National Center for Theoretical Sciences

NCTS/Math Technical Report
2018-008

On Superspecial Abelian Surfaces over Finite Fields II

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

ON SUPERSPECIAL ABELIAN SURFACES OVER FINITE FIELDS II

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

Abstract. In [21, Doc. Math. **21**, 2016] the current authors calculated explicitly the number of isomorphism classes of superspecial abelian surfaces over any finite field of *odd* degree over the prime field $\mathbb{F}_p$. The method reduces the calculation to the prime field case, and calculates the number of isomorphism classes in each isogeny class through a lattice description. In the present paper we treat the *even* degree cases. This complements our earlier results and completes the explicit calculation of superspecial abelian surfaces. Our method reduces the calculation to a seemingly unrelated problem on conjugacy classes of finite order in arithmetic subgroups, which may be of interest in its own right.

1. Introduction

Throughout this paper, p denotes a prime number and q is a power of p. An abelian variety over a field k of characteristic p is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over an algebraic closure $\bar{k}$ of k; it is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over $\bar{k}$. As any supersingular abelian variety is isogenous to a superspecial abelian variety, it is common to study supersingular abelian varieties through investigating the superspecial abelian varieties.

Our goal is to calculate explicitly the number of superspecial abelian surfaces over any finite field. This is motivated by the search for natural generalizations of known explicit results of elliptic curves over finite fields to abelian surfaces, especially from supersingular elliptic curves to supersingular abelian surfaces. Thus, studying superspecial abelian surfaces becomes a vital step for this purpose.

In [21] we calculated explicitly the number of superspecial abelian surfaces over any finite field $\mathbb{F}_q$ of *odd* degree over $\mathbb{F}_p$. This extended our earlier works [19, 20] and [23] contributed to the study of superspecial abelian varieties over finite fields. In this paper we treat the even degree case. Thus, this complements the results in loc. cit. and completes the explicit calculation of superspecial abelian surfaces over any finite field.

A key step in [21] is the reduction to the case where the ground field is a prime finite field. This step is achieved by a Galois cohomology argument. Then we calculate case-by-case the number of superspecial abelian surfaces in each isogeny class over $\mathbb{F}_p$. This approach works fine when the field $\mathbb{F}_q$ of odd degree because we have an explicit lattice description for abelian varieties over $\mathbb{F}_p$. When the degree $[\mathbb{F}_q : \mathbb{F}_p]$ is even, the Galois cohomology argument unfortunately yields no immediate simplification. However, it leads us to a seemingly unrelated problem, which is

Date: January 30, 2018.

2010 *Mathematics Subject Classification.* 11R52, 11G10.

important but is equally challenging, on counting conjugacy classes of elements of finite order in arithmetic subgroups. The connection itself is quite straight forward, though it is applicable to a quite general setting; see Proposition 1.1.

For any group G, we denote by $\mathrm{Cl}\, G$ the set of conjugacy classes of G and $\mathrm{Cl}_0\, G \subset \mathrm{Cl}\, G$ the subset of classes of elements of finite order. Let $D = D_{p,\infty}$ be the definite quaternion $\mathbb{Q}$-algebra ramified exactly at p and ∞, and $\mathcal{O}$ a maximal order in D.

Proposition 1.1. *Let $\mathbb{F}_q$ be any finite field containing $\mathbb{F}_{p^2}$ and d any integer strictly greater than 1. Then the set of $\mathbb{F}_q$-isomorphism classes of d-dimensional superspecial abelian varieties over $\mathbb{F}_q$ is in bijection with the set $\mathrm{Cl}_0\, G$ with $G = \mathrm{GL}_d(\mathcal{O})$.*

By a classical result of Eichler [3], if $d > 1$, then the class number of $M_d(\mathcal{O})$ is equal to one. Thus, for $d \ge 2$, any maximal arithmetic subgroup in $\mathrm{GL}_d(D)$ is conjugate to $\mathrm{GL}_d(\mathcal{O})$ by an element in $\mathrm{GL}_d(D)$ and Proposition 1.1 does not depend on the choice of the maximal order $\mathcal{O}$. The main result of this paper is the following (see Theorem 3.2 our precise formula), which calculates the number of superspecial abelian surfaces over $\mathbb{F}_q \supset \mathbb{F}_{p^2}$ by mean of Proposition 1.1.

Theorem 1.2. *There is an explicit formula for the cardinality of $\mathrm{Cl}_0\, \mathrm{GL}_2(\mathcal{O})$.*

The strategy of the calculation and detailed formulas are described in Section 3. The calculation involves class numbers of certain (possibly non-maximal) orders in the subalgebras of $\mathrm{Mat}_2(D)$ which are the centralizers of elements of finite order. The expression looks familiar with the geometric side of a trace formula but we have no idea for this aspect.

This paper is organized as follows. In Section 2, we provide a rather preliminary account on conjugacy classes of finite orders of groups due to the author's limited knowledge. A proof of Proposition 1.1 is given in this section. Section 3 describes the main results of this paper. The remainder of this paper is to fill the details of the computation in Theorem 1.2.

2. Conjugacy classes of elements of finite order

In this section we provide a preliminary account of conjugacy classes of elements of finite orders of groups.

2.1. **Preliminaries.** For any group G, we denote by $\mathrm{Cl}\, G$ the set of conjugacy classes of G and $\mathrm{Cl}_0\, G \subset \mathrm{Cl}\, G$ the subset of classes of elements of finite order in G. It is a basic question to ask whether $\mathrm{Cl}_0\, G$ is finite, how to calculate its cardinality if it is finite, or whether there are any connections of $\mathrm{Cl}_0\, G$ with other objects of interest. If G is finite, then $\mathrm{Cl}_0\, G = \mathrm{Cl}\, G$ is finite and the cardinality is equal to the number of mutually non-isomorphic complex irreducible representations of G, which are necessarily finite-dimensional.

In general, $\mathrm{Cl}_0\, G$ may not be finite. For example, if G is an abelian group, then $\mathrm{Cl}_0\, G = G_{\mathrm{tors}}$ is the torsion subgroup which can certainly be infinite. In the special case $G = \mathbb{C}^\times$, G_{tors} is the subgroup of all roots of unity, which has rich arithmetic properties. On the other hand, suppose G is a connected compact Lie group. Choose a maximal torus T of G. Since any element of G is contained in a maximal torus and any two maximal tori are conjugate under G, the set $\mathrm{Cl}\, G$ then is in bijection with the quotient T/W, where W is the Weyl group of G relative to T, and we have $\mathrm{Cl}_0\, G \simeq T_{\mathrm{tors}}/W$. Suppose $G = \mathrm{GL}_n(F)$, where F is any field, then $\mathrm{Cl}\, G$ can be parametrized explicitly by rational Jordan canonical forms.

Another interesting type of groups to consider are those of the form $G(F)$ for a reductive algebraic group G over a global field F and their arithmetic subgroups, or of the form $G(F)$ for a local field F and their compact subgroups. When $F = \mathbb{R}$ and G is semisimple, Friedmann and Stanley [5] obtain explicit formulas for the conjugacy classes of fixed finite order in $G(\mathbb{R})$. Below is a finitenss result of $\mathrm{Cl}_0(G(F))$ for an non-archimedean local field F of characteristic zero.

Lemma 2.1. *Let G be a connected reductive group over an non-archimedean local field F of characteristic zero. Then $\mathrm{Cl}_0\, G(F)$ is finite.*

Proof. Since $\mathrm{char}\, F = 0$, every element in $G(F)$ of finite order is semisimple and hence it is contained in a maximal F-torus T of G. Note that there are only finitely many maximal F-tori up to conjugation by $G(F)$. Therefore, one reduces to the case where $G = T$ is a torus. Choose a finite extension K of F over which T splits. One has $T(F) \subset (K^\times)^d$, where $d = \dim T$. Since there are only finitely many roots of unity in $K^\times$, the subgroup $T(F)_{\mathrm{tors}}$ is finite. □

The following is a well-known result due to Borel and Harish-Chandra [1].

Theorem 2.2. *Let G be a reductive group over a number field F, and $\Gamma \subset G(F)$ an S-arithmetic subgroup, where S is a finite set of places of F containing all archimedean ones. Then there are only finitely many finite subgroups of Γ up to conjugation by Γ. In particular, $\mathrm{Cl}_0\, \Gamma$ is finite.*

Proposition 2.3. *Let A be a finite-dimensional semisimple algebra over a number field F. Then $\mathrm{Cl}_0(A^\times)$ is finite.*

Proof. For each positive integer n, denote by $\mathrm{Hom}_F(F[t]/(t^n-1), A)$ the set of F-algebra homomorphisms from $F[t]/(t^n-1)$ to A, and $\mathrm{Hom}^*_F(F[t]/(t^n-1), A)$ the subset consisting of maps φ with $\mathrm{ord}(\varphi(t)) = n$. The group $A^\times$ acts on $\mathrm{Hom}_F(F[t]/(t^n-1), A)$ by conjugation, and we have orbit spaces

$$\mathrm{Hom}^*_F(F[t]/(t^n-1), A)/A^\times \subset \mathrm{Hom}_F(F[t]/(t^n-1), A)/A^\times.$$

Let $\mathrm{Cl}_0(n, A^\times)$ denote the set of conjugacy classes of elements of order n in $A^\times$. Clearly this set agrees with the set $\mathrm{Hom}^*_F(F[t]/(t^n-1), A)/A^\times$.

Since A is separable, by the generalized Neother-Skolem theorem due to Pop and Pop [12], the set $\mathrm{Hom}_F(F[t]/(t^n-1), A)/A^\times$ is finite. Thus, $\mathrm{Cl}_0(n, A^\times)$ is finite for each n. Since $\mathrm{Cl}_0(A^\times)$ is a union of $\mathrm{Cl}_0(n, A^\times)$ and $\mathrm{Cl}_0(n, A^\times)$ is empty for almost all n, we prove the finiteness of $\mathrm{Cl}_0(A^\times)$. □

Now we provide an example showing that $\mathrm{Cl}_0\, G(F)$ can be infinite for a connected reductive group G over a number field F. Take $G = \mathrm{SL}_2$ and $F = \mathbb{Q}$. Consider the subset $\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q})) \subset \mathrm{Cl}_0(\mathrm{SL}_2(\mathbb{Q}))$ of classes of order 4. We choose a base point $\xi_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and set $K := \mathbb{Q}(\xi_0)$, which is isomorphic to $\mathbb{Q}(\sqrt{-1}\,)$. Since every element $\xi \in \mathrm{SL}_2(\mathbb{Q})$ of order 4 is conjugate to ξ_0 by an element g_1 in $\mathrm{GL}_2(\mathbb{Q})$, i.e. $\xi = g_1 \xi_0 g_1^{-1}$. Two elements g_1 and g_2 in $\mathrm{GL}_2(\mathbb{Q})$ give rise to the same element ξ if and only if $g_2 = g_1 z$ for some element $z \in K^\times$. Moreover, suppose ξ_1 and ξ_2 are two elements in $\mathrm{SL}_2(\mathbb{Q})$ of order 4 presented by g_1 and g_2, respectively. Then ξ_1 and

ξ_2 are conjugate in $\mathrm{SL}_2(\mathbb{Q})$ if and only if $g_2 = hg_1z$ for some elements $h \in \mathrm{SL}_2(\mathbb{Q})$ and $z \in K^\times$. Therefore, we have proved a bijection

$$\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q})) \simeq \mathrm{SL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{Q})/K^\times. \tag{2.1}$$

Taking the determinant, we have $\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q})) \simeq \mathbb{Q}^\times/\,\mathrm{N}_{K/\mathbb{Q}}(K^\times)$. Note that $\mathrm{N}_{K/\mathbb{Q}}(K^\times)$ consists of non-zero elements of the form a^2+b^2 with $a, b \in \mathbb{Q}$. By basic number theory, we obtain the following result.

