J. Math. Soc. Japan
Vol. 72, No. 1 (2020) pp. 303–331
doi: 10.2969/jmsj/81438143

On superspecial abelian surfaces over finite fields II

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

(Received Oct. 9, 2018)

Abstract. Extending the results of the current authors [Doc. Math., **21** (2016), 1607–1643] and [Asian J. Math. to appear, arXiv:1404.2978], we calculated explicitly the number of isomorphism classes of superspecial abelian surfaces over an arbitrary finite field of *odd* degree over the prime field $\mathbb{F}_p$. A key step was to reduce the calculation to the prime field case, and we calculated the number of isomorphism classes in each isogeny class through a concrete lattice description. In the present paper we treat the *even* degree case by a different method. We first translate the problem by Galois cohomology into a seemingly unrelated problem of computing conjugacy classes of elements of finite order in arithmetic subgroups, which is of independent interest. We then explain how to calculate the number of these classes for the arithmetic subgroups concerned, and complete the computation in the case of rank two. This complements our earlier results and completes the explicit calculation of superspecial abelian surfaces over finite fields.

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[1], 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 an arbitrary 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. Explicit calculations for supersingular abelian surfaces are certainly more complicated. However, if all supersingular cases are understood, then we would have very good understanding of all abelian surfaces over finite fields, because the cases of ordinary and almost ordinary (simple) abelian surfaces are simpler and have been studied by Waterhouse [**24**]. That would

2010 *Mathematics Subject Classification.* Primary 11R52; Secondary 11G10.

Key Words and Phrases. superspecial abelian surfaces, explicit formulas, conjugacy classes of arithmetic subgroups.

The first author is partially supported by the Natural Science Foundation of China grant #11601395. The second and third authors are partially supported by the MoST grants 104-2115-M-001-001MY3, 104-2811-M-001-066, 105-2811-M-001-108 and 107-2115-M-001-001-MY2.

[1]This is well known when the ground field k is algebraically closed, and is proved in [**32**] for arbitrary k.

improve our knowledge from $d = 1$ (elliptic curves by Deuring in the 1940's) to $d = 2$ (abelian surfaces).

In [**27**] we calculated explicitly the number of superspecial abelian surfaces over an arbitrary finite field $\mathbb{F}_q$ of *odd* degree over $\mathbb{F}_p$. This extended our earlier works [**25**], [**26**] and [**31**], which 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 an explicit calculation of superspecial abelian surfaces over an arbitrary finite field.

A key step in [**27**] 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 $\mathbb{F}_q$ is of odd degree over $\mathbb{F}_p$ because we have a natural concrete lattice description for abelian varieties over $\mathbb{F}_p$ (see [**31**, Theorem 3.1]). When the degree $[\mathbb{F}_q : \mathbb{F}_p]$ is even, the Galois cohomology argument unfortunately yields no immediate simplification. However, it leads to a seemingly unrelated problem, which is important but also equally challenging, on counting conjugacy classes of elements of finite order in arithmetic subgroups. Although the connection itself is straightforward, it is applicable to a rather 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 group elements of finite order. Let $D = D_{p,\infty}$ be the definite quaternion $\mathbb{Q}$-algebra ramified exactly at p and ∞, and $\mathcal{O}$ be a maximal order in D.

Proposition 1.1. *Let $\mathbb{F}_q$ be a finite field containing $\mathbb{F}_{p^2}$, and $d > 1$ be an integer. 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 $\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$.*

By a classical result of Eichler [**7**], if $d > 1$, then the class number of $\mathrm{Mat}_d(\mathcal{O})$ is equal to one, where $\mathrm{Mat}_d(\mathcal{O})$ denotes the ring of $d \times d$ matrices over $\mathcal{O}$. Thus, for $d \geq 2$, 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 hence Proposition 1.1 does not depend on the choice of the maximal order $\mathcal{O}$. We prove the following explicit formula (see Theorem 3.4).

Theorem 1.2. *The cardinality of $\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))$ is equal to*

$$\begin{aligned}
&2 + \left[4 - 2\left(\frac{-3}{p}\right)\right] + \left[2 - \left(\frac{-4}{p}\right)\right] \\
&\quad + 2\left(1 - \left(\frac{-3}{p}\right)\right)\left(\frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right)\right) \\
&\quad + 2\left(\frac{p+3}{3} - \frac{1}{3}\left(\frac{-3}{p}\right)\right)\left(1 - \left(\frac{-4}{p}\right)\right) \\
&\quad + 2\left(\frac{5p+18}{12} + \frac{1}{3}\left(\frac{-3}{p}\right) - \frac{1}{4}\left(\frac{-4}{p}\right)\right)\left(1 - \left(\frac{-3}{p}\right)\right) \\
&\quad + 2\left(1 - \left(\frac{-3}{p}\right)\right)\left(1 - \left(\frac{-4}{p}\right)\right)
\end{aligned}$$

$$+2\left(1-\left(\frac{-3}{p}\right)\right)^2+2o(5)+o(8)+o(12)+o(1,2), \tag{1.1}$$

where

$$o(5)=\begin{cases}1 & \text{if } p=5;\\ 0 & \text{if } p\equiv 1 \pmod 5;\\ 2 & \text{if } p\equiv 2,3 \pmod 5;\\ 4 & \text{if } p\equiv 4 \pmod 5;\end{cases}$$

$$o(8)=\begin{cases}1 & \text{if } p=2;\\ 0 & \text{if } p\equiv 1 \pmod 8;\\ 4 & \text{if } p\equiv 3,5,7 \pmod 8;\end{cases}$$

$$o(12)=\begin{cases}3 & \text{if } p=2,3;\\ 0 & \text{if } p\equiv 1 \pmod{12};\\ 4 & \text{if } p\equiv 5,7,11 \pmod{12};\end{cases}$$

$$o(1,2)=\begin{cases}3 & \text{if } p=3;\\ \dfrac{(p-1)^2}{9}+\dfrac{p+15}{18}\left(1-\left(\dfrac{-3}{p}\right)\right)+\dfrac{p+2}{6}\left(1-\left(\dfrac{-4}{p}\right)\right) & \\ \qquad +\dfrac{1}{6}\left(1-\left(\dfrac{-3}{p}\right)\right)\left(1-\left(\dfrac{-4}{p}\right)\right) & \text{if } p\neq 3.\end{cases}$$

The number $o(n)$ or $o(n_1,n_2)$ is defined in (3.7) (see also Section 3.2), which is the cardinality of a subset of $\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))$. Combining with Proposition 1.1, we obtain an explicit formula for the number of superspecial abelian surfaces over $\mathbb{F}_q\supseteq\mathbb{F}_{p^2}$. By Theorem 1.2, we see that the main term of $|\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))|$ is $o(1,2)$ and obtain the asymptotic behavior of $|\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))|$:

$$\frac{|\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))|}{p^2/9}\longrightarrow 1,\quad \text{as } p\to\infty. \tag{1.2}$$

In fact, the method we use for computing $\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))$ also provides a way of finding structures of $\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$ for higher d; see Section 3.1. However, as d increases, it becomes a daunting or even hopeless task to carry out similar computations as in the proof of Theorem 1.2 for $d=2$. Nevertheless, it is an interesting question to figure out the main term and error terms of $|\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))|$ as d or p varies. Thanks to a finiteness result of Borel (see Theorem 2.2), it also makes sense to ask the similar questions for more general arithmetic subgroups.

This paper is organized as follows. In Section 2, we give a proof of Proposition 1.1. Section 3 describes our main results in details. The remaining part of this paper fills in the details of the computation in Theorem 1.2.

2. Conjugacy classes of elements of finite order.

As in the introduction, for any group G, we denote by $\mathrm{Cl}(G)$ the set of conjugacy classes of G, and by $\mathrm{Cl}_0(G) \subset \mathrm{Cl}(G)$ the subset of classes of elements of finite order in G. In this section we reduce the computation of the number of d-dimensional superspecial abelian varieties to that of $\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))$ (Proposition 1.1). Then we study the finiteness of $\mathrm{Cl}_0(G)$ for a certain special type of groups G. The latter part is of independent interest, and will not be used in the rest of this paper.

