On Superspecial Abelian Surfaces over Finite Fields

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

Received: April 20, 2016
Revised: September 4, 2016

Communicated by Takeshi Saito

Abstract. In this paper we establish a new lattice description for superspecial abelian varieties over a finite field $\mathbb{F}_q$ of $q = p^a$ elements. Our description depends on the parity of the exponent a of q. When q is an odd power of the prime p, we give an explicit formula for the number of superspecial abelian surfaces over $\mathbb{F}_q$.

2010 Mathematics Subject Classification: 11R52, 11G10
Keywords and Phrases: supersingular abelian surfaces, class number formula, Galois cohomology.

1. Introduction

Throughout this paper p denotes a prime number, and $q = p^a$ a power of p with an exponent $a \in \mathbb{N}$, the set of strictly positive integers. The goal of this paper is to calculate explicitly the number of superspecial abelian surfaces over a finite field $\mathbb{F}_q$. This can be regarded as a natural extension of works of the authors [22, 23] and the last named author [26] contributed to the study of supersingular abelian varieties over finite fields.

Recall that 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 $\overline{k}$ of k; it is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over $\overline{k}$. As any supersingular abelian variety is isogenous to a superspecial abelian variety, it is very common to study supersingular abelian varieties through investigating the classification of superspecial abelian varieties.

For any integer $d \geq 1$, let $\mathrm{Sp}_d(\mathbb{F}_q)$ denote the set of isomorphism classes of d-dimensional superspecial abelian varieties over the finite field $\mathbb{F}_q$ of q elements. The case where $d = 1$ concerns the classification of supersingular elliptic curves over finite fields. The theory of elliptic curves over finite fields has been studied by Deuring since 1940's and becomes well known. There are explicit descriptions for each isogeny class; see Waterhouse [21, Section 4]. However, the authors could not find an explicit formula for $|\operatorname{Sp}_1(\mathbb{F}_q)|$ in the literature. For the sake of completeness we include a formula for $|\operatorname{Sp}_1(\mathbb{F}_q)|$, based on the exposition of Deuring's results by Waterhouse [21]. The goal of the present paper is then to find an explicit formula for the number $|\operatorname{Sp}_d(\mathbb{F}_q)|$ in the case where $d=2$.

Before stating our main results, we describe a basic method for counting $\operatorname{Sp}_d(\mathbb{F}_q)$. For simplicity, assume that $\mathbb{F}_q=\mathbb{F}_p$ is the prime finite field for the moment. One can divide the finite set $\operatorname{Sp}_d(\mathbb{F}_p)$ into finitely many subsets according to the isogeny classes of members. Therefore, it suffices to classify all d-dimensional supersingular isogeny classes and to count the number of superspecial members in each supersingular isogeny class. The Honda-Tate theorem allows us to describe isogeny classes over $\mathbb{F}_q$ in terms of multiple Weil q-numbers (which are simply finite nonnegative integral formal sums of Weil q-numbers up to conjugate; see Section 4.1). If π is a supersingular multiple Weil q-number, we denote by $[X_\pi]$ the corresponding supersingular isogeny class (here X_π is an abelian variety in this class), $H(\pi)$ the number of isomorphism classes of abelian varieties in $[X_\pi]$ and $H_{sp}(\pi)$ the number of isomorphism classes of *superspecial* abelian varieties in $[X_\pi]$. Then we have

$$|\operatorname{Sp}_d(\mathbb{F}_p)|=\sum_{\pi}H_{sp}(\pi), \tag{1.1}$$

where π runs through all supersingular multiple Weil p-numbers with $\dim X_\pi=d$. We classify all possible isogeny classes of π's occurring in the sum (see Sections 2–3). The problem then is to compute each term $H_{sp}(\pi)$. One should distinguish the cases according to whether the endomorphism algebra $\operatorname{End}^0(X_\pi)=\operatorname{End}(X_\pi)\otimes\mathbb{Q}$ of X_π satisfies the Eichler condition [19, Section III.4, p.81] or not. We now focus on the case where $d=2$.