Proposition 2.4. *The set* $\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q}))$ *is in bijection with the* $\mathbb{F}_2$*-vector space generated by* -1 *and prime elements* p *with* $p \equiv 3 \pmod 4$. *In particular,* $\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q}))$ *is an infinite set.*

Remark 2.5. Another way to interpret the previous example is through the point of view of *stable conjugacy classes*. Let G be a connected reductive group over F as before. Two elements $\xi_1, \xi_2 \in G(F)$ are said to be *stably conjugate* if there exists $g \in G(\overline{F})$ such that $\xi_1 = g\xi g^{-1}$. Let G_ξ be the centralizer of $\xi \in G(F)$. Langlands [9] establishes a bijection between the set of conjugacy classes within the stable conjugacy class of ξ and $\ker(H^1(F, G_\xi) \to H^1(F, G))$. In the example where $G = \mathrm{SL}_2$ and $F = \mathbb{Q}$, every element of order 4 in $\mathrm{SL}_2(\mathbb{Q})$ is stably conjugate to ξ_0. Since $H^1(\mathbb{Q}, \mathrm{SL}_2) = \{1\}$ and G_{ξ_0} coincides with the norm 1 torus $T :=$ $\ker\big(\mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_{m,K}) \xrightarrow{\mathrm{N}_{K/\mathbb{Q}}} \mathbb{G}_{m,\mathbb{Q}}\big)$, we recover the result

$$\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q})) \simeq H^1(\mathbb{Q}, T) = \mathbb{Q}^\times/\,\mathrm{N}_{K/\mathbb{Q}}(K^\times).$$

2.2. **Galois cohomology and forms.** Let X_0 be a quasi-projective algebraic variety over an arbitrary field k, and denote by $\Gamma_k = \mathrm{Gal}(k_s/k)$ the Galois group of k_s/k, where k_s is a separable closure of k. Let $\Sigma(X_0, k_s/k)$ denote the set of isomorphism classes of k_s/k-forms of X_0. In other words, $\Sigma(X_0, k_s/k)$ classifies algebraic varieties X over k such that there is an isomorphism $X \otimes_k k_s \simeq X_0 \otimes_k k_s$. It is well known due to Weil that there is a natural bijection $\Sigma(X_0, k_s/k) \xrightarrow{\sim} H^1(\Gamma_k, G)$ of pointed sets, where $G = \mathrm{Aut}(X_0 \otimes k_s)$ is the group of automorphisms of $X_0 \otimes_k k_s$ equipped with a continuous Γ_k-action. If Γ_k acts trivially on $\mathrm{Aut}(X_0 \otimes k_s)$, namely the natural inclusion $\mathrm{Aut}(X_0) \hookrightarrow \mathrm{Aut}(X_0 \otimes k_s)$ is bijective, then one has $H^1(\Gamma_k, G) = \mathrm{Hom}(\Gamma_k, G)/G$, where G acts on $\mathrm{Hom}(\Gamma_k, G)$ by conjugation. In addition, if Γ_k is the profinite group $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$, one obtains a natural bijection of pointed sets:

$$\Sigma(X_0, k_s/k) \xrightarrow{\sim} \mathrm{Cl}_0(G), \quad G = \mathrm{Aut}(X_0). \tag{2.2}$$

Applying Weil's result to abelian varieties over finite fields, one obtains the following easy consequence.

Proposition 2.6. *Let* X_0 *be an abelian variety over a finite field* $\mathbb{F}_q$ *such that the endomorphism algebra* $\mathrm{End}^0(X_0 \otimes \overline{\mathbb{F}}_q)$ *is equal to* $\mathrm{End}^0(X_0)$*, and let* $G = \mathrm{Aut}(X_0)$. *Then there is a natural bijection of pointed sets* $\Sigma(X_0, \overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \mathrm{Cl}_0(G)$.

Note that the group G in Proposition 2.6 is an arithmetic subgroup of the reductive group $\underline{G}$ over $\mathbb{Q}$ for which $\underline{G}(R) = (\mathrm{End}^0(X_0) \otimes_{\mathbb{Q}} R)^\times$ for any $\mathbb{Q}$-algebra R.

Proof of Proposition 1.1. We choose an supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ with $\mathrm{End}(E_0) = \mathcal{O}$ under an isomorphism $\mathrm{End}^0(E_0) \simeq D$. Put $X_0 = E_0^d \otimes_{\mathbb{F}_{p^2}} \mathbb{F}_q$, then we have $G = \mathrm{Aut}(X_0) = \mathrm{GL}_d(\mathcal{O})$ and the Galois group $\Gamma_{\mathbb{F}_q}$ acts trivially on

G. By Proposition 2.6, there is a natural bijection $\Sigma(X_0, \overline{\mathbb{F}}_q/\mathbb{F}_q) \xrightarrow{\sim} \mathrm{Cl}_0\, G$. As X_0 is superspecial of dimension $d > 1$, for any d-dimensional superspecial abelian variety X over $\mathbb{F}_q$ there is an isomorphism $X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q \simeq X_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$; see [10, Section 1.6, p.13]. Thus, $\Sigma(X_0, k_s/k)$ classifies d-dimensional superspecial abelian surfaces over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism. This completes the proof of the proposition.

In this paper we compute explicitly the size of $\mathrm{Cl}_0\, G$ in the case $G = \mathrm{GL}_2(\mathcal{O})$ (i.e. $d = 2$). This may serve as a basic sample of calculating $|\mathrm{Cl}_0\, G|$ for arithmetic subgroups G. One easily sees that the calculation becomes very complicated when G is large. Explicit formulas for them seems to be out of reach. Still, the strategy for computation and structures among various invariants would be worthwhile to investigate. Perhaps, it is useful to mention the following work to the interested reader, though these are not used in the present paper.

(a) Conjugacy classes of linear algebraic groups are studied by Springer and Steinberg [14].

(b) Hashimoto [6] deduces a formula which relates optimal embeddings, semisimple conjugacy classes and class numbers of Levi subgroups of an arithmetic subgroup. This generalizes some previous methods for parameterizing conjugacy classes of elements of finite order in Siegel modular groups.

3. The Cardinality of $\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))$

Let D be a finite-dimensional central division $\mathbb{Q}$-algebra, and $\mathcal{O}$ a maximal order in D. Fix an integer $d > 1$. We explain the strategy for calculating the cardinality of $\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$, based on the lattice description of conjugacy classes in [21, Section 6.4]. As remarked in Section 1, $|\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))|$ depends only on d and D, not on the choice of the maximal order $\mathcal{O}$. So it makes sense to set $H(d, D) := |\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))|$. The strategy is carried out in detail for the case $d = 2$ and $D = D_{p,\infty}$ in subsequent sections under a mild condition on p, and the resulting formula for $H(2, D_{p,\infty})$ is stated in Theorem 3.2.

3.1. **The general strategy.** Given an element $x \in \mathrm{GL}_d(\mathcal{O})$ of finite order, its minimal polynomial over $\mathbb{Q}$ is of the form

$$P_{\underline{n}}(T) = \Phi_{n_1}(T) \cdots \Phi_{n_r}(T), \quad 1 \le n_1 < \cdots < n_r \tag{3.1}$$

for some r-tuple $\underline{n} = (n_1, \ldots, n_r) \in \mathbb{N}^r$, where $\Phi_n(T) \in \mathbb{Z}[T]$ denotes the n-th cyclotomic polynomial. For simplicity, we denote the set of strictly increasing r-tuples of positive integers by $\check{\mathbb{N}}^r$. Let $C(\underline{n}) \subseteq \mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$ be the subset of conjugacy classes with minimal polynomial $P_{\underline{n}}(T)$. The subring $\mathbb{Z}[x] \subset \mathrm{Mat}_d(\mathcal{O})$ (resp. subalgebra $\mathbb{Q}[x] \subset \mathrm{Mat}_d(D)$) generated by x is isomorphic to $A_{\underline{n}}$ (resp. $K_{\underline{n}}$) defined as follows

$$A_{\underline{n}} := \frac{\mathbb{Z}[T]}{\prod_{i=1}^r \Phi_{n_i}(T)}, \qquad K_{\underline{n}} := \frac{\mathbb{Q}[T]}{\prod_{i=1}^r \Phi_{n_i}(T)} \cong \prod_{i=1}^r \mathbb{Q}[T]/(\Phi_{n_i}(T)). \tag{3.2}$$

If $r = 1$, we omit the underline in $\underline{n}$ and write A_n and K_n instead. Hence $K_{\underline{n}} \cong \prod_{i=1}^r K_{n_i}$, but this decomposition does *not* hold for $A_{\underline{n}}$ in general. Let $\mathcal{O}^{\mathrm{opp}}$ (resp. D^{opp}) be the opposite ring of $\mathcal{O}$ (resp. D). We define

$$\mathscr{A}_{\underline{n}} := A_{\underline{n}} \otimes_{\mathbb{Z}} \mathcal{O}^{\mathrm{opp}}, \quad \text{and} \quad \mathscr{K}_{\underline{n}} := K_{\underline{n}} \otimes_{\mathbb{Q}} D^{\mathrm{opp}}. \tag{3.3}$$

Clearly, $\mathscr{A}_{\underline{n}}$ is an order in the semisimple $\mathbb{Q}$-algebra $\mathscr{K}_{\underline{n}} \cong \prod_{i=1}^r \mathscr{K}_{n_i}$. Each $\mathscr{K}_n$ is a central simple K_n-algebra, whose left simple module is denoted by W_n. The dimension $e(n)$ of W_n as a left D^{opp}-space (or equivalently, a right D-space) is also the smallest $e \in \mathbb{N}$ such that there exists an embedding $K_n \hookrightarrow \mathrm{Mat}_e(D)$.

Let $V = D^d$ be the right D-space of column vectors, and $M_0 = \mathcal{O}^d \subset V$ the standard $\mathcal{O}$-lattice in V. Then $\mathrm{End}_{\mathcal{O}}(M_0) = \mathrm{Mat}_d(\mathcal{O})$, acting on M_0 from the left by multiplication. The conjugacy class $[x] \in C(\underline{n})$ equips M_0 with a faithful $(A_{\underline{n}}, \mathcal{O})$-bimodule structure, or equivalently, a faithful left $\mathscr{A}_{\underline{n}}$-module structure. Similarly, V is equipped with a faithful left $\mathscr{K}_{\underline{n}}$-module structure. The decomposition of $K_{\underline{n}}$ in (3.2) induces a decomposition

$$V = \oplus_{i=1}^r V_{n_i}, \tag{3.4}$$

where each V_{n_i} is a *nonzero* $\mathscr{K}_{n_i}$-module. Hence $V_{n_i} \simeq (W_{n_i})^{m_i}$ for some $m_i \in \mathbb{N}$. Comparing the D-dimensions, we get

$$d = m_1 e(n_1) + \cdots + m_r e(n_r). \tag{3.5}$$

The r-tuple $\underline{m} = (m_1, \dots, m_r) \in \mathbb{N}^r$ shall be called the *type* of the left $\mathscr{K}_{\underline{n}}$-module V, and the pair $(\underline{n}, \underline{m})$ the *type* of the conjugacy class $[x] \in C(\underline{n}) \subseteq \mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$.

A pair of r-tuples $(\underline{n}, \underline{m}) \in \breve{\mathbb{N}}^r \times \mathbb{N}^r$ is said to be *d-admissible* if it satisfies equation (3.5). Let $C(\underline{n}, \underline{m}) \subseteq \mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$ be the subset of conjugacy classes of type $(\underline{n}, \underline{m})$. Then we have

$$\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O})) = \coprod_{\underline{n}} C(\underline{n}) = \coprod_{(\underline{n}, \underline{m})} C(\underline{n}, \underline{m}), \tag{3.6}$$

where $(\underline{n}, \underline{m})$ runs over all d-admissible pairs. The same proof of [21, Theorem 6.11] establishes a bijection between $C(\underline{n}, \underline{m})$ and the set $\mathscr{L}(\underline{n}, \underline{m})$ of isomorphism classes of $\mathscr{A}_{\underline{n}}$-lattices in the left $\mathscr{K}_{\underline{n}}$-module V of type $\underline{m}$. The latter set is finite according to the Jordan-Zassenhaus Theorem [2, Theorem 24.1, p. 534]. Put $o(\underline{n}) := |C(\underline{n})|$ and $o(\underline{n}, \underline{m}) := |C(\underline{n}, \underline{m})| = |\mathscr{L}(\underline{n}, \underline{m})|$. It follows from (3.6) that

$$H(d, D) = |\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))| = \sum_{\underline{n}} o(\underline{n}) = \sum_{(\underline{n}, \underline{m})} o(\underline{n}, \underline{m}). \tag{3.7}$$

Now fix a d-admissible pair $(\underline{n}, \underline{m}) \in \breve{\mathbb{N}}^r \times \mathbb{N}^r$ and a left $\mathscr{K}_{\underline{n}}$-module V of type $\underline{m}$. The isomorphism class of an $\mathscr{A}_{\underline{n}}$-lattice $\Lambda \subset V$ is denoted by $[\Lambda]$. Two $\mathscr{A}_{\underline{n}}$-lattices $\Lambda_1, \Lambda_2 \subset V$ are isomorphic if and only if there exists $g \in \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)^\times$ such that $\Lambda_1 = \Lambda_2 g$ (In particular, $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$ acts on V from the right). Clearly,

$$\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = \oplus_{i=1}^r \mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}), \text{ and } \mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}) \sim \mathscr{K}_{n_i} = K_{n_i} \otimes_{\mathbb{Q}} D^{\mathrm{opp}}, \tag{3.8}$$

where $\sim$ denotes the Morita equivalence of central simple algebras. On the other hand, $\mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i})^{\mathrm{opp}}$ is canonically isomorphic to the centralizer of K_{n_i} in $\mathrm{End}_D(V_{n_i})$. So by the Centralizer Theorem [4, Theorem 3.15],

$$[K_{n_i} : \mathbb{Q}]^2 [\mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}) : K_{n_i}] = [\mathrm{End}_D(V_{n_i}) : \mathbb{Q}] = [D : \mathbb{Q}](m_i e(n_i))^2. \tag{3.9}$$

The structure of $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$ is completely determined by (3.8) and (3.9).