2.1. 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 $X \otimes_k k_s \simeq X_0 \otimes_k k_s$. A well-known result due to Weil states that there is a natural bijection $\Sigma(X_0, k_s/k) \xrightarrow{\sim} H^1(\Gamma_k, G)$ of pointed sets, where $G = \mathrm{Aut}_{k_s}(X_0) := \mathrm{Aut}_{k_s}(X_0 \otimes_k k_s)$ is the group of automorphisms of $X_0 \otimes_k k_s$ over k_s, equipped with the discrete topology and a continuous Γ_k-action. If Γ_k acts trivially on $\mathrm{Aut}_{k_s}(X_0)$, namely the natural inclusion $\mathrm{Aut}(X_0) \hookrightarrow \mathrm{Aut}_{k_s}(X_0)$ is bijective, then $H^1(\Gamma_k, G) = \mathrm{Hom}(\Gamma_k, G)/G$, where G acts on the set $\mathrm{Hom}(\Gamma_k, G)$ of continuous homomorphisms by conjugation. In addition, if Γ_k is isomorphic to the profinite group $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$, one obtains a natural bijection of pointed sets:

$$\Sigma(X_0, k_s/k) \xrightarrow{\sim} \mathrm{Cl}_0(G), \quad G = \mathrm{Aut}(X_0). \tag{2.1}$$

Let X be an abelian variety over k and k'/k be a field extension. Denote by $\mathrm{End}_{k'}(X) = \mathrm{End}_{k'}(X \otimes_k k')$ the endomorphism ring of $X \otimes_k k'$ over k'; we also write $\mathrm{End}(X)$ for $\mathrm{End}_k(X)$. The endomorphism algebra of $X \otimes_k k'$ is defined to be $\mathrm{End}(X \otimes_k k') \otimes_{\mathbb{Z}} \mathbb{Q}$ and denoted by $\mathrm{End}^0_{k'}(X)$. Applying Weil's result to abelian varieties over finite fields, one obtains the following proposition.

Proposition 2.1. *Let X_0 be an abelian variety over a finite field $\mathbb{F}_q$ such that the endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_q}(X_0)$ 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 2.1 is an arithmetic subgroup of the reductive group $\underline{G}$ over $\mathbb{Q}$ such that $\underline{G}(R) = (\mathrm{End}^0(X_0) \otimes_{\mathbb{Q}} R)^\times$ for any $\mathbb{Q}$-algebra R.

Proof of Proposition 1.1. We choose a 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 2.1, 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 [**13**, Section 1.6, p.13]. Thus, $\Sigma(X_0, k_s/k)$ classifies the d-dimensional superspecial abelian varieties over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism. This completes the proof of the proposition. □

2.2. Finiteness of $\mathrm{Cl}_0(G)$ for some groups G.

We take the opportunity to discuss the finiteness of $\mathrm{Cl}_0(G)$ for a group G that is of the form $H(F)$ for a reductive group H over a global or local field F, or an arithmetic subgroup of $H(F)$ for a global field F. The following is a fundamental result due to Borel; see [**4**, Section 5].

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 the 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.*

We could not find the reference for a similar result of Theorem 2.2 under the condition that F is a global function field.

PROPOSITION 2.3. (1) *Suppose G is a linear algebraic group over a non-archimedean local field F of characteristic zero. Then $\mathrm{Cl}_0(G(F))$ is finite.*

(2) *Let G be a linear algebraic group over $\mathbb{R}$. Then the set $\mathrm{Cl}_0(G(\mathbb{R}))$ is infinite if and only if $G(\mathbb{R})$ contains a non-trivial compact torus S.*

PROOF. (1) 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. By [**16**, Section 6.4, Corollary 3, p.320], there are only finitely many maximal F-tori up to conjugation by $G(F)$. Therefore, one reduces the statement to the case where $G = T$ is a torus. Choose a finite extension K of F over which T splits. Then 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 $T(F)_{\mathrm{tors}} = \mathrm{Cl}_0(T(F))$ is finite.

(2) Suppose that every $\mathbb{R}$-torus T of G is split. Then we use the argument in (1) to prove that $\mathrm{Cl}_0(G(\mathbb{R}))$ is finite, because for a split torus T, the set $\mathrm{Cl}_0(T(\mathbb{R})) = T(\mathbb{R})_{\mathrm{tors}}$ is finite. Now we prove the other direction. Suppose that $G(\mathbb{R})$ contains a non-trivial compact torus S. Then for any positive integer n there is an element of order n in S. Since elements of different orders are not conjugate, the set $\mathrm{Cl}_0(G(\mathbb{R}))$ is infinite. This proves the proposition. □

PROPOSITION 2.4. *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 by $\mathrm{Hom}_F^*(F[t]/(t^n-1), A)$ the subset consisting of all 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 over F and $F[t]/(t^n-1)$ is semisimple, an extension of the Noether–Skolem theorem ([**17**, Theorem 2], also see [**30**, Theorem 1.4]) states 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. Note that $\mathrm{Cl}_0(A^\times)$ is the union of $\mathrm{Cl}_0(n, A^\times)$ for all n, and that $\mathrm{Cl}_0(n, A^\times)$ is empty for almost all n, because the degree of $\mathbb{Q}(\zeta_n)$ is unbounded when n goes large, This proves 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 $\mathbb{Q}(\sqrt{-1}\,)$. 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 $g_2 = h g_1 z$ for some elements $h \in \mathrm{SL}_2(\mathbb{Q})$ and $z \in K^\times$. Therefore, we have proved a bijection

$$\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q})) \simeq \mathrm{SL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{Q}) / K^\times. \tag{2.2}$$

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 all 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 2.5. *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, the set* $\mathrm{Cl}_0(4, \mathrm{SL}_2(\mathbb{Q}))$ *is infinite.*

REMARK 2.6. 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 $\xi_1 = g \xi_2 g^{-1}$. Let G_ξ be the centralizer of $\xi \in G(F)$. Langlands [**12**] 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 $T := \ker\left(\mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_{m,K}) \xrightarrow{\mathrm{N}_{K/\mathbb{Q}}} \mathbb{G}_{m,\mathbb{Q}}\right)$, we recover the result

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

We mention Springer and Steinberg [**20**] and Humphreys [**10**] as important references for conjugacy classes of linear algebraic 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 [**27**, Section 6.4].

As remarked right after Proposition 1.1, $|\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))|$ 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 (see Remark 3.7), and the resulting formula for $H(2, D_{p,\infty})$ is stated in Theorem 3.4. As a convention, $\mathbb{N}$ denotes the set of strictly positive integers, and $\mathbb{Z}_{\geq 0}$ the set of nonnegative ones.

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

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

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 $\breve{\mathbb{N}}^r$. 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).

Let $V = D^d$ be the right D-space of column vectors. The left multiplication of $\mathrm{Mat}_d(D)$ on V induces the identification $\mathrm{Mat}_d(D) = \mathrm{End}_D(V)$. The right scalar action by D on V gives an embedding $D^{\mathrm{opp}} \hookrightarrow \mathrm{End}_{\mathbb{Q}}(V)$ of D^{opp} which commutes with $\mathrm{Mat}_d(D)$, and we have $\mathrm{End}_{\mathbb{Q}}(V) = \mathrm{Mat}_d(D) \otimes D^{\mathrm{opp}}$. Let $M_0 = \mathcal{O}^d \subset V$ be the standard $\mathcal{O}$-lattice in V. Then $\mathrm{End}_{\mathcal{O}}(M_0) = \mathrm{Mat}_d(\mathcal{O}) \subset \mathrm{Mat}_d(D)$. The conjugacy class $[x] \in C(\underline{n})$ equips M_0 with an $(A_{\underline{n}}, \mathcal{O})$-bimodule structure which is faithful as an $A_{\underline{n}}$-module, or equivalently, a faithful left $A_{\underline{n}} \otimes_{\mathbb{Z}} \mathcal{O}^{\mathrm{opp}}$-module structure. Similarly, V is equipped with a faithful left $K_{\underline{n}} \otimes_{\mathbb{Q}} D^{\mathrm{opp}}$-module structure.