Consider the case where π is the Weil p-number $\sqrt{p}$. Correspondingly, X_π is a supersingular abelian surface. It is known (see Tate [17]) that the endomorphism algebra $\operatorname{End}^0(X_\pi)$ of X_π is isomorphic to the totally definite quaternion algebra algebra $D=D_{\infty_1,\infty_2}$ over the quadratic real field $F=\mathbb{Q}(\sqrt{p})$ ramified exactly at the two real places $\{\infty_1,\infty_2\}$ of F. In this case all abelian surfaces in the isogeny class $[X_{\sqrt{p}}]$ are superspecial, i.e. $H(\sqrt{p})=H_{sp}(\sqrt{p})$. When $p=2$ or $p\equiv 3 \pmod 4$, Waterhouse proved that the number $H(\sqrt{p})$ is equal to the class number $h(D)$ of D. The current authors analyzed the remaining case in [22, Section 6] and showed that when $p\equiv 1 \pmod 4$, the number $H(\sqrt{p})$ is equal to the sum of $h(D)$ and the class numbers of two other proper $\mathbb{Z}[\sqrt{p}]$-orders in D of index 8 and 16, respectively (the descriptions of these orders are made concrete by results of [25]). These class numbers are computed systematically in [22], which produces the explicit formulas for $H(\sqrt{p})$ given in Theorem 1.1 below. In what follows we write $K_{m,j}$ for the number field $\mathbb{Q}(\sqrt{m},\sqrt{-j})$ for any square-free integers $m>1$ and $j\ge 1$. If $m\equiv 1 \pmod 4$, then we define

$$\varpi_m := 3[O^\times_{\mathbb{Q}(\sqrt{m})}:\mathbb{Z}[\sqrt{m}]^\times]^{-1}, \tag{1.2}$$

where $O_{\mathbb{Q}(\sqrt{m})}$ denotes the ring of integers of $\mathbb{Q}(\sqrt{m})$. By similar arguments as those in [23, Lemma 4.1 and Section 4.2], we have $\varpi_m \in \{1,3\}$, and $\varpi_m = 3$ if $m \equiv 1 \pmod 8$. The class number of a number field K is denoted by $h(K)$. When $K = \mathbb{Q}(\sqrt{m})$, we write $h(\sqrt{m})$ for $h(\mathbb{Q}(\sqrt{m}))$ instead.

Theorem 1.1. *Let $H(\sqrt{p})$ be the number of $\mathbb{F}_p$-isomorphism classes of abelian varieties in the simple isogeny class corresponding to the Weil p-number $\pi = \sqrt{p}$, and let $F = \mathbb{Q}(\sqrt{p})$. Then*
(1) $H(\sqrt{p}) = 1, 2, 3$ for $p = 2, 3, 5$, respectively.
(2) For $p > 5$ and $p \equiv 3 \pmod 4$, we have
(1.3)
$$H(\sqrt{p}) = \frac{1}{2}h(F)\zeta_F(-1) + \left(\frac{3}{8} + \frac{5}{8}\left(2 - \left(\frac{2}{p}\right)\right)\right)h(K_{p,1}) + \frac{1}{4}h(K_{p,2}) + \frac{1}{3}h(K_{p,3}),$$
where $\zeta_F(s)$ is the Dedekind zeta function of F.
(3) For $p > 5$ and $p \equiv 1 \pmod 4$, we have
(1.4)
$$H(\sqrt{p}) = \begin{cases} 8\zeta_F(-1)h(F) + h(K_{p,1}) + \frac{4}{3}h(K_{p,3}) & \text{for } p \equiv 1 \pmod 8; \\ \dfrac{1}{2}(15\varpi_p + 1)\zeta_F(-1)h(F) + \dfrac{1}{4}(3\varpi_p + 1)h(K_{p,1}) + \dfrac{4}{3}h(K_{p,3}) & \\ & \text{for } p \equiv 5 \pmod 8. \end{cases}$$

The computation in Theorem 1.1 is based on the generalized Eichler class formula [22, Theorem 1.4] that the authors developed. Compared with the *classical* Eichler class number formula [19, Corollary V.2.5] which treats only the Eichler orders, this *generalized* formula allows us to compute the class number of an arbitrary $\mathbb{Z}$-order in a totally definite quaternion over a totally real field F. This $\mathbb{Z}$-order does not necessarily contains the maximal order O_F of F. For a quadratic real field F, the special zeta value $\zeta_F(-1)$ can be calculated by Siegel's formula [28, Table 2, p. 70]

$$\zeta_F(-1) = \frac{1}{60} \sum_{\substack{b^2+4ac=\mathfrak{d}_F \\ a,c>0}} a, \tag{1.5}$$

where $\mathfrak{d}_F$ is the discriminant of $F/\mathbb{Q}$, $b \in \mathbb{Z}$ and $a, c \in \mathbb{N}$.
The first main result of this paper gives the following explicit formula for $|\mathrm{Sp}_2(\mathbb{F}_p)|$, the number of isomorphism classes of superspecial abelian surfaces over $\mathbb{F}_p$. To obtain this formula, we calculate all terms $H_{sp}(\pi)$ with $\pi \neq \pm\sqrt{p}$ in (1.1), and then sum them up together with $H(\sqrt{p})$. The computation of $H_{sp}(\pi)$ uses a lattice description for superspecial abelian varieties; see Section 5 for details. Similar to Theorem 1.1, special attentions have to be paid to the cases with small primes p.