For each prime $\ell \in \mathbb{N}$, let Λ_ℓ be the ℓ-adic completion of Λ, and $\mathscr{L}_\ell(\underline{n}, \underline{m})$ the set of isomorphism classes of $\mathscr{A}_{\underline{n},\ell}$-lattices in V_ℓ. The profinite completion $\Lambda \mapsto \widehat{\Lambda} = \prod_\ell \Lambda_\ell$ induces a surjective map

$$\Phi : \mathscr{L}(\underline{n}, \underline{m}) \to \prod_\ell \mathscr{L}_\ell(\underline{n}, \underline{m}). \tag{3.10}$$

For almost all primes ℓ, the order $\mathscr{A}_{\underline{n},\ell}$ is maximal in $\mathscr{K}_{\underline{n},\ell}$, in which case $\mathscr{L}_\ell(\underline{n},\underline{m})$ is a singleton by [2, Theorem 26.24]. So the right hand side of (3.10) is essentially a finite product. Two lattices Λ_1 and Λ_2 are said to be in the same *genus* if $\Phi([\Lambda_1]) = \Phi([\Lambda_2])$, that is, if they are locally isomorphic at every prime ℓ. The fibers of Φ partition $\mathscr{L}(\underline{n},\underline{m})$ into a disjoint union of genera. More explicitly, for each element $\mathbb{L} = ([\Lambda'_\ell])_\ell \in \prod_\ell \mathscr{L}_\ell(\underline{n},\underline{m})$, let

$$\mathscr{L}(\underline{n},\underline{m},\mathbb{L}) := \Phi^{-1}(\mathbb{L}) = \{[\Lambda] \in \mathscr{L}(\underline{n},\underline{m}) \mid \Lambda_\ell \simeq \Lambda'_\ell, \forall \ell.\}. \tag{3.11}$$

Then $\mathscr{L}(\underline{n},\underline{m}) = \coprod_{\mathbb{L}} \mathscr{L}(\underline{n},\underline{m},\mathbb{L})$, where $\mathbb{L}$ runs over elements of $\prod_\ell \mathscr{L}_\ell(\underline{n},\underline{m})$.

Lastly, we pick an $\mathscr{A}_{\underline{n}}$-lattice $\Lambda \subset V$ with $[\Lambda] \in \mathscr{L}(\underline{n},\underline{m},\mathbb{L})$ and write O_Λ for its endomorphism ring $\mathrm{End}_{\mathscr{A}_{\underline{n}}}(\Lambda) \subset \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$. It follows from [15, Proposition 1.4] that $\mathscr{L}(\underline{n},\underline{m},\mathbb{L})$ is bijective to the set of right ideal classes of O_Λ. In particular,

$$|\mathscr{L}(\underline{n},\underline{m},\mathbb{L})| = h(O_\Lambda). \tag{3.12}$$

Another choice Λ' with $[\Lambda'] \in \mathscr{L}(\underline{n},\underline{m},\mathbb{L})$ produces an endomorphism ring $O_{\Lambda'}$ locally conjugate to O_Λ at every prime ℓ, and hence the same class number $h(O_{\Lambda'}) = h(O_\Lambda)$. If $\mathscr{A}_{\underline{n}}$ is maximal at ℓ, then $(O_\Lambda)_\ell$ is a maximal order in $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)_\ell = \mathrm{End}_{\mathscr{K}_{\underline{n},\ell}}(V_\ell)$

In summary, the calculation of $H(d,D)$ is separated into 3 steps:

(1) for each $1 \le r \le d$, list the set $\mathcal{T}(d,r)$ of all d-admissible pairs $(\underline{n},\underline{m}) \in \breve{\mathbb{N}}^r \times \mathbb{N}^r$. We set $\mathcal{T}(r) = \mathcal{T}(d,r)$ if d is clear from the context.
(2) For each $(\underline{n},\underline{m})$, classify the genera of $\mathscr{A}_{\underline{n}}$-lattices in the left $\mathscr{K}_{\underline{n}}$-module V of type $\underline{m}$. This amounts to classifying the isomorphism classes of $\mathscr{A}_{\underline{n},\ell}$-lattices in V_ℓ. Only the primes ℓ with $\mathscr{A}_{\underline{n},\ell}$ non-maximal come in to play.
(3) For each genus, write down (at least locally) the endomorphism ring of an lattice member and calculate its class number. The sum of all these class numbers is $H(d,D)$.

Remark 3.1. We make a couple simplifications for the calculations.
(i) The center $Z(\mathrm{GL}_d(\mathcal{O})) = \{\pm 1\}$ acts on $\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$ by multiplication and induces a bijection between $C(\underline{n})$ and $C(\underline{n}^\dagger)$, where $\underline{n}^\dagger$ is obtained by first defining an intermediate r-tuple $\underline{n}^\ddagger := (n_1^\ddagger, \dots, n_r^\ddagger)$ with

$$n_i^\ddagger = \begin{cases} 2n_i & \text{if } 2 \nmid n_i, \\ n_i & \text{if } 4 \mid n_i, \\ n_i/2 & \text{otherwise,} \end{cases} \tag{3.13}$$

for each $1 \le i \le r$, and then re-arrange its entries in ascending order. For example, if $\underline{n} = (3,4)$, then $\underline{n}^\dagger = (4,6)$. Thus $o(\underline{n}) = o(\underline{n}^\dagger)$ and only one of them needs to be calculated.
(ii) Let u be the reduced degree of D over $\mathbb{Q}$, and Λ an $\mathscr{A}_{\underline{n}}$-lattice in the $\mathscr{K}_{\underline{n}}$-module V of type $\underline{m}$. For almost all primes ℓ, we have $\mathcal{O}^{\mathrm{opp}} \otimes \mathbb{Z}_\ell \simeq \mathrm{Mat}_u(\mathbb{Z}_\ell)$, and hence $\mathscr{A}_{\underline{n},\ell} \simeq \mathrm{Mat}_u(A_{\underline{n},\ell})$. Fix such an ℓ. It then follows from Morita equivalence that $\Lambda_\ell \simeq (\Lambda'_\ell)^u$ and $V_\ell \simeq (V'_\ell)^u$, where Λ'_ℓ is an $A_{\underline{n},\ell}$-lattice in the $K_{\underline{n},\ell}$-module $V'_\ell = \prod_{i=1}^r V'_{n_i,\ell}$. Each $V'_{n_i,\ell}$ is a free $K_{n_i,\ell}$-module of rank

$$\dim_{\mathbb{Q}}(D^{m_i e(n_i)})/(u[K_{n_i}:\mathbb{Q}]) = u m_i e(n_i)/\varphi(n_i). \tag{3.14}$$

The association $\Lambda_\ell \mapsto \Lambda'_\ell$ establishes a one-to-one correspondence between $\mathscr{L}_\ell(\underline{n},\underline{m})$ and the set of isomorphism classes of $A_{\underline{n},\ell}$-lattice in V'_ℓ. Moreover, $\mathrm{End}_{\mathscr{A}_{\underline{n},\ell}}(\Lambda_\ell) \cong \mathrm{End}_{A_{\underline{n},\ell}}(\Lambda'_\ell)$.

3.2. **Explicit formulas for $H(2, D_{p,\infty})$.** First, we list all 2-admissible pairs $(\underline{n}, \underline{m}) \in \breve{\mathbb{N}}^r \times \mathbb{N}^r$ for $r = 1, 2$. Note that $e(n) \leq 2$ only if $\varphi(n) = [K_n : \mathbb{Q}] \leq 4$, i.e. $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. More explicitly,

- if $n \in \{1, 2\}$, then $K_n = \mathbb{Q}$ and $e(n) = 1$;
- if $n \in \{3, 4, 6\}$, then $[K_n : \mathbb{Q}] = 2$. We have $e(n) = 2$ if p splits in K_n, and $e(n) = 1$ otherwise.
- if $n \in \{5, 8, 10, 12\}$, then $[K_n : \mathbb{Q}] = 4$ and $e(n) \geq 2$. The equality holds if and only if p does *not* split completely in K_n.

Thus we have

$$\mathcal{T}(1) = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}, me(n) = 2\},$$
$$\mathcal{T}(2) = \{((n_1, n_2), (m_1, m_2)) \in \breve{\mathbb{N}}^2 \times \mathbb{N}^2 \mid n_1 < n_2, n_i \in \{1, 2, 3, 4, 6\}, m_i e(n_i) = 1\}.$$

For each $\underline{n} \in \breve{\mathbb{N}}^r$ with $r = 1, 2$, there is at most one $\underline{m} \in \mathbb{N}^r$ such that $(\underline{n}, \underline{m})$ is 2-admissible. So we omit $\underline{m}$ from the notation $\mathscr{L}(\underline{n}, \underline{m})$ and write $\mathscr{L}(\underline{n})$ instead. By Remark 3.1, we have

$$o(1) = o(2) = 1,\ o(3) = o(6),\ o(5) = o(10);$$
$$o(1, 3) = o(2, 6),\ o(1, 4) = o(2, 4),\ o(1, 6) = o(2, 3),\ o(3, 4) = o(4, 6).$$

Theorem 3.2. *Let $D = D_{p,\infty}$ be the quaternion $\mathbb{Q}$-algebra ramified exactly at p and ∞, and $\mathcal{O}$ a maximal order in D. We have*

$$\begin{aligned} H(2, D_{p,\infty}) =& |\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))| = 2 + 2o(3) + o(4) + 2o(5) + o(8) + o(12) \\ & + o(1, 2) + 2o(2, 3) + 2o(2, 4) + 2o(2, 6) + 2o(3, 4) + o(3, 6), \end{aligned} \tag{3.15}$$

where the value of each term is as follows:

- $o(3) = 2 - \left(\frac{-3}{p}\right)$;
- $o(4) = 2 - \left(\frac{-4}{p}\right)$;
- $o(5) = \begin{cases} 1 & \text{if } p = 5; \\ 0 & \text{if } p \equiv 1 \pmod 5; \\ 2 & \text{if } p \equiv 2, 3 \pmod 5; \\ 4 & \text{if } p \equiv 4 \pmod 5; \end{cases}$
- $o(8) = \begin{cases} 1 & \text{if } p = 2; \\ 0 & \text{if } p \equiv 1 \pmod 8; \\ 4 & \text{if } p \equiv 3, 5, 7 \pmod 8; \end{cases}$
- $o(12) = \begin{cases} 3 & \text{if } p = 2, 3; \\ 0 & \text{if } p \equiv 1 \pmod{12}; \\ 4 & \text{if } p \equiv 5, 7, 11 \pmod{12}; \end{cases}$
- $$\begin{aligned} o(1, 2) =& \frac{(p-1)^2}{9} + \frac{p+15}{18}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{p+2}{6}\left(1 - \left(\frac{-4}{p}\right)\right) \\ & + \frac{1}{6}\left(1 - \left(\frac{-3}{p}\right)\right)\left(1 - \left(\frac{-4}{p}\right)\right) \quad \text{if } p \neq 3, \text{ and} \end{aligned}$$
  $$o(1, 2) = 3 \quad \text{if} \quad p = 3;$$

- $o(2,3) = \left(1 - \left(\frac{-3}{p}\right)\right)\left(\frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right)\right)$;
- $o(2,4) = \left(\frac{p+3}{3} - \frac{1}{3}\left(\frac{-3}{p}\right)\right)\left(1 - \left(\frac{-4}{p}\right)\right)$;
- $o(2,6) = \left(\frac{5p+18}{12} + \frac{1}{3}\left(\frac{-3}{p}\right) - \frac{1}{4}\left(\frac{-4}{p}\right)\right)\left(1 - \left(\frac{-3}{p}\right)\right)$;
- $o(3,4) = \left(1 - \left(\frac{-3}{p}\right)\right)\left(1 - \left(\frac{-4}{p}\right)\right)$;
- $o(3,6) = 2\left(1 - \left(\frac{-3}{p}\right)\right)^2$.

Corollary 3.3. *Keeping the notations of Theorem 3.2, we have*

$$\lim_{p\to\infty} \frac{H(2, D_{p,\infty})}{p^2/9} = 1. \tag{3.16}$$

Proof. By Theorem 3.2, the dominant term of $H(2, D_{p,\infty})$ is $o(1,2)$, which is asymptotic to $(p-1)^2/9$ as p tends to infinity. □

For ease of exposition of the present paper, we will work out the calculation of each $o(\underline{n})$ in Theorem 3.2 under the assumption that $A_{\underline{n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is an étale $\mathbb{Z}_p$-algebra. For example, if $r = 1$, this simply requires p to be unramified in K_n. Note that this assumption holds automatically when $p \geq 7$ so it rules out at most $p = 2, 3, 5$. Section 4 treats the *elementary* case where $r = 1$. The remaining case $r = 2$ is called *non-elementary* and is treated in Section 5. The calculation of class numbers of certain complicated orders arose in Section 5 is postponed to Section 6. The handful cases where the assumption fails will be treated in an upcoming paper [22], where the ramification requires much greater care.