For simplicity, we define

$$\mathscr{A}_{\underline{n}} := A_{\underline{n}} \otimes_{\mathbb{Z}} \mathcal{O}^{\mathrm{opp}}, \quad \text{and} \quad \mathscr{K}_{\underline{n}} := K_{\underline{n}} \otimes_{\mathbb{Q}} D^{\mathrm{opp}} = \prod_{i=1}^r K_{n_i} \otimes_{\mathbb{Q}} D^{\mathrm{opp}}. \tag{3.3}$$

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. Let

$$e(n) := \dim_D W_n$$

as a left D^{opp}-space (or equivalently, a right D-space). Note that $e(n)$ is also the smallest $e \in \mathbb{N}$ such that there exists an embedding $K_n \hookrightarrow \mathrm{Mat}_e(D)$.

The decomposition of $\mathscr{K}_{\underline{n}}$ in (3.3) induces a decomposition

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

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 a condition for $(\underline{n}, \underline{m})$:

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

We refer to [**30**, Theorem 1.3] for discussions of the general case where the ground field $\mathbb{Q}$ is replaced by an arbitrary field. The r-tuple $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}^r$ will 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. Let $\mathscr{L}(\underline{n}, \underline{m})$ be the set of isomorphism classes of $\mathscr{A}_{\underline{n}}$-lattices in the left $\mathscr{K}_{\underline{n}}$-module V of type $\underline{m}$. According to the Jordan–Zassenhaus theorem [**6**, Theorem 24.1, p.534], $\mathscr{L}(\underline{n}, \underline{m})$ is a finite set.

LEMMA 3.1. *There is a bijection between $C(\underline{n}, \underline{m})$ and $\mathscr{L}(\underline{n}, \underline{m})$.*

PROOF. As explained above, each conjugacy class $[x] \in C(\underline{n}, \underline{m})$ equips $M_0 = \mathcal{O}^d$ with an $\mathscr{A}_{\underline{n}}$-module structure, thus defines a map from $C(\underline{n}, \underline{m})$ to $\mathscr{L}(\underline{n}, \underline{m})$. Conversely, for any member $[M] \in \mathscr{L}(\underline{n}, \underline{m})$, we regard M as an $(A_{\underline{n}}, \mathcal{O})$-bimodule. Since the class number of $\mathrm{Mat}_d(D)$ is one (as $d > 1$), we have $M \simeq M_0$ as right $\mathcal{O}$-modules. The faithful left $A_{\underline{n}}$-action on M provides an embedding $A_{\underline{n}} \hookrightarrow \mathrm{End}_{\mathcal{O}}(M) \simeq \mathrm{End}_{\mathcal{O}}(M_0) = \mathrm{Mat}_d(\mathcal{O})$, which makes M and M_0 as isomorphic $(A_{\underline{n}}, \mathcal{O})$-bimodules. This shows the surjectivity. Let x, y be two elements of $\mathrm{GL}_d(\mathcal{O})$ such that their conjugacy classes lie in $C(\underline{n}, \underline{m})$. Let M_x (resp. M_y) be the $(A_{\underline{n}}, \mathcal{O})$-bimodule structure on M_0 obtained by the embedding $\varphi_x : A_{\underline{n}} \hookrightarrow \mathrm{Mat}_d(\mathcal{O})$ determined by $\varphi_x(T) = x$ (resp. by $\varphi_y(T) = y$). Then $M_x \simeq M_y$ if and only if there is an $\mathcal{O}$-isomorphism $\alpha : M_0 \xrightarrow{\sim} M_0$ such that $\alpha(\varphi_x(a)m) = \varphi_y(a)\alpha(m)$ for every $a \in A_{\underline{n}}$ and $m \in M_0$. Let $g \in \mathrm{GL}_d(\mathcal{O})$ represent α. Then we have $gx = yg$. This proves the injectivity and hence the lemma. □

Let us denote

$$o(\underline{n}) := |C(\underline{n})| \quad \text{and} \quad o(\underline{n}, \underline{m}) := |C(\underline{n}, \underline{m})| = |\mathscr{L}(\underline{n}, \underline{m})|. \tag{3.7}$$

It follows from (3.6) that

$$H(d, D) = |\mathrm{Cl}_0(\mathrm{GL}_d(\mathcal{O}))| = \sum_{\underline{n}} o(\underline{n}) = \sum_{(\underline{n},\underline{m})} o(\underline{n}, \underline{m}). \tag{3.8}$$

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 $g \in \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)^\times \subset \mathrm{GL}_d(D)$ such that $\Lambda_1 = g\Lambda_2$. Clearly,

$$\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = \prod_{i=1}^{r} \mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}), \text{ and } \mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}) \sim K_{n_i} \otimes_{\mathbb{Q}} D, \tag{3.9}$$

where $\sim$ denotes the Brauer equivalence of central simple algebras. On the other hand, the algebra $\mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i})$ is the centralizer of K_{n_i} in $\mathrm{End}_D(V_{n_i})$. So by the centralizer theorem [**8**, Theorem 3.15],

$$[K_{n_i} : \mathbb{Q}]^2 \, [\mathrm{End}_{\mathscr{K}_{n_i}}(V_{n_i}) : K_{n_i}] = [\mathrm{End}_D(V_{n_i}) : \mathbb{Q}] = [D : \mathbb{Q}](m_i e(n_i))^2. \tag{3.10}$$

The structure of $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$ is completely determined by (3.9) and (3.10).

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

$$\Psi : \mathscr{L}(\underline{n},\underline{m}) \to \prod_\ell \mathscr{L}_\ell(\underline{n},\underline{m}). \tag{3.11}$$

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 [**6**, Theorem 26.24]. So the right hand side of (3.11) is essentially a finite product. Two lattices Λ_1 and Λ_2 are said to be in the same *genus* if $\Psi([\Lambda_1]) = \Psi([\Lambda_2])$, that is, if they are locally isomorphic at every prime ℓ. The fibers of Ψ partition $\mathscr{L}(\underline{n},\underline{m})$ into a disjoint union of genera. More explicitly, for each element $\mathbb{L} = (\mathbb{L}_\ell)_\ell \in \prod_\ell \mathscr{L}_\ell(\underline{n},\underline{m})$, let

$$\mathscr{L}(\underline{n},\underline{m},\mathbb{L}) := \Psi^{-1}(\mathbb{L}) = \{[\Lambda] \in \mathscr{L}(\underline{n},\underline{m}) \mid [\Lambda_\ell] = \mathbb{L}_\ell, \forall \ell\}. \tag{3.12}$$

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 [**21**, Proposition 1.4] that $\mathscr{L}(\underline{n},\underline{m},\mathbb{L})$ is bijective to the set $\mathrm{Cl}(O_\Lambda)$ of locally principal right ideal classes of O_Λ. In particular,

$$|\mathscr{L}(\underline{n},\underline{m},\mathbb{L})| = h(O_\Lambda) := |\,\mathrm{Cl}(O_\Lambda)|. \tag{3.13}$$

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 gives rise to 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 a lattice member and calculate its class number. The sum of all these class numbers is $H(d,D)$.

Remark 3.2. We make a couple of simplifications for the calculations.
(i) The center $Z(\mathrm{GL}_d(\mathcal{O}))=\{\pm1\}$ 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

$$n_i^\ddagger=\begin{cases}2n_i & \text{if } 2\nmid n_i,\\ n_i & \text{if } 4\mid n_i,\\ n_i/2 & \text{otherwise,}\end{cases} \tag{3.14}$$

for each $1\le i\le r$, and then rearranging 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

$$\dim_{\mathbb{Q}}(D^{m_ie(n_i)})/(u[K_{n_i}:\mathbb{Q}])=um_ie(n_i)/\varphi(n_i). \tag{3.15}$$

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, $\mathrm{End}_{\mathscr{A}_{\underline{n},\ell}}(\Lambda_\ell)\cong \mathrm{End}_{A_{\underline{n},\ell}}(\Lambda'_\ell)$. This reduces the classification of lattices over the *non-commutative* order $\mathscr{A}_{\underline{n},\ell}$ to that over the *commutative* order $A_{\underline{n},\ell}$, which is much easier. We make use of this simplification in Section 5; see Table 2.