Theorem 1.2. *We have $|\,\mathrm{Sp}_2(\mathbb{F}_p)| = H(\sqrt{p}) + \Delta(p)$, where the formula for $H(\sqrt{p})$ is stated in Theorem 1.1 and $\Delta(p)$ is the number described as follows.*

(1) $\Delta(p) = 15, 20, 9$ for $p = 2, 3, 5$, respectively.

(2) For $p > 5$ and $p \equiv 1 \pmod 4$, we have

$$\Delta(p) = (\varpi_p + 1)h(K_{p,3}) + h(K_{2p,1}) + h(K_{3p,3}) + h(\sqrt{-p}). \tag{1.6}$$

(3) For $p > 5$ and $p \equiv 3 \pmod 4$, we have

$$\Delta(p) = h(K_{p,3}) + h(K_{2p,1}) + (\varpi_{3p} + 1)h(K_{3p,3}) + \left(4 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}). \tag{1.7}$$

A key ingredient of our computation for $\mathrm{Sp}_2(\mathbb{F}_p)$ is Proposition 5.1, which works only for the prime finite fields. Centeleghe and Stix [4] provide a categorical description of Proposition 5.1 (also compare [26, Theorem 3,1]). However, their results are also limited to the prime finite fields. When the base field $\mathbb{F}_q$ is no longer the prime finite field, direct calculations via the counting method described earlier for $\mathrm{Sp}_d(\mathbb{F}_q)$ (even when $d = 2$) become more complicated.
Our second main result extends the computations of $\mathrm{Sp}_2(\mathbb{F}_p)$ to $\mathrm{Sp}_2(\mathbb{F}_q)$ for more general finite fields $\mathbb{F}_q$ via Galois cohomology. Observe that if $d > 1$, then there is only one isomorphism class of d-dimensional superspecial abelian varieties over $\overline{\mathbb{F}}_p$ (see [12, Section 1.6, p. 13] or Theorem 6.6). Suppose X_0 is any d-dimensional superspecial abelian variety over $\mathbb{F}_p$. Then there is a bijection of finite pointed sets

$$\mathrm{Sp}_d(\mathbb{F}_p) \simeq H^1(\Gamma_{\mathbb{F}_p}, G), \quad d > 1, \tag{1.8}$$

where $\Gamma_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is the absolute Galois group of $\mathbb{F}_p$, and $G = \mathrm{Aut}(X_0 \otimes \overline{\mathbb{F}}_p)$. Thus, computing the Galois cohomology would lead to a second proof of Theorem 1.2. However, the complexity of the final formula as in Theorem 1.2 suggests that the computation of this Galois cohomology is likely on the same level of difficulty as the counting method via (1.1). Nevertheless, the true advantages of connecting to Galois cohomology are two folds.

(a) It naturally relates $\mathrm{Sp}_d(\mathbb{F}_q)$ and $\mathrm{Sp}_d(\mathbb{F}_{q'})$ in the sense of Theorem 1.3 when the exponents in $q = p^a$ and $q' = p^{a'}$ have the same parity.
(b) It gives rise to a lattice description of $\mathrm{Sp}_d(\mathbb{F}_q)$ when $q = p^a$ is an even power of p; see Proposition 6.11.

Theorem 1.3. *Let q and q' be powers of p with same exponent parity and $d \geq 1$ an integer. Then there is a natural bijection $\mathrm{Sp}_d(\mathbb{F}_q) \simeq \mathrm{Sp}_d(\mathbb{F}_{q'})$ preserving isogeny classes. In particular, the same formulas in Theorem 1.2 hold for $|\mathrm{Sp}_2(\mathbb{F}_q)|$ since $|\mathrm{Sp}_d(\mathbb{F}_q)| = |\mathrm{Sp}_d(\mathbb{F}_p)|$ when q is an odd power of p.*

The bijection for the case $d = 1$ is handled separately in Section 4 (see Remark 4.5). For $d \geq 2$, the bijection is established in Theorem 6.7. Along the way, we prove in Section 6.2 the following general result connecting isogeny classes of abelian varieties over $\mathbb{F}_q$ with cohomology classes.