Remark 3.4. Karemaker and Pries [8, Proposition 7.2] give a full classification of the types of principally polarized simple supersingular abelian surfaces (A, λ) over a finite field $\mathbb{F}_q$ with $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(A, \lambda) = \mathbb{Z}/2\mathbb{Z}$. They also prove [8, Proposition 7.6] that if $p \geq 3$, then the portion of $\mathbb{F}_{p^r}$-rational points of the supersingular locus $\mathcal{A}_{2,ss}$ which represent (A, λ) with $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(A, \lambda) \neq \mathbb{Z}/2\mathbb{Z}$ tends to zero as $r \to \infty$. They ask weather or not the majority of principally polarized supersingular abelian surfaces over $\mathbb{F}_{p^r}$ are those with normalized Weil number $(1, 1, -1, -1)$. From Theorem 3.2 and [21, Theorems 1.1 and 1.2] we see that the portion of *superspecial* abelian surfaces over $\mathbb{F}_{p^r}$ with normalized Weil number $(1, 1, -1, -1)$ (with r fixed) tends to one as $p \to \infty$. However, to deduce the similar result for supersingular abelian surfaces, one could use the argument of [18, Section 5] where we compute the size of the isogeny class corresponding to the Weil number $\sqrt{p^r}$ with odd r.

4. Computations of the elementary case

Throughout this section, n denotes one of the integers $\{3, 4, 5, 8, 12\}$, and $D = D_{p,\infty}$, the quaternion $\mathbb{Q}$-algebra ramified exactly at the prime p and ∞. The goal of this section is to calculate the terms $o(n)$ in Theorem 3.2, under the assumption that p is *unramified* in K_n (i.e. $p \nmid n$). Note that p splits completely in K_n if and only if $p \equiv 1 \pmod{n}$. By the discussion at the beginning of Section 3.2, if $n \in \{5, 8, 12\}$ then we further assume that $p \not\equiv 1 \pmod{n}$, for otherwise $o(n) = 0$.

The cyclotomic field K_n with $n \in \{3, 4, 5, 8, 12\}$ has class number 1 by [17, Theorem 11.1]. For $n \in \{3, 4\}$ and $p \equiv 1 \pmod{n}$, let $\mathscr{D}_n$ denote the quaternion K_n-algebra ramified exactly at the two places of K_n above p. Since D^{opp} is canonically isomorphic to D, we have

$$\mathscr{K}_n = K_n \otimes_{\mathbb{Q}} D = \begin{cases} \mathscr{D}_n & \text{if } n \in \{3,4\} \text{ and } p \equiv 1 \pmod{n}, \\ \mathrm{Mat}_2(K_n) & \text{otherwise.} \end{cases} \tag{4.1}$$

The order $\mathscr{A}_n \subset \mathscr{K}_n$ is maximal at every prime $\ell \neq p$. It is also maximal at p when $n \in \{3,4\}$ and $p \equiv 1 \pmod{n}$. Let $V \simeq D^2$ be the unique *faithful* left $\mathscr{K}_n$-module of D-dimension 2 (as a right D-vector space). Then V is a free $\mathscr{K}_n$-module of rank 1 if $n \in \{3,4\}$, and a simple $\mathscr{K}_n$-module if $n \in \{5,8,12\}$. By (3.8) and (3.9), we have

$$\mathscr{E}_n := \mathrm{End}_{\mathscr{K}_n}(V) \simeq \begin{cases} K_n \otimes_{\mathbb{Q}} D & \text{if } n \in \{3,4\}, \\ K_n & \text{if } n \in \{5,8,12\}. \end{cases} \tag{4.2}$$

If $n \in \{3,4\}$, then $\mathscr{E}_n$ is a quaternion algebra over the imaginary quadratic field K_n. Hence $\mathscr{E}_n$ verifies the Eichler condition [13, Definition 34.3], and $\mathrm{Nr}(\mathscr{E}_n^\times) = K_n^\times$ by [16, Theorem III.4.1].

Let Λ be an $\mathscr{A}_n$-lattice in V, and $O_\Lambda := \mathrm{End}_{\mathscr{A}_n}(\Lambda)$. The order $O_\Lambda \subset \mathscr{E}_n$ is maximal at every prime $\ell \neq p$ by the maximality of $\mathscr{A}_{n,\ell}$. If $n \in \{5,8,12\}$, then $A_n \subseteq O_\Lambda \subset K_n$, and hence $O_\Lambda = A_n$, which has class number 1. If $n \in \{3,4\}$, then O_Λ is an A_n-order in $\mathscr{E}_n$. We claim that $h(O_\Lambda) = 1$ in this case as well. If p is inert in K_n, then it will be shown that O_Λ is an Eichler order in Proposition 4.1, otherwise O_Λ is maximal in $\mathscr{E}_n$. Thus $h(O_\Lambda) = h(A_n) = 1$ by [16, Corollaire III.5.7]. It follows that for all $n \in \{3,4,5,8,12\}$ and $p \nmid n$,

$$o(n) = |\prod_\ell \mathscr{L}_\ell(n)| = |\mathscr{L}_p(n)|. \tag{4.3}$$

For each $f \in \mathbb{N}$, let $\mathbb{Z}_{p^f} = W(\mathbb{F}_{p^f})$, the ring of Witt vectors of $\mathbb{F}_{p^f}$. Then $\mathbb{Q}_{p^f} := \mathbb{Z}_{p^f}[1/p]$ is the unique unramified extension of degree f of $\mathbb{Q}_p$.

Proposition 4.1. *Suppose that $n \in \{3,4\}$ and $p \nmid n$. Then*

$$o(3) = 2 - \left(\frac{-3}{p}\right) \qquad \text{and} \qquad o(4) = 2 - \left(\frac{-4}{p}\right).$$

Proof. If p splits in K_n, then $\mathscr{A}_n$ is a maximal order in $\mathscr{K}_n$, so there is a unique genus of $\mathscr{A}_n$-lattices in V. We have $o(n) = 1$ by (4.3).

Suppose that p is inert in K_n. Then $e(n) = 1$, and V is a free $\mathscr{K}_n$-module of rank 1. We have $A_{n,p} = A_n \otimes \mathbb{Z}_p = \mathbb{Z}_{p^2}$, so by [16, Corollaire II.1.7],

$$\mathscr{A}_{n,p} = A_{n,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_p \simeq \begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix}.$$

It follows that any $\mathscr{A}_{n,p}$-lattice $\Lambda_p \subseteq V_p$ is isomorphic to one of the following

$$\begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & p\mathbb{Z}_{p^2} \end{pmatrix}, \quad \begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix}, \quad \begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix}.$$

Correspondingly, $(O_\Lambda)_p$ is isomorphic to

$$\mathrm{Mat}_2(\mathbb{Z}_{p^2}), \quad \begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix}, \quad \mathrm{Mat}_2(\mathbb{Z}_{p^2}),$$

which verifies the claim above (4.3) that O_Λ is an Eichler order when p is inert in K_n. We conclude that $o(n) = 3$ by (4.3). □

Proposition 4.2. *Suppose that $n \in \{5, 8, 12\}$ and $p \nmid n$. Then the formulas for $o(n)$ in Theorem 3.2 hold. More explicitly,*

(1) $o(n) = 0$ if $p \equiv 1 \pmod n$;
(2) $o(5) = 2$ if $p \equiv 2, 3 \pmod 5$;
(3) $o(n) = 4$ in the remaining cases.

Proof. Only part (2) and (3) need to be proved. Suppose that $p \not\equiv 0, 1 \pmod n$. Then $e(n) = 2$, and V is a simple $\mathscr{K}_n$-module.

If $n = 5$ and $p \equiv 2, 3 \pmod 5$, then

$$A_{5,p} \simeq \mathbb{Z}_{p^4}, \quad \text{and} \quad \mathscr{A}_{5,p} = A_{5,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_p \simeq \begin{pmatrix} \mathbb{Z}_{p^4} & \mathbb{Z}_{p^4} \\ p\mathbb{Z}_{p^4} & \mathbb{Z}_{p^4} \end{pmatrix}.$$

Any $\mathscr{A}_{5,p}$-lattice $\Lambda_p \subseteq V_p$ is isomorphic to $\begin{pmatrix} \mathbb{Z}_{p^4} \\ p\mathbb{Z}_{p^4} \end{pmatrix}$ or $\begin{pmatrix} \mathbb{Z}_{p^4} \\ \mathbb{Z}_{p^4} \end{pmatrix}$. Hence $o(5) = 2$ in this case.

For the remaining cases, we have

$$\mathscr{A}_{n,p} = A_{n,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_p \simeq (\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}) \otimes_{\mathbb{Z}_p} \mathcal{O}_p \simeq \begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix} \times \begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix}.$$

Every $\mathscr{A}_{n,p}$-lattice $\Lambda_p \subseteq V_p$ decomposes into $\Lambda_p^{(1)} \oplus \Lambda_p^{(2)}$, where each $\Lambda_p^{(i)}$ is a $\begin{pmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{pmatrix}$-lattice in the simple $\mathrm{Mat}_2(\mathbb{Q}_{p^2})$-module $V_p^{(i)} \simeq (\mathbb{Q}_{p^2})^2$. There are 2 isomorphism classes of $\Lambda_p^{(i)}$ for each $i = 1, 2$. Therefore, $o(n) = 2^2 = 4$. □

5. Computations of non-elementary cases

We treat the non-elementary cases

$$\underline{n} = (n_1, n_2) \in \{(1, 2), (2, 3), (2, 4), (2, 6), (3, 4), (3, 6)\}, \tag{5.1}$$

under the assumption that $A_{\underline{n},p} = A_{\underline{n}} \otimes \mathbb{Z}_p$ is étale over $\mathbb{Z}_p$. Equivalently, p is assumed to satisfy the following two conditions:

(I) p is unramified in $K_{n_i} = \mathbb{Q}[T]/(\Phi_{n_i}(T))$ for $i = 1, 2$;
(II) $A_{\underline{n},p} = \mathbb{Z}_p[T]/(\Phi_{n_1}(T)\Phi_{n_2}(T))$ is maximal in $K_{\underline{n},p}$.

This rules out at most $p = 2, 3$. There exists a *faithful* left $\mathscr{K}_{\underline{n}}$-module $V \simeq D^2$ if and only if $e(n_i) = 1$ for both $i = 1, 2$. Thus $o(\underline{n}) = 0$ unless p is inert in K_{n_i} when $[K_{n_i} : \mathbb{Q}] = 2$. So we make further restrictions on p as listed in Table 1.

By (3.4), $V = V_{n_1} \oplus V_{n_2}$, where each V_{n_i} is a simple $\mathscr{K}_{n_i}$-module with $\dim_D V_{n_i} = 1$. Therefore, $\mathscr{E}_{\underline{n}} := \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = \mathrm{End}_{\mathscr{K}_{n_1}}(V_{n_1}) \times \mathrm{End}_{\mathscr{K}_{n_2}}(V_{n_2})$, and

$$\forall i = 1, 2, \qquad \mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}) = \begin{cases} D & \text{if } K_{n_i} = \mathbb{Q}; \\ K_{n_i} & \text{if } [K_{n_i} : \mathbb{Q}] = 2. \end{cases} \tag{5.2}$$

Let $O_{K_{\underline{n}}} = \mathbb{Z}[T]/(\Phi_{n_1}(T)) \times \mathbb{Z}[T]/(\Phi_{n_2}(T))$ be the maximal order of $K_{\underline{n}}$. There is an exact sequence of $A_{\underline{n}}$-modules

$$0 \to A_{\underline{n}} \to O_{K_{\underline{n}}} \xrightarrow{\psi} \mathbb{Z}[T]/(\Phi_{n_1}(T), \Phi_{n_2}(T)) \to 0, \tag{5.3}$$

where $\psi : (x, y) \mapsto \bar{x} - \bar{y}$. The indices $[O_{K_{\underline{n}}} : A_{\underline{n}}]$ are listed in Table 1.

Table 1.