Remark 3.3. When $D=D_{p,\infty}$, many numerical invariants discussed in this subsection admit natural geometric meanings. Assume that $\mathbb{F}_q$ has even degree $a:=[\mathbb{F}_q:\mathbb{F}_p]$ over its prime field as in Proposition 1.1. Recall that an algebraic integer $\pi\in\overline{Q}$ is said to be a *Weil q-number* if $|\iota(\pi)|=q^{1/2}$ for every embedding $\iota:\mathbb{Q}(\pi)\hookrightarrow\mathbb{C}$. One class of examples is given by $\pi_n:=(-p)^{a/2}\zeta_n$ for $n\in\mathbb{N}$, where ζ_n denotes a primitive n-th root of unity. By the Honda–Tate theorem, there is a unique simple abelian variety X_n over $\mathbb{F}_q$ up to isogeny corresponding to the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy class of π_n. It is known [**27**, Subsection 6.2] that X_n is a supersingular abelian variety of dimension $e(n)$. Fix an integer $d>1$ and let $(\underline{n},\underline{m})\in\breve{\mathbb{N}}^r\times\mathbb{N}^r$ be a d-admissible pair. By [**27**, Proposition 6.11], $o(\underline{n},\underline{m})$ counts the number of $\mathbb{F}_q$-isomorphism classes of d-dimensional *superspecial* abelian varieties over $\mathbb{F}_q$ in the isogeny class of $X_{\underline{n},\underline{m}}:=\prod_{i=1}^r(X_{n_i})^{m_i}$. In particular, r measures the number of $\mathbb{F}_q$-isotypic parts of $X_{\underline{n},\underline{m}}$. By [**27**, Lemma 6.3], we

have $\mathrm{End}^0(X_{\underline{n},\underline{m}}) \simeq \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$, where V is a left $\mathscr{K}_{\underline{n}}$-module of type $\underline{m}$.

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 $e(n) \le 2$ only if $\varphi(n) = [K_n : \mathbb{Q}] \le 4$, 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 $e(n) \ge 2$. We have $e(n) = 2$ if and only if p does *not* split completely in K_n.

Thus we have

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

Note that 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. For brevity, we omit $\underline{m}$ from the notation $\mathscr{L}(\underline{n}, \underline{m})$ and write $\mathscr{L}(\underline{n})$ instead. Similarly, we discuss only the value of $o(\underline{n})$ rather than that of $o(\underline{n}, \underline{m})$. Thus there should be no ambiguity of the notation $o(1, 2)$ for $\underline{n} = (1, 2)$. Using this notation, we have 19 2-admissible elements:

$$\mathcal{T}(1) = \{1, 2, 3, 4, 5, 6, 8, 10, 12\},$$
$$\mathcal{T}(2) = \{(1,2), (1,3), (1,4), (1,6), (2,3), (2,4), (2,6), (3,4), (3,6), (4,6)\}.$$

By Remark 3.2(i), we have

$$o(1) = o(2) = 1,\ o(3) = o(6),\ o(5) = o(10); \tag{3.16}$$
$$o(1,3) = o(2,6),\ o(1,4) = o(2,4),\ o(1,6) = o(2,3),\ o(3,4) = o(4,6). \tag{3.17}$$

Let $q = p^a$ be an *even* power of p. By Remark 3.3, each $o(\underline{n})$ above counts the number of isomorphism classes of superspecial abelian surfaces over $\mathbb{F}_q$ in a supersingular isogeny class over $\mathbb{F}_q$ determined by $\underline{n} \in \breve{\mathbb{N}}^r$. If $r = 1$ so that $\underline{n} = n \in \mathbb{N}$, then the isogeny class is isotypic; it is even simple if $e(n) = 2$. If $r = 2$, then the isogeny class is non-isotypic: every member is $\mathbb{F}_q$-isogenous to a product of two mutually non-isogenous supersingular elliptic curves over $\mathbb{F}_q$.

THEOREM 3.4. *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*

$$\begin{aligned} H(2, D_{p,\infty}) = |\mathrm{Cl}_0(\mathrm{GL}_2(\mathcal{O}))| &= 2 + 2o(3) + o(4) + 2o(5) + o(8) + o(12) \\ &\quad + o(1,2) + 2o(2,3) + 2o(2,4) + 2o(2,6) + 2o(3,4) + o(3,6), \end{aligned} \tag{3.18}$$

where the value of each $o(\underline{n})$ is as follows:

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

Here if $p = 2$, then $(\cdot/2)$ is understood as the Kronecker symbol [**1**, Definition 10.2.1]. That is,

$$\left(\frac{n}{2}\right) = \begin{cases} 0 & \text{if } 2|n; \\ 1 & \text{if } n \equiv 1, 7 \pmod 8; \\ -1 & \text{if } n \equiv 3, 5 \pmod 8. \end{cases}$$

COROLLARY 3.5. *Keeping the notation of Theorem* 3.4*, we have*

$$\lim_{p\to\infty} \frac{H(2, D_{p,\infty})}{p^2/9} = 1. \tag{3.19}$$

PROOF. By Theorem 3.4, 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. □

REMARK 3.6. Karemaker and Pries [**11**, 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 [**11**, Proposition 7.6] that if $p \geq 3$, then the proportion of $\mathbb{F}_{p^t}$-rational points of the supersingular locus $\mathcal{A}_{2,\mathrm{ss}}$ which represent (A, λ) with $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(A, \lambda) \neq \mathbb{Z}/2\mathbb{Z}$ tends to zero as $t \to \infty$. They ask whether or not the majority of principally polarized supersingular abelian surfaces over $\mathbb{F}_{p^t}$ are those with normalized Weil numbers $(1, 1, -1, -1)$. From Theorem 3.4 and [**27**, Theorems 1.1 and 1.2] we see that the proportion of *superspecial* abelian surfaces over $\mathbb{F}_{p^t}$ with normalized Weil numbers $(1, 1, -1, -1)$ (with t fixed) tends to one as $p \to \infty$. However, to deduce a similar result for supersingular abelian surfaces, one could use the argument of [**28**] where we compute the size of the isogeny class corresponding to the Weil number $\sqrt{p^t}$ with odd t.

In the calculations for Theorem 3.4, we make frequent use of *Eichler orders*, so let us briefly recall the definition and basic properties. Let R be a Dedekind domain with fractional field F, and D be a quaternion F-algebra (not necessarily division). An R-order O in D is called an *Eichler order* if it can be written as the intersection of two maximal orders; see [**5**, Corollary 2.2] for an equivalent characterization of Eichler orders. The R-ideal index [**19**, Chapter III, Section 1] of an Eichler order O relative to any maximal R-order is called the *level* of O. Assume further that R is a complete discrete valuation ring, and let π be a local parameter of R. If D is division, then there is a unique maximal order in D, hence a unique Eichler order O. Any O-lattice in a left D-vector space of dimension m is isomorphic to O^m. Next, suppose that $D = \mathrm{Mat}_2(F)$. Then any maximal order of D is conjugate to $M_2(R)$. An order O is Eichler if and only if there exists a nonnegative integer $n \geq 0$ such that O is conjugate to $O_n := \begin{bmatrix} R & R \\ \pi^n R & R \end{bmatrix}$. Up to isomorphism, any O_n-lattice in the left $\mathrm{Mat}_2(F)$-module $\mathrm{Mat}_{2,m}(F)$ has the form

$$\bigoplus_{i=1}^{w} \begin{bmatrix} R \\ \pi^{t_i} R \end{bmatrix}^{s_i}, \quad \text{where} \quad \sum_{i=1}^{w} s_i = m \quad \text{and} \quad n \geq t_1 > \cdots > t_w \geq 0. \tag{3.20}$$

This gives rise to a bijection between the isomorphism classes of O_n-lattices in $\mathrm{Mat}_{2,m}(F)$ and the pairs of tuples $(\underline{s}, \underline{t}) \in \mathbb{N}^w \times \mathbb{Z}^w_{\geq 0}$ (for some w between 1 and m) with $\underline{s} = (s_1, \ldots, s_w)$ and $\underline{t} = (t_1, \ldots, t_w)$ satisfying (3.20). We refer to [**22**, Chapter II, Section 2] and [**2**, Chapter 1, Subsection 1.2] for more details on Eichler orders.