Proposition 1.4. *Let $[X_0]$ be the $\mathbb{F}_q$-isogeny class of an arbitrary abelian variety X_0 over $\mathbb{F}_q$, and $G_{\mathbb{Q}} = \mathrm{End}^0(\overline{X}_0)^\times$ where $\overline{X}_0 = X_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. We write $E^0(\overline{\mathbb{F}}_q/\mathbb{F}_q, [X_0])$ for the set of $\mathbb{F}_q$-isogeny classes of abelian varieties $[X]$ such* *that $\overline{X}$ is isogenous to $\overline{X}_0$ over $\overline{\mathbb{F}}_q$. Then there is a canonical bijection of pointed sets*

$$E^0(\overline{\mathbb{F}}_q/\mathbb{F}_q,[X_0]) \xrightarrow{\sim} H^1(\Gamma_{\mathbb{F}_q},G_{\mathbb{Q}})$$

sending $[X_0]$ to the trivial cohomology class.

Theorem 1.3 together with Proposition 5.1 give a new lattice description in Corollary 6.9 for $\mathrm{Sp}_d(\mathbb{F}_q)$ when q is an odd power of p. When q is an even power of p, a lattice description of $\mathrm{Sp}_d(\mathbb{F}_q)$ completely different from the odd case is given in Proposition 6.11, which paves the way to explicit formulas of $|\mathrm{Sp}_2(\mathbb{F}_q)|$. The detailed formulas and computations will be presented in a separated paper.

The paper is organized as follows. In Section 2, we parameterize simple isogeny classes of supersingular abelian varieties over $\mathbb{F}_q$ using Weil q-numbers. Their dimensions are calculated in Section 3. In Section 4 we treat the dimension 1 case and calculate the number of isomorphism classes of supersingular elliptic curves over finite fields. The dimension 2 case is then treated in Section 5, except we work exclusively over the prime field $\mathbb{F}_p$, and some arithmetic calculations are postponed to Section 7. Section 6 studies the parity property via Galois cohomology, thus providing means to extend results of Section 5 to all $\mathbb{F}_{p^a}$ with a odd. The aforementioned lattices descriptions are obtained in this process.

2. Parameterization of supersingular isogeny classes

2.1. Let $q = p^a$ be a power of a prime number p. In this section we parameterize simple isogeny classes of supersingular abelian varieties over $\mathbb{F}_q$. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. If two algebraic numbers $\alpha, \beta \in \overline{\mathbb{Q}}$ are conjugate over $\mathbb{Q}$, then we write $\alpha \sim \beta$. Recall that an algebraic integer $\pi \in \overline{\mathbb{Q}}$ is said to be a *Weil q-number* if $|\iota(\pi)| = q^{1/2}$ for any embedding $\iota : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$. By the Honda-Tate theory, the simple isogeny classes of abelian varieties over $\mathbb{F}_q$ are in bijection with the conjugacy classes of Weil q-numbers. A Weil q-number is said to be *supersingular* if the corresponding isogeny class consists of supersingular abelian varieties. Let W_q^{ss} denote the set of conjugacy classes of supersingular Weil q-numbers. We will find a unique representative for each conjugacy class in W_q^{ss}.

Let π be a supersingular Weil q-number. It is known (the Manin-Oort Theorem, cf. [27, Theorem 2.9]) that $\pi = \sqrt{q}\,\zeta$ for a root of unity ζ. Let $K := \mathbb{Q}(\pi)$ and $L := \mathbb{Q}(\sqrt{q},\zeta)$. Note that both L and K are abelian extensions over $\mathbb{Q}$. For any $n \in \mathbb{N}$ (the set of positive integers), write $\zeta_n := e^{2\pi i/n} \in \overline{\mathbb{Q}}$.

Lemma 2.1. *Any supersingular Weil q-number π is conjugate to $\sqrt{q}\,\zeta_n$ or $-\sqrt{q}\,\zeta_n$ with $n \not\equiv 2 \pmod 4$.*

Proof. Let $\pi = \sqrt{q}\,\zeta_m^{\nu}$ for some positive integers ν and m with $(\nu, m) = 1$. Choose an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\zeta_m^{\nu}) = \zeta_m$, Then $\sigma(\pi) = \pm\sqrt{q}\,\zeta_m$.