$\underline{n}$	$K_{\underline{n}} = K_{n_1} \times K_{n_2}$	$[O_{K_{\underline{n}}} : A_{\underline{n}}]$	$\mathscr{E}_{\underline{n}}$	Conditions on p
$(1,2)$	$\mathbb{Q}\times\mathbb{Q}$	2	$D\times D$	$p\neq 2$
$(2,3)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{-3}\,)$	1	$D\times\mathbb{Q}(\sqrt{-3}\,)$	$p\equiv 2\ (3)$
$(2,4)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{-1}\,)$	2	$D\times\mathbb{Q}(\sqrt{-1}\,)$	$p\equiv 3\ (4)$
$(2,6)$	$\mathbb{Q}\times\mathbb{Q}(\sqrt{-3}\,)$	3	$D\times\mathbb{Q}(\sqrt{-3}\,)$	$p\equiv 2\ (3)$
$(3,4)$	$\mathbb{Q}(\sqrt{-3}\,)\times\mathbb{Q}(\sqrt{-1}\,)$	1	$\mathbb{Q}(\sqrt{-3}\,)\times\mathbb{Q}(\sqrt{-1}\,)$	$p\equiv 11\ (12)$
$(3,6)$	$\mathbb{Q}(\sqrt{-3}\,)\times\mathbb{Q}(\sqrt{-3}\,)$	4	$\mathbb{Q}(\sqrt{-3}\,)\times\mathbb{Q}(\sqrt{-3}\,)$	$p\equiv 2\ (3),\ p\neq 2$

For $s=2,3$, let $\mathfrak{p}_s$ be the unique prime ideal of A_{2s} above s, which has residue field $A_{2s}/\mathfrak{p}_s\cong\mathbb{F}_s$. Similarly, let $\mathfrak{q}_2=2A_3$ be the prime ideal of A_3 above 2. We write down the non-maximal orders $A_{\underline{n}}$ explicitly using (5.3):

$$A_{(1,2)}=\{(a,b)\in\mathbb{Z}\times\mathbb{Z}\mid a\equiv b \pmod 2\};\tag{5.4}$$

$$A_{(2,2s)}=\{(a,b)\in\mathbb{Z}\times A_{2s}\mid (a \bmod s)\equiv(b \bmod \mathfrak{p}_s)\}\text{ for } s=2,3;\tag{5.5}$$

$$A_{(3,6)}\simeq\{(a,b)\in A_3\times A_3\mid a\equiv b \pmod{\mathfrak{q}_2}\},\tag{5.6}$$

where $A_6=\mathbb{Z}[T]/(T^2-T+1)$ is identified with $A_3=\mathbb{Z}[T]/(T^2+T+1)$ via a change of variable $T\mapsto -T$. Applying [21, Lemma 7.2] if necessary, we have

$$h(A_{(3,4)})=h(A_{(3,6)})=1.\tag{5.7}$$

Recall that the class number of $\mathcal{O}$ is given by

$$h(\mathcal{O})=\frac{p-1}{12}+\frac{1}{3}\left(1-\left(\frac{-3}{p}\right)\right)+\frac{1}{4}\left(1-\left(\frac{-4}{p}\right)\right).\tag{5.8}$$

By our assumptions, the order $\mathscr{A}_{\underline{n}}$ is non-maximal at a prime ℓ if and only if one of the following mutually exclusive conditions holds: (i) $\ell=p$ and $\underline{n}\neq(1,2)$; (ii) $\ell\mid[O_{K_{\underline{n}}}:A_{\underline{n}}]$.

Proposition 5.1. *Let $\underline{n}=(n_1,n_2)$ be a pair in (5.1), and $p\in\mathbb{N}$ a prime satisfying the corresponding condition in Table 1. Then*

$$|\mathscr{L}_p(\underline{n})|=[K_{n_1}:\mathbb{Q}][K_{n_2}:\mathbb{Q}].$$

For any $\mathscr{A}_{\underline{n}}$-lattice $\Lambda\subset V$, the endomorphism ring $O_\Lambda=\mathrm{End}_{\mathscr{A}_{\underline{n}}}(\Lambda)$ is maximal at p.

Proof. By assumption (II), $A_{\underline{n},p}=A_{n_1,p}\times A_{n_2,p}$. Consequently, Λ_p decomposes as $\Lambda_{n_1,p}\oplus\Lambda_{n_2,p}$, where each $\Lambda_{n_i,p}$ is an $\mathscr{A}_{n_i,p}$-lattice in the simple $\mathscr{K}_{n_i,p}$-module $V_{n_i,p}$. It is enough to show that the number of isomorphic classes of $\mathscr{A}_{n_i,p}$-lattices in $V_{n_i,p}$ is $[K_{n_i}:\mathbb{Q}]$, and $\mathrm{End}_{\mathscr{A}_{n_i,p}}(\Lambda_{n_i,p})$ is maximal for each $i=1,2$.

If $K_{n_i}=\mathbb{Q}$, then $\mathscr{A}_{n_i,p}=\mathcal{O}_p$. We have $\Lambda_{n_i,p}\simeq\mathcal{O}_p$, and $\mathrm{End}_{\mathscr{A}_{n_i,p}}(\Lambda_{n_i,p})=\mathcal{O}_p$.

If $[K_{n_i}:\mathbb{Q}]=2$, then $A_{n_i,p}\simeq\mathbb{Z}_{p^2}$ since p is inert in K_{n_i} by our assumption. It follows that $\mathscr{A}_{n_i,p}=\mathbb{Z}_{p^2}\otimes_{\mathbb{Z}_p}\mathcal{O}_p\simeq\begin{pmatrix}\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2}\\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2}\end{pmatrix}$, and $\Lambda_{n_i,p}$ is isomorphic to either $\begin{pmatrix}\mathbb{Z}_{p^2}\\ p\mathbb{Z}_{p^2}\end{pmatrix}$ or $\begin{pmatrix}\mathbb{Z}_{p^2}\\ \mathbb{Z}_{p^2}\end{pmatrix}$. In both cases, $\mathrm{End}_{\mathscr{A}_{n_i,p}}(\Lambda_{n_i,p})=\mathbb{Z}_{p^2}$. □

Corollary 5.2. *(1)* $o(2,3)=\left(1-\left(\frac{-3}{p}\right)\right)h(\mathcal{O})$ *for all* $p\neq 3$.
(2) $o(3,4)=\left(1-\left(\frac{-3}{p}\right)\right)\left(1-\left(\frac{-4}{p}\right)\right)$ *for all* $p\neq 2,3$.

Proof. Suppose that $\underline{n}\in\{(2,3),(3,4)\}$, and p satisfies the corresponding condition in Table 1. We have $A_{\underline{n}}=O_{K_{\underline{n}}}$, so $\mathscr{A}_{\underline{n}}$ is maximal at every prime $\ell\neq p$. By Proposition 5.1, the endomorphism rings of $\mathscr{A}_{\underline{n}}$-lattices in V are maximal orders in $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$, which share the same class number. It follows that $o(\underline{n})=|\mathscr{L}_p(\underline{n})|h(O_\Lambda)$ for any $\mathscr{A}_{\underline{n}}$-lattice $\Lambda\subset V$. If $\underline{n}=(2,3)$, then $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)=D\times K_3$, and $h(O_\Lambda)=h(\mathcal{O})h(A_3)=h(\mathcal{O})$. If $\underline{n}=(3,4)$, then $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)=K_3\times K_4$, and $O_\Lambda=A_3\times A_4$, which has class number 1.

For the remaining primes p considered in the corollary, both sides of the formulas are zero. The corollary is proved. □

For the rest of this section we assume that

$$\underline{n}\in\{(1,2),(2,4),(2,6),(3,6)\}\tag{5.9}$$

and $\ell\in\mathbb{N}$ a prime divisor of $[O_{K_{\underline{n}}}:A_{\underline{n}}]$. Note that ℓ is uniquely determined by $\underline{n}$ for each $\underline{n}$. Since $\ell\neq p$ by our assumption, we have $\mathcal{O}_\ell\simeq\mathrm{Mat}_2(\mathbb{Z}_\ell)$. By Remark 3.1, the classification of isomorphism classes of $\mathscr{A}_{\underline{n},\ell}$-lattices in V_ℓ reduces to that of $A_{\underline{n},\ell}$-lattices in the $K_{\underline{n},\ell}$-module V'_ℓ, where $V_\ell=(V'_\ell)^2$ and

$$V'_\ell\simeq\begin{cases}(K_{\underline{n},\ell})^2=(\mathbb{Q}_2\times\mathbb{Q}_2)^2 & \text{if } \underline{n}=(1,2)\ \text{ and } \ell=2;\\ (K_{2,\ell})^2\times K_{2s,\ell}=\mathbb{Q}_s^2\times K_{2s,s} & \text{if } \underline{n}=(2,2s) \text{ and } \ell=s\in\{2,3\};\\ K_{\underline{n},\ell}=\mathbb{Q}_4\times\mathbb{Q}_4 & \text{if } \underline{n}=(3,6)\ \text{ and } \ell=2.\end{cases}\tag{5.10}$$

First, we treat the cases $\underline{n}\in\{(1,2),(3,6)\}$, for which V'_ℓ is a free $K_{\underline{n},\ell}$-module, and $\ell=2$ for both $\underline{n}$. Let $t_{\underline{n}}$ be the $K_{\underline{n},2}$-rank of V'_2, i.e. $t_{\underline{n}}=2$ if $\underline{n}=(1,2)$, and $t_{\underline{n}}=1$ if $\underline{n}=(3,6)$. By [21, Lemma 7.1], $A_{\underline{n}}$ is a Bass order for both[1] $\underline{n}$, and so is $A_{\underline{n},2}=A_{\underline{n}}\otimes\mathbb{Z}_2$ since the Bass property is local (See [2, Section 37] for the concept of Bass orders). It follows from the results of Borevich and Faddeev [2, Section 37, p.789] that any $A_{\underline{n},2}$-lattice $\Lambda'_2\subset V'_2$ is isomorphic to $R_1\oplus\cdots\oplus R_{t_{\underline{n}}}$ for orders $R_1\subseteq\cdots\subseteq R_{t_{\underline{n}}}$ containing $A_{\underline{n},2}$ in $K_{\underline{n},2}$. The multiset $\{R_1,\dots,R_{t_{\underline{n}}}\}$ of orders with multiplicities is completely determined by the isomorphism class of Λ'_2, and vice versa.

Proposition 5.3. $o(3,6)=2\left(1-\left(\frac{-3}{p}\right)\right)^2$ *for all* $p\neq 2,3$.

Proof. Only the case $p\equiv 2\pmod 3$ and $p\neq 2$ requires a proof. For $\underline{n}=(3,6)$, $O_{K_{\underline{n},2}}$ is the only order in $K_{\underline{n},2}$ properly containing $A_{\underline{n},2}$ by (5.6). So any $A_{\underline{n},2}$-lattice Λ'_2 in $V'_2\simeq K_{\underline{n},2}$ is isomorphic to $A_{\underline{n},2}$ or $O_{K_{\underline{n},2}}$. Correspondingly,

$$\mathrm{End}_{A_{\underline{n},2}}(\Lambda'_2)=\begin{cases}A_{\underline{n},2} & \text{if } \Lambda'_2\simeq A_{\underline{n},2},\\ O_{K_{\underline{n},2}} & \text{if } \Lambda'_2\simeq O_{K_{\underline{n},2}},\end{cases}\tag{5.11}$$

and the same holds for $\mathrm{End}_{\mathscr{A}_{\underline{n},2}}(\Lambda_2)$ by Remark 3.1. It follows from Proposition 5.1 that

$$\mathrm{End}_{\mathscr{A}_{\underline{n}}}(\Lambda)=\begin{cases}A_{\underline{n}} & \text{if } \Lambda_2\simeq(A_{\underline{n},2})^2,\\ O_{K_{\underline{n}}} & \text{if } \Lambda_2\simeq(O_{K_{\underline{n},2}})^2\end{cases}$$

[1] In fact, $A_{\underline{n}}$ is Bass for all $\underline{n}=(n_1,n_2)\in\breve{\mathbb{N}}^2$. But the same cannot be said for $\underline{n}\in\breve{\mathbb{N}}^r$ with $r\geq 3$ since $A_{(1,2,4)}=\mathbb{Z}[T]/(T^4-1)$ already provides a counterexample.

for any $\mathscr{A}_{\underline{n}}$-lattice $\Lambda \subset V$. Recall that $h(A_{\underline{n}}) = h(O_{K_{\underline{n}}}) = 1$ by (5.7). Therefore, when $\underline{n} = (3, 6)$, $p \equiv 2 \pmod 3$ and $p \neq 2$, we have

$$o(\underline{n}) = |\mathscr{L}_2(\underline{n})| \cdot |\mathscr{L}_p(\underline{n})| = 2 \cdot 4 = 2\left(1 - \left(\frac{-3}{p}\right)\right)^2. \qquad \square$$

Now suppose that $\underline{n} = (1, 2)$. Then $K_{\underline{n}} = \mathbb{Q} \times \mathbb{Q}$, and $A_{\underline{n}}$ is the unique suborder of index 2 in $O_{K_{\underline{n}}} = \mathbb{Z} \times \mathbb{Z}$. To write down the formula for $o(1, 2)$, we define a few auxiliary orders. Let $\mathbb{O}_1(1, 2) := \mathcal{O} \times \mathcal{O}$, a maximal order in $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = D \times D$. Fix an isomorphism $\mathcal{O}_2 \simeq \mathrm{Mat}_2(\mathbb{Z}_2)$, and thereupon an isomorphism

$$\mathbb{O}_1(1, 2)_2 = (\mathcal{O} \times \mathcal{O}) \otimes \mathbb{Z}_2 \simeq \mathrm{Mat}_2(\mathbb{Z}_2 \times \mathbb{Z}_2) = \mathrm{Mat}_2(O_{K_{\underline{n},2}}).$$