REMARK 3.7. We explain what we mean by "a mild condition on p" at the beginning of Section 3. For ease of exposition of the present paper, we will work out the calculation of each $o(\underline{n})$ in Theorem 3.4 under the assumption that $A_{\underline{n},p} = A_{\underline{n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is

an étale $\mathbb{Z}_p$-algebra. If $r = 1$, this simply requires p to be unramified in K_n. For $r = 2$, an equivalent but more concrete assumption on p is made at the beginning of Section 5. The purpose for this assumption is so that $\mathscr{A}_{\underline{n},p} = A_{\underline{n},p} \otimes_{\mathbb{Z}_p} \mathcal{O}_p$ is a product of Eichler orders (cf. [**14**, Lemma 2.11]), and the proofs of Propositions 4.1, 4.2, and 5.1 rely on this result (also compare with [**14**, Lemma 2.12] for the case where p is ramified in K_n). Note that the assumption holds automatically when $p \geq 7$ so it rules out at most $p = 2, 3, 5$.

The remaining part of the paper is organized as follows. Section 4 treats the *isotypic* case where $r = 1$. The *non-isotypic* case where $r = 2$ is treated in Section 5. The calculation of class numbers of certain complicated orders arising in Section 5 is postponed to Section 6. The handful of cases where the assumption fails will be treated in an upcoming paper [**29**], where the ramification requires much greater care.

4. Computations of the isotypic cases.

We keep the notation of Section 3 and put $D = D_{p,\infty}$, the quaternion $\mathbb{Q}$-algebra ramified exactly at the prime p and ∞. The goal of this section is to calculate the terms $o(n)$ with $n \in \{3, 4, 5, 8, 12\}$ in Theorem 3.4, under the assumption that p is *unramified* in K_n (i.e. $p \nmid n$). According to (3.16), this covers the isotypic case for such p. 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 [**23**, 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

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

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 (3.9) and (3.10), 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 [**18**, Definition 34.3], and $\mathrm{Nr}(\mathscr{E}_n^\times) = K_n^\times$ by [**22**, 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 [**22**, Corollaire III.5.7]. It follows that for all $n \in \{3, 4, 5, 8, 12\}$ and $p \nmid n$,

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

For each $f \in \mathbb{N}$, let $\mathbb{Q}_{p^f}$ be the unique unramified extension of degree f over $\mathbb{Q}_p$, and $\mathbb{Z}_{p^f}$ be its ring of integers.

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 [**22**, 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 from (3.20) 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 the opposite ring of

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

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* 3.4 *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 the non-isotypic cases.

In this section, we calculate the values of $o(\underline{n})$ with

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

According to (3.17), this treats all the non-isotypic cases. As mentioned in Remark 3.7, we assume 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 both $i = 1, 2$;

(II) $A_{\underline{n},p} = \mathbb{Z}_p[T]/(\Phi_{n_1}(T)\Phi_{n_2}(T))$ is a maximal $\mathbb{Z}_p$-order in $K_{\underline{n},p}$.

This rules out at most $p = 2, 3$ according to Table 1 below. 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.

5.1. General structures.

We explore the general structures of objects of interest such as $A_{\underline{n}}$, $\mathscr{L}_p(\underline{n})$ and so on for all $\underline{n}$ in (5.1). This sets up the stage for a case-by-case calculation of $o(\underline{n})$ in the next subsection.

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

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

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

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

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), $p \neq 2$

Observe that $A_{(2,3)}$ and $A_{(3,4)}$ are maximal orders. Let $\mathfrak{p}_2$ (resp. $\mathfrak{q}_2$) be the unique dyadic prime of A_4 (resp. A_3), and $\mathfrak{p}_3$ be the unique prime ideal of A_6 above 3. Then $A_4/\mathfrak{p}_2 \simeq \mathbb{F}_2$ and $A_6/\mathfrak{p}_3 \simeq \mathbb{F}_3$. We write down the non-maximal orders $A_{\underline{n}}$ explicitly using (5.3):

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

$$A_{(2,4)} = \{(a,b) \in \mathbb{Z} \times A_4 \mid a \equiv b \pmod{\mathfrak{p}_2}\}; \tag{5.5}$$

$$A_{(2,6)} = \{(a,b) \in \mathbb{Z} \times A_6 \mid a \equiv b \pmod{\mathfrak{p}_3}\}; \tag{5.6}$$

$$A_{(3,6)} \simeq \{(a,b) \in A_3 \times A_3 \mid a \equiv b \pmod{\mathfrak{q}_2}\}, \tag{5.7}$$

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 [**27**, Lemma 7.2] if necessary, we have

$$h(A_{(3,4)}) = h(A_{(3,6)}) = 1. \tag{5.8}$$

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

$$h(\mathcal{O}) = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right). \tag{5.9}$$

By our assumptions, the order $\mathscr{A}_{\underline{n}}$ is non-maximal at a prime $\ell \in \mathbb{N}$ 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 every $\mathscr{A}_{\underline{n}}$-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 $\mathscr{H}_{n_i,p}$-module $V_{n_i,p}$.

It is enough to show that the number of isomorphism 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, $\mathrm{End}_{\mathscr{A}_{n_i,p}}(\Lambda_{n_i,p})=\mathbb{Z}_{p^2}$. □

Next, we consider the other class of primes at which $\mathscr{A}_{\underline{n}}$ is non-maximal, namely the prime divisors of $[O_{K_{\underline{n}}}:A_{\underline{n}}]$. According to Table 1, there exists a prime ℓ dividing $[O_{K_{\underline{n}}}:A_{\underline{n}}]$ only if

$$\underline{n}\in\{(1,2),(2,4),(2,6),(3,6)\},\tag{5.10}$$

and each $\underline{n}$ above determines uniquely such a prime ℓ. Since $\ell\neq p$ by our assumption, we have $\mathcal{O}_\ell\simeq\mathrm{Mat}_2(\mathbb{Z}_\ell)$. By Remark 3.2(ii), 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 $V_\ell=(V'_\ell)^2$. The value of ℓ and the structure of V'_ℓ for each $\underline{n}$ is given by the following table.

Table 2.

$\underline{n}$	ℓ	V'_ℓ
$(1,2)$	2	$(K_{\underline{n},\ell})^2=(\mathbb{Q}_2\times\mathbb{Q}_2)^2$
$(2,4)$	2	$(K_{2,\ell})^2\times K_{4,\ell}=\mathbb{Q}_2^2\times K_{4,2}$
$(2,6)$	3	$(K_{2,\ell})^2\times K_{6,\ell}=\mathbb{Q}_3^2\times K_{6,3}$
$(3,6)$	2	$K_{\underline{n},\ell}=\mathbb{Q}_4\times\mathbb{Q}_4$

To classify the isomorphism classes of $A_{\underline{n},\ell}$-lattices in V'_ℓ in each of the above cases, we apply the theory of *Bass orders*. Recall that a Bass order is a Gorenstein order for which every order containing it in the ambient algebra is Gorenstein as well [**6**, Section 37]. We provide a couple of equivalent characterizations in the commutative case. Let R be a Dedekind domain with fractional field F, and B be an R-order in a finite dimensional separable semisimple F-algebra E. Denote the maximal R-order in E by O_E. The following are equivalent:

(i) B is a Bass order, i.e. every R-order B' with $B\subseteq B'\subseteq O_E$ is Gorenstein;

(ii) every ideal I of B can be generated by two elements;

(iii) the quotient O_E/B is a cyclic B-module.

Characterization (ii) above is due to Bass [**3**, Section 7], and (iii) is due to Borevich and Faddeev (see [**6**, Section 37, p.789]). Thanks to (iii) and (5.3), $A_{\underline{n}}$ is a Bass order for any arbitrary[2] $\underline{n}\in\breve{\mathbb{N}}^2$. The Bass property is local in the sense that B is Bass if and only if

[2]However, the same does not hold for $\underline{n}\in\breve{\mathbb{N}}^r$ with $r\geq 3$, because $A_{(1,2,4)}=\mathbb{Z}[T]/(T^4-1)$ already provides a counterexample.

$B_{\mathfrak{p}}$ is Bass for every nonzero prime $\mathfrak{p} \subseteq R$. In particular, $A_{\underline{n},\ell}$ is Bass for all $\underline{n}$ in (5.10) and the corresponding prime ℓ determined by $\underline{n}$.