If $m \not\equiv 2 \pmod 4$, then we are done. Suppose that $m = 2k$ for an odd integer $k = 1 - 2u$. Clearly $(k, u) = 1$. Since $\zeta_{2k} = \zeta_{2k}^{k+2u} = -\zeta_{2k}^{2u} = -\zeta_k^u$, we have

$$\pm\sqrt{q}\,\zeta_{2k} = \mp\sqrt{q}\,\zeta_k^u \sim \epsilon\sqrt{q}\,\zeta_k, \quad \text{for some } \epsilon \in \{\pm 1\}$$

by the previous argument. □

By Lemma 2.1, there is a unique subset W of $\{\pm\sqrt{q}\,\zeta_n; n \not\equiv 2 \pmod 4\}$ that contains $\{\sqrt{q}\,\zeta_n; n \not\equiv 2 \pmod 4\}$ and represents W_q^{ss}. We often identify W with W_q^{ss}. To determine the set W_q^{ss}, we need to characterize when $\sqrt{q}\,\zeta_n$ and $-\sqrt{q}\,\zeta_n$ are conjugate.
As usual, the Galois group $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is naturally identified with $(\mathbb{Z}/n\mathbb{Z})^\times$ by mapping any $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ to the element $\sigma_r \in G_n$ with $\sigma_r(\zeta_n) = \zeta_n^r$.

2.2. Let us first assume that a is even, i.e., $\sqrt{q} \in \mathbb{Q}$. Then $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$ if and only if there is an element $\sigma_r \in G_n$ such that $\sigma_r(\zeta_n) = -\zeta_n$. It is easy to see that

$$\zeta_n^r = -\zeta_n \iff 2|n \text{ and } r = \frac{n}{2} + 1, \tag{2.1}$$

and if $4|n$, then $(r, n) = 1$. As $n \not\equiv 2 \pmod 4$, this gives

$$\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff 4|n. \tag{2.2}$$

Thus,

$$W_q^{\mathrm{ss}} \simeq \{\pm\sqrt{q}\,\zeta_n \ ; \ 2 \nmid n\} \cup \{\sqrt{q}\,\zeta_n \ ; \ 4|n\}. \tag{2.3}$$

Alternatively, since $\sqrt{q} \in \mathbb{Q}$, we have $\sqrt{q}\,\zeta_n^\nu \sim \sqrt{q}\,\zeta_n$ for any $\nu \in \mathbb{N}$ with $(\nu, n) = 1$. It follows that

$$W_q^{\mathrm{ss}} \simeq \{\sqrt{q}\,\zeta_n \ ; \ n \in \mathbb{N}\}. \tag{2.4}$$

The two descriptions (2.3) and (2.4) match, because when n is odd, $-\zeta_n$ is a primitive $2n$-th root of unity and hence $-\sqrt{q}\,\zeta_n$ is conjugate to $\sqrt{q}\,\zeta_{2n}$.

2.3. We now assume that a is odd. Let $\mathfrak{d}_p$ be the discriminant of $\mathbb{Q}(\sqrt{p}\,)$. In other words, $\mathfrak{d}_p = p$ if $p \equiv 1 \pmod 4$, otherwise $\mathfrak{d}_p = 4p$. By [7, Chapter V, Theorem 48], $\sqrt{p} \in \mathbb{Q}(\zeta_n)$ if and only if $\mathfrak{d}_p \mid n$. Suppose this is the case. Let

$$\chi : G_n = (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\sqrt{p}\,)/\mathbb{Q}) = \{\pm 1\}, \quad \sigma_r(\sqrt{p}\,) = \chi(r)\sqrt{p} \tag{2.5}$$

be the associated quadratic character. Clearly, χ factors through $G_{\mathfrak{d}_p} = \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathfrak{d}_p})/\mathbb{Q})$.

LEMMA 2.2. *Let n be a positive integer with $n \not\equiv 2 \pmod 4$ and $q = p^a$ an odd power of p.*
(i) *If $\sqrt{p} \notin \mathbb{Q}(\zeta_n)$, then $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$.*
(ii) *Suppose that $\sqrt{p} \in \mathbb{Q}(\zeta_n)$, i.e., n is divisible by $\mathfrak{d}_p$. Then*

$$\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff 4|n \text{ and } \chi(n/2 + 1) = 1. \tag{2.6}$$

