$ in (3.2). It has been shown in Sections 2.11 and 2.12 that

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

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 3.3, where it has been shown that $w(B_{1,2}) = 4$ and $w(B_{1,4}) = 2$. $\square$

3.6. 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 [9, Chapter 2], a $\mathbb{Z}$-basis of O_K is given by $\{1, \sqrt{-1}, \sqrt{2}, (\sqrt{2} + \sqrt{-2})/2\}$. 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

$$w(O_K) = 4 \quad \text{and} \quad w(B) = 2. \tag{3.4}$$

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 $h(B) = h(O_K) = 1$.

3.7. 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, $h(B_{1,3}) = h(O_K) = 1$.

3.8. Let D be a totally definite quaternion algebra over $F = \mathbb{Q}(\sqrt{p})$ of discriminant ideal $\mathcal{D} \subset O_F$, and $\mathcal{O}$ an Eichler order of level $\mathcal{N}$, where $\mathcal{N} \subset O_F$ is a square-free prime-to-$\mathcal{D}$ ideal. The mass formula [14, Chapter V, Corollary 2.3] states that

$$\mathrm{Mass}(\mathcal{O}) = \frac{1}{2}\zeta_F(-1)h(F)\prod_{\mathfrak{p}|\mathcal{D}}(N(\mathfrak{p}) - 1)\prod_{\mathfrak{p}|\mathcal{N}}(N(\mathfrak{p}) + 1) =: M, \tag{3.5}$$

where $\zeta_F(s)$ is the Dedekind zeta function of F. For any O_F-order B in a quadratic extension K/F, we define the Artin symbol

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

and the Eichler symbol

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

where $\mathfrak{f}(B) \subseteq O_F$ is the conductor of B. Define

$$
\begin{aligned}
E_{K,\mathcal{D},\mathcal{N}} &:= \prod_{\mathfrak{p}|\mathcal{D}} \left(1 - \left(\frac{K}{\mathfrak{p}}\right)\right) \prod_{\mathfrak{p}|\mathcal{N}} \left(1 + \left(\frac{K}{\mathfrak{p}}\right)\right), \\
E_{B,\mathcal{D},\mathcal{N}} &:= \prod_{\mathfrak{p}|\mathcal{D}} \left(1 - \left(\frac{B}{\mathfrak{p}}\right)\right) \prod_{\mathfrak{p}|\mathcal{N}} \left(1 + \left(\frac{B}{\mathfrak{p}}\right)\right).
\end{aligned} \tag{3.6}
$$

By the formula [14, p. 94], one has

$$\prod_{\mathfrak{p}} m_{\mathfrak{p}}(B) = E_{B,\mathcal{D},\mathcal{N}}.$$

For an ideal $\mathfrak{a} \subset O_F$ and a square-free integer n, we can write $\mathfrak{a} = \mathfrak{a}_{(n)}\mathfrak{a}^{(n)}$ as the product of an n-primary ideal $\mathfrak{a}_{(n)}$ and a prime-to-n ideal $\mathfrak{a}^{(n)}$. For any two O_F-ideals $\mathfrak{a}, \mathfrak{b}$, we set

$$C_{\mathfrak{a},\mathfrak{b}} := \delta_{\mathfrak{a},(1)} 2^s,$$

where $\delta_{\mathfrak{a},(1)}$ is the usual delta function and s is the number of prime ideals $\mathfrak{p}$ dividing $\mathfrak{b}$. If there is a unique prime ideal $\mathfrak{p}_2$ of O_F lying over 2 and the conductor $\mathfrak{f}(B)$ is $\mathfrak{p}_2$-primary, then

$$E_{B,\mathcal{D},\mathcal{N}} = E_{B,\mathcal{D}_{(2)},\mathcal{N}_{(2)}} \cdot E_{B,\mathcal{D}^{(2)},\mathcal{N}^{(2)}} = C_{\mathcal{D}_{(2)},\mathcal{N}_{(2)}} \cdot E_{K,\mathcal{D}^{(2)},\mathcal{N}^{(2)}}. \tag{3.7}$$