Let $\mathbb{O}_8(1, 2)$ and $\mathbb{O}_{16}(1, 2)$ be the suborders of $\mathbb{O}_1(1, 2)$ index 8 and 16 respectively such that

$$\begin{aligned} &\mathbb{O}_8(1,2)_2 = \begin{pmatrix} A_{\underline{n},2} & 2O_{K_{\underline{n},2}} \\ O_{K_{\underline{n},2}} & O_{K_{\underline{n},2}} \end{pmatrix}, \qquad \mathbb{O}_{16}(1,2)_2 = \mathrm{Mat}_2(A_{\underline{n},2}); \\ &\mathbb{O}_i(1,2)_{\ell'} = \mathbb{O}_1(1,2)_{\ell'} \qquad \forall \text{ prime } \ell' \neq 2 \text{ and } i = 8, 16. \end{aligned} \tag{5.12}$$

Proposition 5.4. *If $p = 3$, then $o(1, 2) = 3$. For $p \neq 2, 3$, we have*

$$\begin{aligned} o(1,2) =& h(\mathbb{O}_1(1,2)) + h(\mathbb{O}_8(1,2)) + h(\mathbb{O}_{16}(1,2)) \\ =& \frac{(p-1)^2}{9} + \frac{p+15}{18}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{p+2}{6}\left(1 - \left(\frac{-4}{p}\right)\right) \\ &+ \frac{1}{6}\left(1 - \left(\frac{-3}{p}\right)\right)\left(1 - \left(\frac{-4}{p}\right)\right). \end{aligned} \tag{5.13}$$

Proof. Throughout this proof, we assume that $p \neq 2$. By (5.10), V_2' is a free $K_{\underline{n},2}$-module of rank 2. Any $A_{\underline{n},2}$-lattice $\Lambda_2' \subseteq V_2'$ is isomorphic to $A_{\underline{n},2}^j \oplus (O_{K_{\underline{n},2}})^{2-j}$ with $j = 0, 1, 2$. Correspondingly, the endomorphism ring $\mathrm{End}_{A_{\underline{n},2}}(\Lambda_2')$ is isomorphic to

$$\mathbb{O}_1(1,2)_2, \qquad \mathbb{O}_8(1,2)_2, \qquad \mathbb{O}_{16}(1,2)_2.$$

Since $|\mathscr{L}_p(\underline{n})| = 1$ by Proposition 5.1, there are three genera of $\mathscr{A}_{\underline{n}}$-lattices in V. Each is represented by a lattice with endomorphism ring $\mathbb{O}_i(1, 2)$ for $i \in \{1, 8, 16\}$, respectively. It follows that

$$o(1,2) = h(\mathbb{O}_1(1,2)) + h(\mathbb{O}_8(1,2)) + h(\mathbb{O}_{16}(1,2)). \tag{5.14}$$

The class numbers $h(\mathbb{O}_8(1, 2))$ is given by (6.6). If $p = 3$, then $h(\mathbb{O}_{16}(1, 2)) = 1$ by Remark 6.6, otherwise $h(\mathbb{O}_{16}(1, 2))$ is give by (6.12). Lastly, we have $h(\mathbb{O}_1(1, 2)) = h(\mathcal{O})^2$. The explicit formula for $o(1, 2)$ follows from (5.14). $\square$

Finally, we study the terms $o(2, 2s)$ for $s \in \{2, 3\}$. We have $[O_{K_{\underline{n}}} : A_{\underline{n}}] = s$, and $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = D \times K_{2s}$ by (5.2). Let $\mathbb{O}_1(2, 2s)$ be the maximal order $\mathcal{O} \times A_{2s} \subset \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$. Recall that $p \neq s$ by our assumption, so we fix an isomorphism $\mathcal{O}_s \simeq \mathrm{Mat}_2(\mathbb{Z}_s)$. By an abuse of notation, we still write $\mathfrak{p}_s$ for the unique prime ideal of $A_{2s,s}$ above s. Let $\mathbb{O}_{s^2}(2, 2s)$ be the suborder of index s^2 in $\mathbb{O}_1(2, 2s)$ such that

$$\begin{aligned} &\mathbb{O}_{s^2}(2,2s)_s = \left\{ \left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, b \right) \in \mathbb{O}_1(2,2s)_s \,\middle|\, \begin{matrix} a_{21} \equiv 0 \pmod s \\ (a_{22} \bmod s) \equiv (b \bmod \mathfrak{p}_s) \end{matrix} \right\}; \\ &\mathbb{O}_{s^2}(2,2s)_{\ell'} = \mathbb{O}_1(2,2s)_{\ell'} \qquad \forall \text{ prime } \ell' \neq s. \end{aligned} \tag{5.15}$$

Proposition 5.5. *Suppose that $s \in \{2,3\}$ and p satisfies the corresponding condition for $\underline{n} = (2,2s)$ in Table 1. Then $o(2,2s) = 2h(\mathbb{O}_1(s,2s)) + 2h(\mathbb{O}_{s^2}(2,2s))$. More explicitly,*

$$\begin{aligned} o(2,4) &= \left(\frac{p+3}{3} - \frac{1}{3}\left(\frac{-3}{p}\right)\right)\left(1-\left(\frac{-4}{p}\right)\right) \qquad \text{if } p \neq 2; \\ o(2,6) &= \left(\frac{5p+18}{12} + \frac{1}{3}\left(\frac{-3}{p}\right) - \frac{1}{4}\left(\frac{-4}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right) \qquad \text{if } p \neq 3. \end{aligned}$$

Proof. For the explicit formulas for $o(2,4)$ and $o(2,6)$, only the cases that p satisfies the corresponding condition in Table 1 is nontrivial and need a proof.

Let $V_s' = \mathbb{Q}_s^2 \times K_{2s,s} = \mathbb{Q}_s \oplus K_{\underline{n},s}$ be the module over $K_{\underline{n},s} = \mathbb{Q}_s \times K_{2s,s}$ in (5.10). We claim that any $A_{\underline{n},s}$-lattice $\Lambda_s' \subset V_s'$ is isomorphic to $\Sigma_0 := \mathbb{Z}_s \oplus O_{K_{\underline{n},s}}$ or $\Sigma := \mathbb{Z}_s \oplus A_{\underline{n},s}$.

Without lose of generality, we may assume that

$$O_{K_{\underline{n},s}} \cdot \Lambda_s' = \mathbb{Z}_s^2 \oplus A_{2s,s} = \mathbb{Z}_s \oplus O_{K_{\underline{n},s}} = \Sigma_0. \tag{5.16}$$

By (5.5), the Jacobson radical $\mathfrak{J}_s = s\mathbb{Z}_s \times \mathfrak{p}_s$ of $O_{K_{\underline{n},s}}$ is contained in $A_{\underline{n},s}$, and thus coincides with the Jacobson radical of $A_{\underline{n},s}$. The quotient $A_{\underline{n},s}/\mathfrak{J}_s \simeq \mathbb{F}_s$ embeds diagonally into $O_{K_{\underline{n},s}}/\mathfrak{J}_s \simeq \mathbb{F}_s \times \mathbb{F}_s$. We have

(i) $\mathfrak{J}_s\Sigma_0 \subset \Lambda_s'$;
(ii) the $\mathbb{F}_s$-vector space $\bar{\Lambda}_s' := \Lambda_s'/\mathfrak{J}_s\Sigma_0$ generates the $\mathbb{F}_s \times \mathbb{F}_s$-module $\bar{\Sigma}_0 := \Sigma_0/\mathfrak{J}_s\Sigma_0 \simeq \mathbb{F}_s^2 \times \mathbb{F}_s$.

In particular, $\dim_{\mathbb{F}_s} \bar{\Lambda}_s' \geq 2$ since $\bar{\Lambda}_s'$ projects surjectively onto both factors $\mathbb{F}_s^2$ and $\mathbb{F}_s$ of $\bar{\Sigma}_0$. By Nakayama's lemma, the association $\Lambda_s' \mapsto \bar{\Lambda}_s'$ establishes a one-to-one correspondence between the set of $A_{\underline{n},s}$-sublattices of Σ_0 satisfying (5.16) and the set of $\mathbb{F}_s$-subspaces of $\bar{\Sigma}_0$ satisfying property (ii) above. Two $A_{\underline{n},s}$-sublattices Λ_s' and Λ_s'' of Σ_0 satisfying (5.16) are isomorphic if and only if there exists

$$g \in \mathrm{End}_{O_{K_{\underline{n},s}}}(\Sigma_0)^\times = \mathrm{GL}_2(\mathbb{Z}_s) \times A_{2s,s}^\times$$

such that $\Lambda_s' g = \Lambda_s''$. In light of the correspondence above, $\Lambda_s' \simeq \Lambda_s''$ if and only if there exists $\bar{g} \in \mathrm{End}_{\mathbb{F}_s \times \mathbb{F}_s}(\bar{\Sigma}_0)^\times = \mathrm{GL}_2(\mathbb{F}_s) \times \mathbb{F}_s^\times$ such that $\bar{\Lambda}_s'\bar{g} = \bar{\Lambda}_s''$. There are two cases to consider:

- if $\dim_{\mathbb{F}_s} \bar{\Lambda}_s' = 3$, then $\bar{\Lambda}_s' = \bar{\Sigma}_0$, and hence $\Lambda_s' = \Sigma_0$;
- if $\dim_{\mathbb{F}_s} \bar{\Lambda}_s' = 2$, then there exists $\bar{g} \in \mathrm{GL}_2(\mathbb{F}_s) \times \mathbb{F}_s^\times$ such that $\bar{\Lambda}_s'\bar{g} = \bar{\Sigma} = \mathbb{F}_s \oplus (A_{\underline{n},s}/\mathfrak{J}_s)$. Therefore, $\Lambda_s' \simeq \Sigma$ in this case.

The claim is verified. Direct calculation shows that

$$\mathrm{End}_{A_{\underline{n},s}}(\Lambda_s') = \begin{cases} \mathbb{O}_1(2,2s)_s & \text{if } \Lambda_s' \simeq \Sigma_0; \\ \mathbb{O}_{s^2}(2,2s)_s & \text{if } \Lambda_s' \simeq \Sigma. \end{cases}$$

The classification at s partitions the set of isomorphism classes of $\mathscr{A}_{\underline{n}}$-lattices $\Lambda \subset V$ into two subsets, according to the local isomorphism classes of Λ_s. Each subset consists of two genera by Proposition 5.1. Taking into account of the maximality of $\mathrm{End}_{\mathscr{A}_{\underline{n},p}}(\Lambda_p)$ for every Λ, we have

$$o(2,2s) = 2h(\mathbb{O}_1(2,2s)) + 2h(\mathbb{O}_{s^2}(2,2s)). \tag{5.17}$$

The class number of $\mathbb{O}_4(2,4)$ and $\mathbb{O}_9(2,6)$ are calculated in Proposition 6.4, and $h(\mathbb{O}_1(2,2s)) = h(\mathcal{O})h(A_{2s}) = h(\mathcal{O})$ for $s \in \{2,3\}$. The explicit formulas for $o(2,4)$ and $o(2,6)$ follow directly. □

Remark 5.6. When $\underline{n} = (2,6)$, $A_{\underline{n}} \simeq A_{(1,3)} = \mathbb{Z}[T]/(T^3-1)$ coincides with the group ring $\mathbb{Z}[C_3]$ for the cyclic group C_3 of order 3. The classification of $A_{\underline{n},3}$-lattices is equivalent to that of $\mathbb{Z}_3$-representations of C_3. Similarly, $A_{(2,4)}$ is a quotient of $\mathbb{Z}[C_4]$. Therefore, one may also apply the result of Heller and Reiner [7] on indecomposable integral representations over cyclic groups of order $\wp^2$ ($\wp \in \mathbb{N}$ a prime) to obtain the claim in Proposition 5.5.

6. Class numbers of certain orders

In this section, we compute the class numbers of the orders $\mathbb{O}_8(1,2), \mathbb{O}_{16}(1,2), \mathbb{O}_4(2,4)$ and $\mathbb{O}_9(2,6)$, defined in (5.12) and (5.15). Throughout this section, the prime p is assumed to satisfy the corresponding condition in Table 1 for $\underline{n} = (1,2),(2,4),(2,6)$ respectively.