Proof. (i) As $\sqrt{p} \notin \mathbb{Q}(\zeta_n)$, there is an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\zeta_n) = \zeta_n$ and $\sigma(\sqrt{p}\,) = -\sqrt{p}$. Then $\sigma(\sqrt{q}\,\zeta_n) = -\sqrt{q}\,\zeta_n$.
(ii) First, $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$ if and only if there is an element $\sigma_r \in G_n$ such that $\sigma_r(\sqrt{q}\,\zeta_n) = \chi(r)\sqrt{q}\,\zeta_n^r = -\sqrt{q}\,\zeta_n$. If $\chi(r) = -1$, then $\zeta_n^r = \zeta_n$ and $\sigma_r = 1$, which is impossible. If $\chi(r) = 1$, then $\zeta_n^r = -\zeta_n$ and hence $4|n$ and $r = n/2+1$ by (2.1). This concludes our assertion (2.6). $\square$

Proposition 2.3. *Let n and q be as in Lemma 2.2.*
(a) *Suppose that $p = 2$. Then*

$$\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff 8 \nmid n \text{ or } 16|n. \tag{2.7}$$

(b) *Suppose that $p \equiv 1 \pmod 4$. Then*

$$\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff p \nmid n \text{ or } 4p|n. \tag{2.8}$$

(c) *Suppose that $p \equiv 3 \pmod 4$. Then*

$$\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff 4p \nmid n \text{ or } 8p|n. \tag{2.9}$$

Proof. (a) By Lemma 2.2, we have $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$ if and only if either $8 \nmid n$, or both $8|n$ and $\chi(n/2+1) = 1$. Suppose $8|n$. Note that $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}\,,\sqrt{-1}\,)$ and $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. It follows that

$$\chi(r) = \begin{cases} 1 & \text{if } r \equiv 1, 7 \pmod 8; \\ -1 & \text{if } r \equiv 3, 5 \pmod 8. \end{cases} \tag{2.10}$$

If $8||n$, then $r = n/2 + 1 \equiv 5 \pmod 8$ and $\chi(r) = -1$. If $16|n$, then $r = n/2 + 1 \equiv 1 \pmod 8$ and $\chi(r) = 1$. Thus, $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff 8 \nmid n$ or $16|n$.
(b) By Lemma 2.2, we have $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$ if and only if one of the following two conditions holds: (i) $p \nmid n$; (ii) $4p|n$ and $\chi(n/2 + 1) = 1$. If $4p\,|n$, then $\chi(n/2 + 1) = 1$ since $n/2 + 1 \equiv 1 \pmod p$. Thus, $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff p \nmid n$ or $4p|n$.
(c) By Lemma 2.2, we have $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$ if and only if one of the following two conditions holds: (i) $4p \nmid n$; (ii) $4p\,|n$ and $\chi(n/2 + 1) = 1$. Suppose that $4p|n$ and write $G_{4p} = G_4 \times G_p$. Since $r = n/2 + 1 \equiv 1 \pmod p$, the image of σ_r in G_p is trivial. In particular, it fixes $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$. As $\sqrt{-p} \cdot \sqrt{-1} = -\sqrt{p}$, one has $\chi(r) = 1$ if and only if $r \equiv 1 \pmod 4$. Write $n = 4pk$ for some integer k. Then $r = 2pk + 1 \equiv 1 \pmod 4$ if and only if $k \equiv 0 \pmod 2$. Therefore, we get $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n \iff 4p \nmid n$ or $8p|n$. $\square$

As typical examples, we have (a) $\sqrt{2}\,\zeta_8 \not\sim -\sqrt{2}\,\zeta_8$ and $\sqrt{2}\,\zeta_{16} \sim -\sqrt{2}\,\zeta_{16}$, (b) $\sqrt{5}\,\zeta_5 \not\sim -\sqrt{5}\,\zeta_5$ and $\sqrt{5}\,\zeta_{20} \sim -\sqrt{5}\,\zeta_{20}$, and (c) $\sqrt{3}\,\zeta_{12} \not\sim -\sqrt{3}\,\zeta_{12}$ and $\sqrt{3}\,\zeta_{24} \sim -\sqrt{3}\,\zeta_{24}$.