Note that V'_ℓ is a free $K_{\underline{n},\ell}$-module when $\underline{n} = (1,2)$ or $(3,6)$. Let B be a commutative Bass order and M be a B-lattice in a *free* E-module of rank m. It follows from the result of Borevich and Faddeev [**6**] that there exists an ascending chain of R-orders

$$B \subseteq B_1 \subseteq \cdots \subseteq B_m \tag{5.11}$$

and an invertible B_m-ideal J such that

$$M \simeq B_1 \oplus \cdots \oplus B_{m-1} \oplus J.$$

The chain of orders (5.11) and the isomorphism class of J in the Picard group $\mathrm{Pic}(B_m)$ determine uniquely the B-isomorphism class of M, and vice versa. If R is local, then $\mathrm{Pic}(B_m)$ is trivial, and we have

$$M \simeq B_1 \oplus \cdots \oplus B_m. \tag{5.12}$$

In this case, the chain (5.11) alone forms the isomorphic invariant of M. We will apply this result in the proofs of Propositions 5.3 and 5.4.

For $\underline{n} = (2, 2\ell)$ with $\ell \in \{2,3\}$, the $K_{\underline{n},\ell}$-module V'_ℓ is no longer free. Nevertheless, we can use the Krull–Schmidt–Azumaya theorem [**6**, Theorem 6.12] to write any $A_{\underline{n},\ell}$-lattice $\Lambda'_\ell \subset V'_\ell$ into a direct sum of indecomposable sublattices. Every indecomposable lattice over a commutative Bass order is isomorphic to an ideal by [**3**, Section 7] (see [**6**, Theorem 37.16] for the general case). This allows us to classify up to isomorphism all the indecomposable $A_{\underline{n},\ell}$-lattices, and hence all $A_{\underline{n},\ell}$-lattices in V'_ℓ. We work out this in detail in the proof of Proposition 5.5.

5.2. Case-by-case calculations of $o(\underline{n})$.

We arrange the calculations of $o(\underline{n})$ in the order essentially according to the complexity of V'_ℓ as a $K_{\underline{n},\ell}$-module in Table 2. We first treat the cases $\underline{n} = (2,3)$ and $\underline{n} = (3,4)$ in Proposition 5.2. The orders $A_{\underline{n}}$ are already maximal orders in $K_{\underline{n}}$ for these two $\underline{n}$, so no classification of local lattices is needed at any prime distinct from p. Next, we treat the case $\underline{n} = (3,6)$ in Proposition 5.3, where V'_ℓ is a free $K_{\underline{n},\ell}$-module of rank 1. After that, we treat the case $\underline{n} = (1,2)$ in Proposition 5.4, where V'_ℓ is a free $K_{\underline{n},\ell}$-module of rank 2. In both previous cases, we apply the result of Borevich and Faddeev on Bass orders. Lastly, we treat the cases $\underline{n} = (2, 2\ell)$ with $\ell \in \{2,3\}$ in Proposition 5.5. The $K_{\underline{n},\ell}$-module V'_ℓ is not free for these two $\underline{n}$, so we take the Krull–Schmidt–Azumaya approach instead. The calculation of class numbers of certain complicated orders (to be defined in (5.14) and (5.17)) is postponed to Section 6.

PROPOSITION 5.2. (1) *We have* $o(2,3) = (1 - (-3/p))\, h(\mathcal{O})$ *for all* $p \neq 3$. *See* (5.9) *for the formula of* $h(\mathcal{O})$.

(2) *We have* $o(3,4) = (1 - (-3/p))(1 - (-4/p))$ *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 $\ell \neq p$. 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 $h(O_\Lambda) = h(\mathcal{O})h(A_3) = h(\mathcal{O})$. By Proposition 5.1, we get $o(2,3) = 2h(\mathcal{O})$. If $\underline{n} = (3,4)$, then $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = K_3 \times K_4$, and $O_\Lambda = A_3 \times A_4 = A_{(3,4)}$, which has class number 1 as remarked in (5.8). By Proposition 5.1, we get $o(3,4) = 4$.

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

PROPOSITION 5.3. *We have $o(3,6) = 2(1-(-3/p))^2$ for all $p \neq 2,3$.*

PROOF. Assume that $p \neq 2,3$. Only the case $p \equiv 2 \pmod 3$ 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 (5.7). 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 $O_{K_{\underline{n},2}}$ by (5.12). Correspondingly,

$$\mathrm{End}_{A_{\underline{n},2}}(\Lambda_2') = \begin{cases} A_{\underline{n},2} & \text{if } \Lambda_2' \simeq A_{\underline{n},2}, \\ O_{K_{\underline{n},2}} & \text{if } \Lambda_2' \simeq O_{K_{\underline{n},2}}, \end{cases} \tag{5.13}$$

and the same holds for $\mathrm{End}_{\mathscr{A}_{\underline{n},2}}(\Lambda_2)$ by Remark 3.2(ii). It follows from Proposition 5.1 that

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

for any $\mathscr{A}_{\underline{n}}$-lattice $\Lambda \subset V$. Recall that $h(A_{\underline{n}}) = h(O_{K_{\underline{n}}}) = 1$ by (5.8). 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 $\mathbb{O}_1(1,2)$ of index 8 and 16 respectively such that

$$\begin{aligned} &\mathbb{O}_8(1,2)_2 = \begin{pmatrix} A_{\underline{n},2} & 2O_{K_{\underline{n},2}} \\ O_{K_{\underline{n},2}} & O_{K_{\underline{n},2}} \end{pmatrix}, \qquad \mathbb{O}_{16}(1,2)_2 = \mathrm{Mat}_2(A_{\underline{n},2}); \\ &\mathbb{O}_i(1,2)_{\ell'} = \mathbb{O}_1(1,2)_{\ell'} \qquad \forall \text{ prime } \ell' \neq 2 \text{ and } i = 8, 16. \end{aligned} \tag{5.14}$$

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

$$\begin{aligned} o(1,2) &= h(\mathbb{O}_1(1,2)) + h(\mathbb{O}_8(1,2)) + h(\mathbb{O}_{16}(1,2)) \\ &= \frac{(p-1)^2}{9} + \frac{p+15}{18}\left(1-\left(\frac{-3}{p}\right)\right) + \frac{p+2}{6}\left(1-\left(\frac{-4}{p}\right)\right) \\ &\quad + \frac{1}{6}\left(1-\left(\frac{-3}{p}\right)\right)\left(1-\left(\frac{-4}{p}\right)\right). \end{aligned} \tag{5.15}$$

PROOF. Throughout this proof, we assume that $p \neq 2$. By Table 2, V_2' is a free $K_{\underline{n},2}$-module of rank 2. According to (5.12), 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

$$o(1,2) = h(\mathbb{O}_1(1,2)) + h(\mathbb{O}_8(1,2)) + h(\mathbb{O}_{16}(1,2)). \tag{5.16}$$

The class number $h(\mathbb{O}_8(1,2))$ is given by Proposition 6.5, and $h(\mathbb{O}_{16}(1,2))$ is given by Proposition 6.7. Lastly, we have $h(\mathbb{O}_1(1,2)) = h(\mathcal{O})^2$ (see (5.9)). The explicit formula for $o(1,2)$ follows from (5.16). □

Finally, we study the terms $o(2, 2\ell)$ for $\ell \in \{2, 3\}$. We have $[O_{K_{\underline{n}}} : A_{\underline{n}}] = \ell$, and $\mathrm{End}_{\mathscr{K}_{\underline{n}}}(V) = D \times K_{2\ell}$, the product (not the tensor product) of D and $K_{2\ell}$, by (5.2). Let $\mathbb{O}_1(2, 2\ell)$ be the maximal order $\mathcal{O} \times A_{2\ell} \subset \mathrm{End}_{\mathscr{K}_{\underline{n}}}(V)$. Recall that $p \neq \ell$ by our assumption, so we fix an isomorphism $\mathcal{O}_\ell \simeq \mathrm{Mat}_2(\mathbb{Z}_\ell)$. By an abuse of notation, we still write $\mathfrak{p}_\ell$ for the unique prime ideal of $A_{2\ell,\ell}$ above ℓ. Let $\mathbb{O}_{\ell^2}(2, 2\ell)$ be the suborder of index ℓ^2 in $\mathbb{O}_1(2, 2\ell)$ such that

$$\begin{aligned} \mathbb{O}_{\ell^2}(2,2\ell)_\ell &= \left\{ \left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, b \right) \in \mathbb{O}_1(2,2\ell)_\ell \,\middle|\, \begin{array}{ll} a_{21} \equiv 0 & (\mathrm{mod}\ \ell) \\ a_{22} \equiv b & (\mathrm{mod}\ \mathfrak{p}_\ell) \end{array} \right\}; \\ \mathbb{O}_{\ell^2}(2,2\ell)_{\ell'} &= \mathbb{O}_1(2,2\ell)_{\ell'} \qquad \forall \text{ prime } \ell' \neq \ell. \end{aligned} \tag{5.17}$$