We now have everything to compute the class number $h(\mathcal{O})$. Recall that $K_j = \mathbb{Q}(\sqrt{p}, \sqrt{-j})$ for $j \in \{1,2,3\}$. By Section 2.8 and Proposition 3.1, if $p \equiv 1 \pmod 4$ and $p > 5$, then the only orders with nonzero contributions to the elliptic part $\mathrm{Ell}(\mathcal{O})$ are O_{K_1} and O_{K_3}, with $w(O_{K_1}) = 2$ and $w(O_{K_3}) = 3$ respectively. We have

$$h(\mathcal{O}) = M + \frac{1}{4} h(K_1) E_{K_1,\mathcal{D},\mathcal{N}} + \frac{1}{3} h(K_3) E_{K_3,\mathcal{D},\mathcal{N}} \tag{3.8}$$

for $p \equiv 1 \pmod 4$ and $p > 5$. On the other hand, for $p \equiv 3 \pmod 4$ and $p > 5$, we have calculated the following numerical invariants of all orders B with $w(B) > 1$ (see Section 2.8, Propositions 3.1 and 3.3 and Lemma 3.5):

$p \equiv 3 \pmod 4$	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, by Eichler's class number formula we obtain

$$
\begin{aligned}
h(\mathcal{O}) = M &+ \frac{5}{8} \left(2 - \left(\frac{2}{p}\right)\right) h(K_1) C_{\mathcal{D}_{(2)},\mathcal{N}_{(2)}} E_{K_1,\mathcal{D}^{(2)},\mathcal{N}^{(2)}} \\
&+ \frac{3}{8} h(K_1) E_{K_1,\mathcal{D},\mathcal{N}} + \frac{1}{4} h(K_2) E_{K_2,\mathcal{D},\mathcal{N}} + \frac{1}{3} h(K_3) E_{K_3,\mathcal{D},\mathcal{N}}
\end{aligned} \tag{3.9}
$$

for $p \equiv 3 \pmod 4$ and $p > 5$. For $p = 2, 3, 5$, the formulas for $h(\mathcal{O})$ can be obtained in the same way using Sections 2.8, 3.6 and 3.7.

4. 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 4.1. *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 $u \in A \cap O_F^\times = A^\times$. □

4.2. If $p \equiv 5 \pmod 8$, 2 is inert in O_F, and we have $(O_F/2O_F)^\times \cong \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$. 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, $O_F^\times/A^\times \cong \mathbb{Z}/3\mathbb{Z}$, 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 [13]. For any $p \equiv 1 \pmod 4$, we define

$$\varpi := [O_F^\times : A^\times] \in \{1, 3\}. \tag{4.1}$$

By Lemma 4.1, $\varpi = 1$ if $p \equiv 1 \pmod 8$.

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

$$A_+^\times = (A^\times)^2. \tag{4.2}$$

If $\epsilon \in A$, then $A^\times = O_F^\times = \langle \epsilon \rangle \times \{\pm 1\}$. Since ϵ is not totally positive by Lemma 2.4, 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 4.2. It follows that $A_+^\times = \langle \epsilon^6 \rangle = (A^\times)^2$. So either way, (4.2) holds.

Lemma 4.4. *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*

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

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

Proof. By Section 2.3, 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 4.2, $O_F^\times / A^\times \cong \mathbb{Z}/3\mathbb{Z}$. Assume $K = \mathbb{Q}(\zeta_{10})$, then