First, we recall some properties about ideal classes in more general settings. Let $\mathcal{R} \subset \mathcal{S}$ be two $\mathbb{Z}$-orders in a finite dimensional semisimple $\mathbb{Q}$-algebra $\mathcal{B}$. There is a natural *surjective* map between the sets of locally principal right ideal classes

$$\pi : \mathrm{Cl}(\mathcal{R}) \to \mathrm{Cl}(\mathcal{S}), \qquad [I] \mapsto [I\mathcal{S}].$$

The surjectivity is best seen using the idelic language, where π is given by

$$\pi : \mathcal{B}^\times \backslash \widehat{\mathcal{B}}^\times / \widehat{\mathcal{R}}^\times \to \mathcal{B}^\times \backslash \widehat{\mathcal{B}}^\times / \widehat{\mathcal{S}}^\times, \qquad \mathcal{B}^\times x \widehat{\mathcal{R}}^\times \mapsto \mathcal{B}^\times x \widehat{\mathcal{S}}^\times, \quad \forall x \in \widehat{\mathcal{B}}^\times. \tag{6.1}$$

Let $J \subset \mathcal{B}$ be a locally principal right $\mathcal{S}$-ideal. We study the fiber $\pi^{-1}([J])$. Write $\widehat{J} = x\widehat{\mathcal{S}}$ for some $x \in \widehat{\mathcal{B}}^\times$, and set $\mathcal{S}_J := O_l(J) = \mathcal{B} \cap x\widehat{\mathcal{S}}x^{-1}$, the associated left order of J. By (6.1), we have

$$\pi^{-1}([J]) = \pi^{-1}(\mathcal{B}^\times x \widehat{\mathcal{S}}^\times) = \mathcal{B}^\times \backslash (\mathcal{B}^\times x \widehat{\mathcal{S}}^\times)/\widehat{\mathcal{R}}^\times. \tag{6.2}$$

Multiplying $\mathcal{B}^\times x \widehat{\mathcal{S}}^\times$ from the left by x^{-1} induces a bijection between $\mathcal{B}^\times \backslash (\mathcal{B}^\times x \widehat{\mathcal{S}}^\times)/\widehat{\mathcal{R}}^\times$ and the set

$$(x^{-1}\mathcal{B}^\times x) \backslash (x^{-1}\mathcal{B}^\times x \widehat{\mathcal{S}}^\times)/\widehat{\mathcal{R}}^\times$$

which is in turn isomorphic to $(x^{-1}\mathcal{B}^\times x \cap \widehat{\mathcal{S}}^\times) \backslash \widehat{\mathcal{S}}^\times / \widehat{\mathcal{R}}^\times$. Therefore, we obtain a double coset description of the fiber

$$\pi^{-1}([J]) \simeq (x^{-1}\mathcal{S}_J^\times x) \backslash \widehat{\mathcal{S}}^\times / \widehat{\mathcal{R}}^\times. \tag{6.3}$$

Lemma 6.1. *Suppose that $\widehat{\mathcal{S}}^\times \subseteq \mathcal{N}(\widehat{\mathcal{R}})$, the normalizer of $\widehat{\mathcal{R}}$ in $\widehat{\mathcal{B}}^\times$. Then the suborder $\mathcal{R}_J := x\widehat{\mathcal{R}}x^{-1} \cap \mathcal{B}$ of $\mathcal{S}_J$ is independent of the choice of $x \in \widehat{\mathcal{B}}^\times$ for J, and*

$$|\pi^{-1}([J])| = \frac{[\widehat{\mathcal{S}}^\times : \widehat{\mathcal{R}}^\times]}{[\mathcal{S}_J^\times : \mathcal{R}_J^\times]}.$$

Proof. Suppose that $\widehat{J} = x'\widehat{\mathcal{S}}$ for $x' \in \widehat{\mathcal{B}}^\times$ as well. Then there exists $u \in \widehat{\mathcal{S}}^\times$ such that $x' = xu$. Since $\widehat{\mathcal{S}}^\times \subseteq \mathcal{N}(\widehat{\mathcal{R}})$, we have

$$x'\widehat{\mathcal{R}}x'^{-1} \cap \mathcal{B} = xu\widehat{\mathcal{R}}u^{-1}x^{-1} \cap \mathcal{B} = x\widehat{\mathcal{R}}x^{-1} \cap \mathcal{B} = \mathcal{R}_J \subset \mathcal{S}_J,$$

which proves the independence of $\mathcal{R}_J$ on the choice of x. If I is a locally principal right $\mathcal{R}$-ideal such that $I\mathcal{S} = J$, then $\mathcal{R}_J = O_l(I)$, the associated left order of I. Conjugating by $x \in \widehat{\mathcal{B}}^\times$ on the right hand side of (6.3), we obtain

$$\pi^{-1}([J]) \simeq \mathcal{S}_J^\times \backslash (x\widehat{\mathcal{S}}^\times x^{-1})/(x\widehat{\mathcal{R}}^\times x^{-1}) = \mathcal{S}_J^\times \backslash \widehat{\mathcal{S}}_J^\times / \widehat{\mathcal{R}}_J^\times. \tag{6.4}$$

The assumption $\widehat{\mathcal{S}}^\times \subseteq \mathcal{N}(\widehat{\mathcal{R}})$ also implies that $\widehat{\mathcal{R}}^\times \trianglelefteq \widehat{\mathcal{S}}^\times$, and hence $\widehat{\mathcal{R}}_J^\times \trianglelefteq \widehat{\mathcal{S}}_J^\times$ and $\mathcal{R}_J^\times \trianglelefteq \mathcal{S}_J^\times$. The left action of $S_J^\times$ on the quotient group $\widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times$ factors through $\mathcal{S}_J^\times/\mathcal{R}_J^\times \subseteq \widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times$, and its orbits are the right cosets of $\mathcal{S}_J^\times/\mathcal{R}_J^\times$ in $\widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times$. Thus

$$|\pi^{-1}([J])| = [\widehat{\mathcal{S}}_J^\times : \widehat{\mathcal{R}}_J^\times]/[\mathcal{S}_J^\times : \mathcal{R}_J^\times] = [\widehat{\mathcal{S}}^\times : \widehat{\mathcal{R}}^\times]/[\mathcal{S}_J^\times : \mathcal{R}_J^\times]. \qquad \square$$

Remark 6.2. The condition $\widehat{\mathcal{S}}^\times \subseteq \mathcal{N}(\widehat{\mathcal{R}})$ implies that $\widehat{\mathcal{R}}^\times \trianglelefteq \widehat{\mathcal{S}}^\times$. However, the converse does not hold in general. It is enough to provide a counterexample locally at a prime ℓ, say, $\ell = 2$. Let $\mathcal{S}_2 := \mathrm{Mat}_2(\mathbb{Z}_2)$, and $\mathcal{R}_2 = \begin{pmatrix} \mathbb{Z}_2 & 2\mathbb{Z}_2 \\ 2\mathbb{Z}_2 & \mathbb{Z}_2 \end{pmatrix}$, an Eichler order of level 4 in $\mathcal{S}_2$. Then

$$\mathcal{R}_2^\times = \{x \in \mathrm{Mat}_2(\mathbb{Z}_2) \mid x \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2\mathcal{S}_2}\} \trianglelefteq \mathcal{S}_2^\times = \mathrm{GL}_2(\mathbb{Z}_2).$$

On the other hand, let $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathcal{S}_2^\times$, and $y = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{R}_2$. Then

$$uyu^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix} \notin \mathcal{R}_2.$$

Corollary 6.3. *Keep the notation and assumption of Lemma 6.1. If the natural homomorphism $\mathcal{S}_J^\times \to \widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times$ is surjective for each ideal class $[J] \in \mathrm{Cl}(\mathcal{S})$, then π is bijective.*

Proof. It is enough to show that π is injective. The surjectivity of $\mathcal{S}_J^\times \to \widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times$ implies that the monomorphism $\mathcal{S}_J^\times/\mathcal{R}_J^\times \hookrightarrow \widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times$ is an isomorphism, and hence $|\pi^{-1}([J])| = [\widehat{\mathcal{S}}_J^\times/\widehat{\mathcal{R}}_J^\times : \mathcal{S}_J^\times/\mathcal{R}_J^\times] = 1$. $\square$

Let $D = D_{p,\infty}$ be the unique quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞, and $\mathcal{O} \subset D$ a maximal order in D. Let $s \in \{2, 3\}$, and assume that $p \neq s$. Fix an isomorphism $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_s \simeq \mathrm{Mat}_2(\mathbb{Z}_s)$. We write $\mathcal{O}^{(s)}$ for the Eichler order of level s in $\mathcal{O}$ such that $\mathcal{O}^{(s)} \otimes \mathbb{Z}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$ for every prime $\ell \neq s$, and

$$\mathcal{O}^{(s)} \otimes \mathbb{Z}_s = \begin{bmatrix} \mathbb{Z}_s & \mathbb{Z}_s \\ s\mathbb{Z}_s & \mathbb{Z}_s \end{bmatrix}.$$

The formula for $h(\mathcal{O}^{(s)})$ is given in [11, Theorem 16]:

$$\begin{aligned} h(\mathcal{O}^{(s)}) = &\frac{(p-1)(s+1)}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right)\left(1 + \left(\frac{-3}{s}\right)\right) \\ &+ \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right)\left(1 + \left(\frac{-4}{s}\right)\right), \quad \text{for } s \in \{2,3\} \text{ and } p \neq s. \end{aligned} \tag{6.5}$$

Proposition 6.4. *Suppose that $s \in \{2, 3\}$ and $p \neq s$. Let $\mathbb{O}_{s^2}(2, 2s)$ be the order defined in (5.15). Then*

(a) $h(\mathbb{O}_4(2, 4)) = \frac{1}{4}\left(p - \left(\frac{-4}{p}\right)\right)$ *if $p \neq 2$;*

(b) $h(\mathbb{O}_9(2, 6)) = \frac{1}{3}\left(p - \left(\frac{-3}{p}\right)\right)$ *if $p \neq 3$.*

Proof. For simplicity, we set $\mathbb{O}_{s^2} = \mathbb{O}_{s^2}(2, 2s)$, and define $\mathbb{O}_s := \mathcal{O}^{(s)} \times A_{2s}$, which contains $\mathbb{O}_{s^2}$ and is a suborder of index s in $\mathbb{O}_1(2, 2s) = \mathcal{O} \times A_{2s}$. Recall that $\mathfrak{p}_s$ denotes the unique ramified prime in A_{2s}. We have $A_{2s}/\mathfrak{p}_s = \mathbb{F}_s$, and the canonical map $A_{2s}^\times \to (A_{2s}/\mathfrak{p}_s)^\times = \mathbb{F}_s^\times$ is surjective.

It is straight forward to check that $\widehat{\mathbb{O}}_s^\times \subseteq \mathcal{N}(\widehat{\mathbb{O}}_{s^2})$, and $\widehat{\mathbb{O}}_s^\times/\widehat{\mathbb{O}}_{s^2}^\times \cong \mathbb{F}_s^\times$. Let $Z(\mathbb{O}_s)$ be the center of $\mathbb{O}_s$. Then $Z(\mathbb{O}_s) = \mathbb{Z}\times A_{2s}$, and its unit group $Z(\mathbb{O}_s)^\times = \{\pm 1\}\times A_{2s}^\times$ maps surjectively onto $\widehat{\mathbb{O}}_s^\times/\widehat{\mathbb{O}}_{s^2}^\times$. Since $Z(\mathbb{O}_s) = Z(O_l(J))$ for every locally principal right ideal J of $\mathbb{O}_s$, the assumptions of Corollary 6.3 are satisfied. Therefore,

$$h(\mathbb{O}_{s^2}) = h(\mathbb{O}_s) = h(\mathcal{O}^{(s)})h(A_{2s}) = h(\mathcal{O}^{(s)}), \qquad \text{for } s = 2, 3.$$

Applying formula (6.5), we obtain

$$\begin{aligned} h(\mathbb{O}_4(2,4)) &= h(\mathcal{O}^{(2)}) = \frac{1}{4}\left(p - \left(\frac{-4}{p}\right)\right) && \text{if } p \neq 2; \\ h(\mathbb{O}_9(2,6)) &= h(\mathcal{O}^{(3)}) = \frac{1}{3}\left(p - \left(\frac{-3}{p}\right)\right) && \text{if } p \neq 3. \qquad \square \end{aligned}$$

Next, we assume $p \neq 2$ and calculate the class numbers of the orders $\mathbb{O}_8(1,2)$, $\mathbb{O}_{16}(1,2) \subset D^2$ defined in (5.12). By an abuse of notation, we still write $\mathcal{O}^{(2)}$ for the Eichler order of $\mathcal{O}$ of level 2 such that $\mathcal{O}^{(2)}\otimes\mathbb{Z}_2 = \begin{bmatrix}\mathbb{Z}_2 & 2\mathbb{Z}_2\\ \mathbb{Z}_2 & \mathbb{Z}_2\end{bmatrix}$ and $\mathcal{O}^{(2)}\otimes\mathbb{Z}_\ell = \mathcal{O}\otimes\mathbb{Z}_\ell$ for all $\ell \neq 2$. For simplicity, let $\mathbb{O}_s = \mathbb{O}_s(1,2)$ for $s = 1, 8, 16$, and define $\mathscr{O}_4 := \mathcal{O}^{(2)}\times\mathcal{O}^{(2)}$, which is a suborder of $\mathbb{O}_1$ of index 4 containing $\mathbb{O}_8$. One checks that $\widehat{\mathscr{O}}_4^\times \subseteq \mathcal{N}(\widehat{\mathbb{O}}_8)$, and $\widehat{\mathbb{O}}_8^\times = \widehat{\mathscr{O}}_4^\times$, so the assumptions of Corollary 6.3 are automatically satisfied. We have

$$h(\mathbb{O}_8(1,2)) = h(\mathcal{O}^{(2)}\times\mathcal{O}^{(2)}) = h(\mathcal{O}^{(2)})^2 = \frac{1}{16}\left(p - \left(\frac{-4}{p}\right)\right)^2. \tag{6.6}$$

To calculate the class number of $\mathbb{O}_{16}$, we first note that $2\mathbb{O}_1 \subset \mathbb{O}_{16}$, and the quotient ring $\mathbb{O}_{16}/2\mathbb{O}_1 \cong \mathrm{Mat}_2(\mathbb{F}_2)$ embeds diagonally into $\mathbb{O}_1/2\mathbb{O}_1 \cong \mathrm{Mat}_2(\mathbb{F}_2)^2$. In this case, $\widehat{\mathbb{O}}_{16}^\times$ is *not* normal in $\widehat{\mathbb{O}}_1^\times$, so $\widehat{\mathbb{O}}_1^\times \not\subseteq \mathcal{N}(\widehat{\mathbb{O}}_{16})$.