PROPOSITION 5.5. *For $\ell \in \{2, 3\}$, we have $o(2, 2\ell) = 2h(\mathbb{O}_1(2, 2\ell)) + 2h(\mathbb{O}_{\ell^2}(2, 2\ell))$. More explicitly,*

$$\begin{aligned} o(2,4) &= \left(\frac{p+3}{3} - \frac{1}{3}\left(\frac{-3}{p}\right)\right)\left(1-\left(\frac{-4}{p}\right)\right) \quad \textit{if } p \neq 2; \\ o(2,6) &= \left(\frac{5p+18}{12} + \frac{1}{3}\left(\frac{-3}{p}\right) - \frac{1}{4}\left(\frac{-4}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right) \quad \textit{if } p \neq 3. \end{aligned} \tag{5.18}$$

PROOF. As discussed before Section 5.1, $o(2,4) = 0$ if $p \equiv 1 \pmod 4$ and $o(2,6) = 0$ if $p \equiv 1 \pmod 3$. Thus, we shall assume $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$ for $\ell = 2, 3$, respectively.

Let $V'_\ell = \mathbb{Q}_\ell^2 \times K_{2\ell,\ell} = \mathbb{Q}_\ell \oplus K_{\underline{n},\ell}$ be the module over $K_{\underline{n},\ell} = \mathbb{Q}_\ell \times K_{2\ell,\ell}$ in Table 2. We claim that any $A_{\underline{n},\ell}$-lattice $\Lambda'_\ell \subset V'_\ell$ is isomorphic to $\Sigma_0 := \mathbb{Z}_\ell \oplus O_{K_{\underline{n},\ell}}$ or $\Sigma := \mathbb{Z}_\ell \oplus A_{\underline{n},\ell}$. By the Krull–Schmidt–Azumaya theorem [**6**, Theorem 6.12], every $A_{\underline{n},\ell}$-lattice is uniquely expressible as a finite direct sum of indecomposable sublattices, up to isomorphism and order of occurrence of the summands. Recall that any indecomposable lattice over a Bass order is isomorphic to an ideal [**3**, Section 7]. Let I_ℓ be an $A_{\underline{n},\ell}$-ideal. Then $I_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is isomorphic to $\mathbb{Q}_\ell$, $K_{2\ell,\ell}$ or $K_{\underline{n},\ell}$. If $I_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq K_{\underline{n},\ell}$, then the result of Borevich and Faddeev [**6**, Section 37, p.789] implies that I_ℓ is isomorphic to either $A_{\underline{n},\ell}$ or $O_{K_{\underline{n},\ell}} = \mathbb{Z}_\ell \oplus A_{2\ell,\ell}$. Clearly, $O_{K_{\underline{n},\ell}}$ is decomposable. Therefore, if I_ℓ is indecomposable, then we have

$$I_\ell \simeq \begin{cases} \mathbb{Z}_\ell & \text{if } \ I_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell; \\ A_{2\ell,\ell} & \text{if } \ I_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq K_{2\ell,\ell}; \\ A_{\underline{n},\ell} & \text{if } \ I_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq K_{\underline{n},\ell}. \end{cases} \tag{5.19}$$

Write $\Lambda'_\ell = \mathbb{Z}_\ell^{t_1} \oplus A_{2\ell,\ell}^{t_2} \oplus A_{\underline{n},\ell}^{t_3}$. Since $\Lambda'_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^2 \times K_{2\ell,\ell}$, we have $(t_1, t_2, t_3) = (2, 1, 0)$ or $(1, 0, 1)$. The claim is verified.

Direct calculation shows that

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

The classification at ℓ 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_ℓ. 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

$$o(2, 2\ell) = 2h(\mathbb{O}_1(2, 2\ell)) + 2h(\mathbb{O}_{\ell^2}(2, 2\ell)). \tag{5.20}$$

As $\mathbb{O}_1(2, 2\ell)$ is a maximal order, one has $h(\mathbb{O}_1(2, 2\ell)) = h(\mathcal{O})h(A_{2\ell}) = h(\mathcal{O})$, whose formula is given in (5.9). The class numbers of $\mathbb{O}_4(2, 4)$ and $\mathbb{O}_9(2, 6)$ are calculated in Proposition 6.4. By the formulas for $h(\mathcal{O})$, $h(\mathbb{O}_4(2, 4))$ and $h(\mathbb{O}_9(2, 6))$, we obtain for $p \neq 2$,

$$o(2, 4) = \begin{cases} 2\left(\dfrac{p+3}{3} - \dfrac{1}{3}\left(\dfrac{-3}{p}\right)\right) & \text{if } \ p \equiv 3 \pmod 4; \\ 0 & \text{if } \ p \equiv 1 \pmod 4, \end{cases} \tag{5.21}$$

and for $p \neq 3$,

$$o(2, 6) = \begin{cases} 2\left(\dfrac{5p+14}{12} - \dfrac{1}{4}\left(\dfrac{-4}{p}\right)\right) & \text{if } \ p \equiv 2 \pmod 3; \\ 0 & \text{if } \ p \equiv 1 \pmod 3. \end{cases} \tag{5.22}$$

We rewrite (5.21) and (5.22) into (5.18), which will also hold for $p = 2, 3$ [**29**]. □

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 [**9**] 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 (5.14) and (5.17). 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. We first work out $h(\mathbb{O}_4(2,4))$ and $h(\mathbb{O}_9(2,6))$ in Proposition 6.4, and then $h(\mathbb{O}_8(1,2))$ in Proposition 6.5, and lastly $h(\mathbb{O}_{16}(1,2))$ in Proposition 6.7.

We recall some properties of 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 adelic 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

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

and the latter 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 $\mathcal{R}_J$ of 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

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

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 $\ell\in\{2,3\}$, and assume that $p\neq\ell$. Fix an isomorphism $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_\ell\simeq\mathrm{Mat}_2(\mathbb{Z}_\ell)$. We write $\mathcal{O}^{(\ell)}$ for the Eichler order of level ℓ in $\mathcal{O}$ such that $\mathcal{O}^{(\ell)}\otimes\mathbb{Z}_{\ell'}=\mathcal{O}\otimes\mathbb{Z}_{\ell'}$ for every prime $\ell'\neq\ell$, and

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

The formula for $h(\mathcal{O}^{(\ell)})$ is given in [**15**, Theorem 16]:

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

PROPOSITION 6.4. *Suppose that $\ell \in \{2,3\}$ and $p \neq \ell$. Let $\mathbb{O}_{\ell^2}(2,2\ell)$ be the order defined in* (5.17). *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 $\mathbb{O}_{\ell^2} = \mathbb{O}_{\ell^2}(2,2\ell)$, and define $\mathbb{O}_\ell := \mathcal{O}^{(\ell)} \times A_{2\ell}$, which contains $\mathbb{O}_{\ell^2}$ and is a suborder of index ℓ in $\mathbb{O}_1(2,2\ell) = \mathcal{O} \times A_{2\ell}$. Recall that $\mathfrak{p}_\ell$ denotes the unique ramified prime in $A_{2\ell}$. We have $A_{2\ell}/\mathfrak{p}_\ell = \mathbb{F}_\ell$, and the canonical map $A_{2\ell}^\times \to (A_{2\ell}/\mathfrak{p}_\ell)^\times = \mathbb{F}_\ell^\times$ is surjective.