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

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 the assumption that B is a proper A-order. On the other hand, if $B^\times / A^\times \supseteq \langle \bar{\zeta}_{10} \rangle \cong \mathbb{Z}/5\mathbb{Z}$, 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 $\phi_K \colon u \mapsto u/\iota(u)$ is the map given in (2.2). Clearly, $\phi_K(B^\times) \neq \{1\}$. Otherwise, $B^\times \subseteq O_F^\times \cap B = A^\times$, contradicting 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 (4.2), 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 2.1, $\phi_K(O_K^\times) = \boldsymbol{\mu}_K^2 = \{\pm 1\}$ 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 2.3, we must have $K = K_3 = F(\sqrt{-3})$ since all other possibilities have been exhausted. □

4.5. Suppose that $K = K_1$. It has been shown in Lemma 4.4 that $B \supseteq B_{1,4} = \mathbb{Z}[\sqrt{p}, \sqrt{-1}]$. By Section 2.12,

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

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 3.5. 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,

$$w(B_{1,2}) = w(B_{1,4}) = 2. \tag{4.3}$$

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

$$h(B_{1,2}) = \frac{1}{\varpi}\left(2 - \left(\frac{2}{p}\right)\right) h(O_{K_1}) \quad \text{and} \quad h(B_{1,4}) = \frac{2}{\varpi}\left(2 - \left(\frac{2}{p}\right)\right) h(O_{K_1}). \tag{4.4}$$

4.6. Suppose that $K = K_3$. By Exercise 42 of [9, Chapter 2], a $\mathbb{Z}$-basis of $\mathcal{O}_{K_3}$ is

$$\left\{1,\ \omega_p = \frac{1+\sqrt{p}}{2},\ \zeta_6 = \frac{1+\sqrt{-3}}{2},\ \omega_p\zeta_6 = \frac{(1+\sqrt{p})(1+\sqrt{-3})}{4}\right\}. \tag{4.5}$$

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 $O_K/\mathfrak{p}_1 \cong O_K/\mathfrak{p}_2 \cong \mathbb{F}_4$. Therefore, $O_L/2O_L \cong \mathbb{F}_4$ embeds diagonally[1] into

$$O_K/2O_K \cong (O_K/\mathfrak{p}_1) \times (O_K/\mathfrak{p}_2) \cong \mathbb{F}_4 \times \mathbb{F}_4. \tag{4.6}$$

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 (3.2) with $\mathfrak{a} = 2O_K$. It has already been shown that $(B_{3,4}/2O_K)^\times \cong \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$, and

$$(O_K/2O_K)^\times \cong (O_K/\mathfrak{p}_1)^\times \times (O_K/\mathfrak{p}_2)^\times \cong (\mathbb{Z}/3\mathbb{Z})^2. \tag{4.7}$$

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

$$w(B_{3,4}) = 3, \quad h(B_{3,4}) = \frac{3h(O_{K_3})}{\varpi} = \begin{cases} 3h(O_{K_3}) & \text{if } \epsilon \in A, \\ h(O_{K_3}) & \text{if } \epsilon \notin A. \end{cases} \tag{4.8}$$

4.7. 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 4.1. For any quadratic proper A-order B with $w(B) > 1$, we have

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

[1]Since the isomorphisms $O_K/\mathfrak{p}_i \cong \mathbb{F}_4$ is *not* canonical, the diagonal of $(O_K/\mathfrak{p}_1) \times (O_K/\mathfrak{p}_2)$ depends on the choice of $(O_K/\mathfrak{p}_1) \cong (O_K/\mathfrak{p}_2)$. Here both of them are identified naturally with $O_L/2O_L$. In Section 4.8, we have a different diagonal. However, whichever diagonal we choose, the prime field $A/2O_F \cong \mathbb{F}_2$ embeds canonically in it.

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.