Consider the natural surjective map $\pi : \mathrm{Cl}(\mathbb{O}_{16}) \to \mathrm{Cl}(\mathbb{O}_1)$. If $[J] \in \mathrm{Cl}(\mathbb{O}_1)$ is a right ideal class of $\mathbb{O}_1$ with $\widehat{J} = x\widehat{\mathbb{O}}_1$ for an element $x \in (\widehat{D}^\times)^2$, then by (6.3) one has a bijection

$$\pi^{-1}([J]) \simeq x^{-1}\mathbb{O}_J^\times x\backslash\widehat{\mathbb{O}}_1^\times/\widehat{\mathbb{O}}_{16}^\times, \quad \text{where} \quad \mathbb{O}_J = O_l(J) = D^2 \cap x\widehat{\mathbb{O}}_1 x^{-1}. \tag{6.7}$$

If $p \neq 2, 3$, then $\mathbb{O}_J^\times \simeq C_{2j_1}\times C_{2j_2}$ for some $1 \leq j_1, j_2 \leq 3$. Here C_n denotes a cyclic group of order n. Given an arbitrary set X, we write $\Delta(X)$ for the diagonal of X^2.

Lemma 6.5. *(1) Let $[J] \in \mathrm{Cl}(\mathbb{O}_1)$ be a right ideal class of $\mathbb{O}_1$. If $\mathbb{O}_J^\times \simeq C_{2j_1}\times C_{2j_2}$, where $1 \leq j_1, j_2 \leq 3$, then there is a bijection $\pi^{-1}([J]) \simeq C_{j_1}\backslash S_3/C_{j_2}$, where S_n denotes the symmetric group of n letters.*

(2) For $1 \leq j_1, j_2 \leq 3$, put $c_{j_1,j_2} := |C_{j_1}\backslash S_3/C_{j_2}|$, whose value is listed in the table below:

c_{j_1,j_2}	1	2	3
1	6	3	2
2	3	2	1
3	2	1	2

Proof. (1) We may regard $C_{2j_1}\times C_{2j_2} = x^{-1}\mathbb{O}_J^\times x$ as a subgroup of $\widehat{\mathbb{O}}_1^\times$. As $1+2\widehat{\mathbb{O}}_1 \subset \widehat{\mathbb{O}}_{16}^\times$, modulo this subgroup, one has $\widehat{\mathbb{O}}_1^\times/\widehat{\mathbb{O}}_{16}^\times \simeq (\mathrm{GL}_2(\mathbb{F}_2)\times\mathrm{GL}_2(\mathbb{F}_2))/\Delta(\mathrm{GL}_2(\mathbb{F}_2))$. For any unit $\zeta \in \mathcal{O}^\times$, we have either $\zeta^4 = 1$ or $\zeta^6 = 1$, and $\mathbb{Z}[\zeta]$ coincides with the ring of integers of $\mathbb{Q}(\zeta)$. By a lemma of Serre, if ζ is a root of unity which is congruent to 1 modulo 2, then $\zeta = \pm 1$. Thus, for $1 \leq j \leq 3$, the map $C_{2j} \to$

$\mathrm{GL}_2(\mathbb{F}_2)$ factors through an embedding $C_j \simeq (C_{2j}/C_2) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_2)$. Note that $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. Since cyclic subgroups of order j of S_3 are conjugate, the double coset space $(C_{j_1} \times C_{j_2})\backslash(S_3 \times S_3)/\Delta(S_3)$ does not depend on how C_j embeds into S_3. Every element of $(S_3 \times S_3)/\Delta(S_3)$ is represented by a unique $(a, 1)$ with $a \in S_3$. For $(c_1, c_2) \in C_{j_1} \times C_{j_2}$, one has $(c_1, c_2) \cdot (a, 1) = (c_1 s, c_2) \sim (c_1 a c_2^{-1}, 1)$. The map $(a, 1) \mapsto a$ yields a bijection $(C_{j_1} \times C_{j_2})\backslash(S_3 \times S_3)/\Delta(S_3) \simeq C_{j_1}\backslash S_3/C_{j_2}$. Therefore, there is a bijection

$$\pi^{-1}([J]) \simeq (C_{j_1} \times C_{j_2})\backslash \mathrm{GL}_2(\mathbb{F}_2)^2/\Delta(\mathrm{GL}_2(\mathbb{F}_2)) \simeq C_{j_1}\backslash S_3/C_{j_2}.$$

(2) This is clear if one of j_i is 1 or 3 as C_3 is a normal subgroup of S_3. To see $c_{2,2} = 2$, one may view C_2 as a Borel subgroup of $S_3 = \mathrm{GL}_2(\mathbb{F}_2)$ and this follows from the Bruhat decomposition. □

Remark 6.6. Suppose that $p = 3$. By [16, Proposition V.3.1], we have $h(\mathcal{O}) = 1$, and $\mathcal{O}^\times/\{\pm 1\} \simeq S_3$. It follows that $h(\mathbb{O}_1) = h(\mathcal{O})^2 = 1$, and hence $\mathrm{Cl}(\mathbb{O}_{16}) = \pi^{-1}([\mathbb{O}_1]) \simeq \mathbb{O}_1^\times\backslash\widehat{\mathbb{O}}_1^\times/\widehat{\mathbb{O}}_{16}^\times$ by (6.3). The same line of argument as that of part (1) of Lemma 6.5 shows that $h(\mathbb{O}_{16}) = |(S_3)^2\backslash(S_3)^2/\Delta(S_3)| = 1$.

Now assume that $p \neq 2, 3$. For $n = 1, 2, 3$, put

$$\mathrm{Cl}_n(\mathcal{O}) := \{[I] \in \mathrm{Cl}(\mathcal{O}) \mid O_l(I)^\times \simeq C_{2n}\}, \quad \text{and} \quad h_n = h_n(\mathcal{O}) := |\mathrm{Cl}_n(\mathcal{O})|. \tag{6.8}$$

By [16, Proposition V.3.2], if $p \neq 2, 3$, then

$$h_2(\mathcal{O}) = \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right), \quad h_3(\mathcal{O}) = \frac{1}{2}\left(1 - \left(\frac{-3}{p}\right)\right), \tag{6.9}$$

$$\begin{aligned} h_1(\mathcal{O}) &= h(\mathcal{O}) - h_2(\mathcal{O}) - h_3(\mathcal{O}) \\ &= \frac{p-1}{12} - \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) - \frac{1}{6}\left(1 - \left(\frac{-3}{p}\right)\right). \end{aligned} \tag{6.10}$$

Since there are $h_{j_1} h_{j_2}$ classes $[J] \in \mathrm{Cl}(\mathbb{O}_1)$ with $\mathbb{O}_J^\times \simeq C_{2j_1} \times C_{2j_2}$, we obtain

$$h(\mathbb{O}_{16}) = \sum_{1 \le j_1, j_2 \le 3} h_{j_1} h_{j_2} c_{j_1, j_2}. \tag{6.11}$$

Observe that

$$c_{j_1,j_2} = \begin{cases} \frac{6}{j_1 j_2} & \text{if } (j_1, j_2) \neq (2,2) \text{ or } (j_1, j_2) \neq (3,3); \\ \frac{6}{j_1 j_2} + \frac{1}{2} & \text{for } (j_1, j_2) = (2,2); \\ \frac{6}{j_1 j_2} + \frac{4}{3} & \text{for } (j_1, j_2) = (3,3). \end{cases}$$

We can express (6.11) as

(6.12)

$$\begin{aligned} h(\mathbb{O}_{16}(1,2)) &= \sum_{1 \le j_1, j_2 \le 3} h_{j_1} h_{j_2} \frac{6}{j_1 j_2} + \frac{1}{2} h_2^2 + \frac{4}{3} h_3^2 \\ &= 6\left(h_1 + \frac{h_2}{2} + \frac{h_3}{3}\right)^2 + \frac{1}{8}\left(1 - \left(\frac{-4}{p}\right)\right)^2 + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right)^2 \\ &= \frac{(p-1)^2}{24} + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{2}{3}\left(1 - \left(\frac{-3}{p}\right)\right) \quad \text{for } p \neq 2, 3. \end{aligned}$$

Acknowledgments

J. Xue is partially supported by the 1000-plan program for young talents and Natural Science Foundation grant #11601395 of PRC. He thanks Academia Sinica and NCTS for their hospitality and great working conditions. TC Yang and CF Yu are partially supported by the grants MoST 104-2115-M-001-001MY3, 104-2811-M-001-066 and 105-2811-M-001-108.

References

[1] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[2] 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.

[3] M. Eichler. über die Idealklassenzahl hyperkomplexer Systeme. *Math. Z.*, 43(1):481–494, 1938.

[4] Benson Farb and R. Keith Dennis. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[5] Tamar Friedmann and Richard P. Stanley. Counting conjugacy classes of elements of finite order in Lie groups. *European J. Combin.*, 36:86–96, 2014.

[6] Ki-ichiro Hashimoto. A formula for the number of semisimple conjugacy classes in the arithmetic subgroups. *Proc. Japan Acad. Ser. A Math. Sci.*, 61(2):48–50, 1985.

[7] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers. I. *Ann. of Math. (2)*, 76:73–92, 1962.

[8] V. Karemaker and R. Pries. Fully maximal and fully minimal abelian varieties. *ArXiv e-prints*, March 2017, `arXiv:1703.10076`.

[9] R. P. Langlands. Stable conjugacy: definitions and lemmas. *Canad. J. Math.*, 31(4):700–725, 1979.

[10] Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998.

[11] Arnold Pizer. On the arithmetic of quaternion algebras. *Acta Arith.*, 31(1):61–89, 1976.

[12] Florian Pop and Horia Pop. An extension of the Noether-Skolem theorem. *J. Pure Appl. Algebra*, 35(3):321–328, 1985.

[13] 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.

[14] T. A. Springer and R. Steinberg. Conjugacy classes. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 167–266. Springer, Berlin, 1970.

[15] Richard G. Swan. Torsion free cancellation over orders. *Illinois J. Math.*, 32(3):329–360, 1988.

[16] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[17] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[18] J. Xue and C.-F. Yu. Counting abelian varieties over finite fields. *ArXiv e-prints*, January 2018, `arXiv:1801.00229`.

[19] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Supersingular abelian surfaces and Eichler class number formula. *ArXiv e-prints*, April 2014, `arXiv:1404.2978`.

[20] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Numerical invariants of totally imaginary quadratic $\mathbb{Z}[\sqrt{p}]$-orders. *Taiwanese J. Math.*, 20(4):723–741, 2016.

[21] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. On superspecial abelian surfaces over finite fields. *Doc. Math.*, 21:1607–1643, 2016.

[22] Jiangwei Xue, Chia-Fu Yu, and Yuqiang Zheng. On superspecial abelian surfaces over finite fields III. In preparation.

[23] Chia-Fu Yu. Superspecial abelian varieties over finite prime fields. *J. Pure Appl. Algebra*, 216(6):1418–1427, 2012.

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

(Xue) Hubei Key Laboratory of Computational Science (Wuhan University), 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, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN.
E-mail address: chiafu@math.sinica.edu.tw

(Yu) National Center for Theoretical Sciences, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN.
E-mail address: chiafu@math.sinica.edu.tw