Corollary 2.4. *Suppose that q is an odd power of p and $n \not\equiv 2 \pmod 4$.*
(1) *If $p \equiv 1 \pmod 4$, then*

$$W_q^{\rm ss} = \{\sqrt{q}\,\zeta_n\,;\, n \not\equiv 2 \pmod 4\,\} \cup \{-\sqrt{q}\,\zeta_n\,;\, 2 \nmid n \text{ and } p|n\,\}.$$

(2) *If $p \equiv 3 \pmod 4$ or $p = 2$, then*

$$W_q^{\rm ss} = \{\sqrt{q}\,\zeta_n\,;\, n \not\equiv 2 \pmod 4\,\} \cup \{-\sqrt{q}\,\zeta_n\,;\, 4p \mid n \text{ and } 8p \nmid n\,\}.$$

Proof. (1) By Proposition 2.3, $\sqrt{q}\,\zeta_n \not\sim -\sqrt{q}\,\zeta_n$ if and only if $p|n$ and $4p \nmid n$, i.e. $p|n$ and $2 \nmid n$. (2) We have $\sqrt{q}\,\zeta_n \not\sim -\sqrt{q}\,\zeta_n$ if and only if $4p|n$ and $8p \nmid n$. □

DEFINITION 2.5. Let $\mathfrak{d}_q$ be the smallest positive integer such that $\mathbb{Q}(\sqrt{q}\,) \subset \mathbb{Q}(\zeta_{\mathfrak{d}_q})$. More specifically, $\mathfrak{d}_q = \mathfrak{d}_p$ if q is an odd power of p, otherwise $\mathfrak{d}_q = 1$. We say a positive integer n is *critical at* q if $\mathfrak{d}_q|n$ and $2\mathfrak{d}_q \nmid n$.

It is clear from the definition that for a fixed $n \in \mathbb{N}$, the condition that n is critical at $q = p^a$ depends only on p and the parity of a.

PROPOSITION 2.6. *Let $n \not\equiv 2 \pmod 4$ be a positive integer and $q = p^a$ a power of a prime number p. Then $\sqrt{q}\,\zeta_n \sim -\sqrt{q}\,\zeta_n$ if and only if n is not critical at q.*

Proof. The proposition reduces to either (2.2) or Proposition 2.3 according to whether a is even or odd respectively. □

COROLLARY 2.7. *We have*

$$W_q^{\mathrm{ss}} = \{\sqrt{q}\,\zeta_n\,;\, n \not\equiv 2 \pmod 4\,\} \cup \{-\sqrt{q}\,\zeta_n\,;\, n \not\equiv 2 \pmod 4 \text{ and } n \text{ is critical at } q\,\}.$$

3. DIMENSION OF SUPERSINGULAR ABELIAN VARIETIES

3.1. Let $q = p^a$ be a power of a prime number p, and π a supersingular Weil q-number as in the previous section. Replacing π by a suitable conjugate, we may assume that $\pi = \pm\sqrt{q}\,\zeta_n$ for a positive integer n with $n \not\equiv 2 \pmod 4$. Let X_π be a simple abelian variety over $\mathbb{F}_q$ in the isogeny class corresponding to π. Its endomorphism algebra $\mathcal{E} = \mathcal{E}_\pi := \mathrm{End}^0(X_\pi)$ is a central division algebra over $K := \mathbb{Q}(\pi)$, unique up to isomorphism depending only on π and not on the choice of X_π. The field K is either a totally real field or a CM field [18, Section 1]. The goal of this section is to determine the dimension $d(\pi)$ of X_π. For each $d \in \mathbb{N}$, define

$$W_q^{\mathrm{ss}}(d) := \{\pi \in W_q^{\mathrm{ss}} \mid d(\pi) = d\}. \tag{3.1}$$

According to the Honda-Tate theory (ibid.), one has

$$d(\pi) = \frac{1}{2}[K:\mathbb{Q}]\sqrt{[\mathcal{E}:K]} = \frac{1}{2}\deg_{\mathbb{Q}}(\mathcal{E}).$$

(For a semisimple algebra over a field F, its F-degree is the degree of any of its maximal commutative semi-simple F-subalgebras.) Moreover, the invariants of $\mathcal{E}$ at a place v of K is given by

$$\mathrm{inv}_v(\mathcal{E}) = \begin{cases} 1/2 & \text{if } v \text{ is real;} \\ [K_v:\mathbb{Q}_p]v(\pi)/v(q) & \text{if } v|p; \\ 0 & \text{otherwise.} \end{cases}$$

Here K_v is the completion of K at the place v. Observe that $d(\pi) = d(-\pi)$. As $v(\pi)/v(q) = 1/2$ for all $v|p$, every invariant $\mathrm{inv}_v(\mathcal{E})$ is a 2-torsion. It follows from the Albert-Brauer-Hasse-Noether theorem that $\mathcal{E}$ is either a quaternion K-algebra or the field K itself (henceforth labeled as case (Q) or (F) respectively).