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

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

Applying formula (6.5), we obtain

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

Next, we assume that $p \neq 2$ and calculate the class numbers of the orders $\mathbb{O}_8(1,2)$ and $\mathbb{O}_{16}(1,2)$ defined in (5.14). For simplicity, let $\mathbb{O}_i = \mathbb{O}_i(1,2)$ for $i \in \{1,8,16\}$.

PROPOSITION 6.5. *Suppose that $p \neq 2$. Then*

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

PROOF. 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 primes $\ell' \neq 2$. Put $\mathscr{O}_4 := \mathcal{O}^{(2)} \times \mathcal{O}^{(2)}$, 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 $\widehat{\mathbb{O}}_1^\times \not\subseteq \mathcal{N}(\widehat{\mathbb{O}}_{16})$. This prevents us from applying Lemma 6.1 or Corollary 6.3 to the current situation.

We consider the natural surjective map $\pi : \mathrm{Cl}(\mathbb{O}_{16}) \to \mathrm{Cl}(\mathbb{O}_1)$ and work out explicitly the cardinality of each fiber. 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 6.6. (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 on n letters.*

(2) *Let $c_{j_1,j_2} := |C_{j_1} \backslash S_3 / C_{j_2}|$ for $1 \leq j_1, j_2 \leq 3$. Then the values of c_{j_1,j_2} are listed in the following table*:

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 the 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 $S_3 = \mathrm{GL}_2(\mathbb{F}_2)$; then the result follows from the Bruhat decomposition. □

PROPOSITION 6.7. *We have*

$$h(\mathbb{O}_{16}(1,2)) = \frac{(p-1)^2}{24} + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{2}{3}\left(1 - \left(\frac{-3}{p}\right)\right) \quad \textit{if } p \neq 2,3.$$

Moreover, if $p = 3$, *then* $h(\mathbb{O}_{16}(1,2)) = 1$.

PROOF. First suppose that $p = 3$. By [**22**, 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 6.6 shows that $h(\mathbb{O}_{16}) = |(S_3)^2 \backslash (S_3)^2 / \Delta(S_3)| = 1$.

Next, suppose 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 [**22**, 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 $\mathbb{O}_J^\times \simeq C_{2j_1} \times C_{2j_2}$, it follows from Lemma 6.6 that

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

Observe that

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

We can express (6.11) as

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

□

Acknowledgements. The first author thanks Academia Sinica and NCTS for their hospitality and great working conditions. The authors thank the referee for a careful reading and helpful comments that have improved the exposition of the paper.

References

[1] S. Alaca and K. S. Williams, Introductory Algebraic Number Theory, Cambridge Univ. Press, Cambridge, 2004.
[2] M. Alsina and P. Bayer, Quaternion Orders, Quadratic Forms, and Shimura Curves, CRM Monogr. Ser., **22**, Amer. Math. Soc., Providence, RI, 2004.
[3] H. Bass, On the ubiquity of Gorenstein rings, Math. Z., **82** (1963), 8–28.
[4] A. Borel, Arithmetic properties of linear algebraic groups, In: Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, 10–22.
[5] J. Brzeziński, On orders in quaternion algebras, Comm. Algebra, **11** (1983), 501–522.
[6] C. W. Curtis and I. Reiner, Methods of Representation Theory. Vol. I: With Applications to Finite Groups and Orders, Wiley Classics Lib., John Wiley & Sons, Inc., New York, 1990. Reprint of the 1981 original, A Wiley-Interscience Publication.
[7] M. Eichler, Über die Idealklassenzahl hyperkomplexer Systeme, Math. Z., **43** (1938), 481–494.
[8] B. Farb and R. K. Dennis, Noncommutative Algebra, Grad. Texts in Math., **144**, Springer-Verlag, New York, 1993.
[9] A. Heller and I. Reiner, Representations of cyclic groups in rings of integers. I, Ann. of Math. (2), **76** (1962), 73–92.
[10] J. E. Humphreys, Conjugacy Classes in Semisimple Algebraic Groups, Math. Surveys Monogr., **43**, Amer. Math. Soc., Providence, RI, 1995.
[11] V. Karemaker and R. Pries, Fully maximal and fully minimal abelian varieties, J. Pure Appl. Algebra, **223** (2019), 3031–3056.
[12] R. P. Langlands, Stable conjugacy: definitions and lemmas, Canad. J. Math., **31** (1979), 700–725.
[13] K.-Z. Li and F. Oort, Moduli of Supersingular Abelian Varieties, Lecture Notes in Math., **1680**, Springer-Verlag, Berlin, 1998.
[14] Q. Li, J. Xue and C.-F. Yu, Unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields, (July 2018), arXiv:1807.04736.
[15] A. Pizer, On the arithmetic of quaternion algebras, Acta Arith., **31** (1976), 61–89.
[16] V. Platonov and A. Rapinchuk, Algebraic Groups and Number Theory, Pure Appl. Math., **139**, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by R. Rowen.
[17] F. Pop and H. Pop, An extension of the Noether–Skolem theorem, J. Pure Appl. Algebra, **35** (1985), 321–328.
[18] I. Reiner, Maximal Orders, London Math. Soc. Monogr.(N.S.), **28**, The Clarendon Press, Oxford Univ. Press, Oxford, 2003. Corrected reprint of the 1975 original, with a foreword by M. J. Taylor.
[19] J.-P. Serre, Local Fields, Grad. Texts in Math., **67**, Springer-Verlag, New York, 1979. Translated from the French by M. J. Greenberg.
[20] T. A. Springer and R. Steinberg, Conjugacy classes, In: Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, NJ, 1968/69), Lecture Notes in Math., **131**, Springer, Berlin, 1970, 167–266.
[21] R. G. Swan, Torsion free cancellation over orders, Illinois J. Math., **32** (1988), 329–360.
[22] M.-F. Vignéras, Arithmétique des Algèbres de Quaternions, Lecture Notes in Math., **800**, Springer, Berlin, 1980.
[23] L. C. Washington, Introduction to Cyclotomic Fields, second edition, Grad. Texts in Math., **83**, Springer-Verlag, New York, 1997.
[24] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. (4), **2** (1969), 521–560.
[25] J. Xue, T.-C. Yang and C.-F. Yu, Supersingular abelian surfaces and Eichler's class number formula, (April 2014), arXiv:1404.2978, to appear in Asian J. Math.
[26] J. Xue, T.-C. Yang and C.-F. Yu, Numerical invariants of totally imaginary quadratic $\mathbb{Z}[\sqrt{p}]$-orders, Taiwanese J. Math., **20** (2016), 723–741.

[27] J. Xue, T.-C. Yang and C.-F. Yu, On superspecial abelian surfaces over finite fields, Doc. Math., **21** (2016), 1607–1643.
[28] J. Xue and C.-F. Yu, On counting certain abelian varieties over finite fields, (January 2018), arXiv:1801.00229v2, to appear in Acta Math. Sin. (Engl. Ser.).
[29] J. Xue, C.-F. Yu and Y. Zheng, On superspecial abelian surfaces over finite fields III, in preparation.
[30] C.-F. Yu, Embeddings of fields into simple algebras: generalizations and applications, J. Algebra, **368** (2012), 1–20.
[31] C.-F. Yu, Superspecial abelian varieties over finite prime fields, J. Pure Appl. Algebra, **216** (2012), 1418–1427.
[32] C.-F. Yu, A note on supersingular abelian varieties, (December 2014), arXiv:1412.7107.

Jiangwei Xue
Collaborative Innovation Centre of Mathematics
School of Mathematics and Statistics
Wuhan University
Luojiashan, Wuhan
Hubei 430072, P.R. China
and
Hubei Key Laboratory of Computational Science
Wuhan University
Hubei 430072, P.R. China
E-mail: 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: tsechung@math.sinica.edu.tw

Chia-Fu Yu
Institute of Mathematics
Academia Sinica
Astronomy-Mathematics Building
No. 1, Sec. 4, Roosevelt Road
Taipei 10617, Taiwan
and
National Center for Theoretical Sciences
Astronomy-Mathematics Building
No. 1, Sec. 4, Roosevelt Road
Taipei 10617, Taiwan
E-mail: chiafu@math.sinica.edu.tw