4.8. 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

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

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

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

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 an 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 (4.5). 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,

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

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 $O_F/2O_F \cong \mathbb{F}_4$, 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

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

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,

$$w(B_{3,2}) = w(B'_{3,2}) = 3. \tag{4.9}$$

Using (3.2), one sees that

$$h(B_{3,2}) = h(B'_{3,2}) = h(O_{K_3}). \tag{4.10}$$

Acknowledgments

The authors thank Markus Kirschmer and Yifan Yang for very helpful discussions. The revision of the present manuscript is made during CF Yu's stay at the Max-Planck-Institut für Mathematik. He is grateful to the Institute for kind hospitality and excellent working conditions. The authors also thank the referee for his/her careful reading and helpful comments. J. Xue was partially supported by the grant NSC 102-2811-M-001-090. TC Yang and CF Yu are partially supported by the grants MoST 100-2628-M-001-006-MY4, 103-2811-M-001-142 and 103-2918-I-001-009.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. `http://dx.doi.org/10.1006/jsco.1996.0125`

[2] D. A. Buell, H. C. Williams and K. S. Williams, *On the imaginary bicyclic biquadratic fields with class-number* 2, Math. Comp. **31** (1977), no. 140, 1034–1042. `http://dx.doi.org/10.1090/s0025-5718-1977-0441914-1`

[3] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Series in Pure Mathematics **8**, World Scientific, Singapore, 1988. `http://dx.doi.org/10.1142/0663`

[4] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151. `http://dx.doi.org/10.1515/crll.1955.195.127`

[5] G. Herglotz, *Über einen Dirichletschen Satz*, Math. Z. **12** (1922), no. 1, 255–261. `http://dx.doi.org/10.1007/bf01482079`

[6] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), 56–82. `http://dx.doi.org/10.2969/jmsj/02610056`

[7] O. Körner, *Traces of Eichler-Brandt matrices and type numbers of quaternion orders*, Proc. Indian Acad. Sci. Math. Sci. **97** (1987), no. 1-3, 189–199. `http://dx.doi.org/10.1007/bf02837823`

[8] S. Lang, *Algebraic Number Theory*, Second edition, Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1994. `http://dx.doi.org/10.1007/978-1-4612-0853-2`

[9] D. A. Marcus, *Number Fields*, Universitext, Springer-Verlag, New York, 1977. `http://dx.doi.org/10.1007/978-1-4684-9356-6`

[10] T. M. McCall, C. J. Parry and R. Ranalli, *Imaginary bicyclic biquadratic fields with cyclic 2-class group*, J. Number Theory **53** (1995), no. 1, 88–99.
http://dx.doi.org/10.1006/jnth.1995.1079

[11] J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaten [Fundamental Principles of Mathematical Sciences], **322**, Springer-Verlag, Berlin, 1999. http://dx.doi.org/10.1007/978-3-662-03983-0

[12] A. Pizer, *On the arithmetic of quaternion algebras II*, J. Math. Soc. Japan **28** (1976), no. 4, 676–688. http://dx.doi.org/10.2969/jmsj/02840676

[13] W. Roonguthai, *The On-Line Encyclopedia of Integer Sequences*, Published electronically at (Primes $p \equiv 5 \pmod 8$ such that the Diophantine equation $x^2 - py^2 = -4$ has no solution in odd integers x, y.)

[14] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, [Arithmetic of quaternion algebras] Lecture Notes in Mathematics **800**, Springer, Berlin, 1980.
http://dx.doi.org/10.1007/bfb0091027

[15] L. C. Washington, *Introduction to Cyclotomic Fields*, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.
http://dx.doi.org/10.1007/978-1-4612-1934-7

[16] J. Xue, T.-C. Yang, and C.-F. Yu, *Supersingular abelian surfaces and Eichler's class number formula*, arXiv:1404.2978v3.

[17] Z. Zhang and Q. Yue, *Fundamental units of real quadratic fields of odd class number*, J. Number Theory **137** (2014), 122–129.
http://dx.doi.org/10.1016/j.jnt.2013.10.019

Jiangwei 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

Tse-Chung 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

Chia-Fu Yu
Institute of Mathematics, Academia Sinica and NCTS, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan
and
The Max-Planck-Institut für Mathematik, Vivatsgasse 7, Bonn, Germany 53111
E-mail address: chiafu@math.sinica.edu.tw, chiafu@mpim-bonn.mpg.de