3.2. TOTALLY REAL CASE. The case where K is a totally real field is well known.
(a) If a is even, then $K = \mathbb{Q}$ and $\mathcal{E}$ is the quaternion algebra over $\mathbb{Q}$ ramified exactly at $\{p, \infty\}$. One has $\pi = \pm p^{a/2}$ (two isogeny classes) and $d(\pi) = 1$.
(b) If a is odd, then $K = \mathbb{Q}(\sqrt{p})$ and $\mathcal{E}$ is the quaternion algebra over K ramified exactly at the two real places $\{\infty_1, \infty_2\}$ of K. One has $\pi = q^{1/2}$ (one isogeny class) and $d(\pi) = 2$.

3.3. CM CASE. Consider the case where K is a CM field, i.e., $n > 2$. Put $L := \mathbb{Q}(\sqrt{q}, \zeta_n) \supseteq K$. As K and L are abelian extensions of $\mathbb{Q}$, the degree $[K_v : \mathbb{Q}_p]$ is even for one $v|p$ if and only if it is so for all $v|p$. Thus, we have the following two possibilities:

(F) $[K_v : \mathbb{Q}_p]$ is even for all $v|p$.
(Q) $[K_v : \mathbb{Q}_p]$ is odd for all $v|p$.

As K is CM, Condition (F) holds if and only if all invariants of $\mathcal{E}$ vanish. In this case $\mathcal{E} = K$ and $d(\pi) = [K : \mathbb{Q}]/2$.

3.4. THE CASE WHERE a IS EVEN. Suppose that $n > 2$. One has $K = \mathbb{Q}(\zeta_n)$ and $[K : \mathbb{Q}] = \varphi(n)$. Thus,

$$d(\pi) = \begin{cases} \varphi(n)/2 & \text{if (F) holds;} \\ \varphi(n) & \text{if (Q) holds.} \end{cases} \tag{3.2}$$

The ramification index of any ramified prime p in $\mathbb{Q}(\zeta_n)$ is even, so if $p \mid n$, then (F) holds. When $p \nmid n$, Condition (F) holds if and only if the order of $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ is even. In particular, if $[K : \mathbb{Q}]$ is a power of 2, then Condition (Q) holds if and only if $K_v = \mathbb{Q}_p$, or equivalently $p \equiv 1 \pmod{n}$. We have the following list, which enables us to list concretely all π with small values of $d(\pi)$.

$n \not\equiv 2 \pmod 4$	3	4	5	7	8	9	11	12	15	16	20	21	24	rest
$d(\pi)$, (Q) holds	2	2	4	6	4	6	10	4	8	8	8	12	8	> 8
$d(\pi)$, (F) holds	1	1	2	3	2	3	5	2	4	4	4	6	4	> 4

PROPOSITION 3.1. *Let $\pi = \pm\sqrt{q}\,\zeta_n$ be a supersingular Weil q-number with $n \geq 1$ and $n \not\equiv 2 \pmod 4$. Suppose that $q = p^a$ is an even power of p.*

(1) We have $d(\pi) = 1$ if and only if $n = 1$, or $n = 3, 4$ and $p \not\equiv 1 \pmod{n}$.
(2) We have $d(\pi) = 2$ if and only if
  (a) $n = 3, 4$ and $p \equiv 1 \pmod{n}$, or
  (b) $n = 5, 8, 12$ and $p \not\equiv 1 \pmod{n}$.
(3) We have $d(\pi) = 3$ if and only if $n = 7$ and $p \not\equiv 1, 2, 4 \pmod 7$, or $n = 9$ and $p \not\equiv 1, 4, 7 \pmod 9$.
(4) We have $d(\pi) = 4$ if and only if
  (a) $n = 5, 8, 12$ and $p \equiv 1 \pmod{n}$, or
  (b) $n = 15, 16, 20, 24$ and $p \not\equiv 1 \pmod{n}$.

3.5. THE CASE WHERE a IS ODD. Suppose that $n > 1$ and $n \not\equiv 2 \pmod 4$. Put

$$m := \begin{cases} n/2 & \text{if } n \text{ is even,} \\ n & \text{if } n \text{ is odd,} \end{cases} \quad \text{and} \quad K := \mathbb{Q}(\sqrt{p}\,\zeta_n). \tag{3.3}$$

We have the following towers of number fields.

$$\begin{tikzcd}[column sep=small] & L = \mathbb{Q}(\sqrt{p}\,, \zeta_n) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{p}\,, \zeta_m) \arrow[dr, dash] & K = \mathbb{Q}(\sqrt{p}\,\zeta_n) \arrow[d, dash] & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\ & E = \mathbb{Q}(\zeta_m) & \end{tikzcd} \tag{3.4}$$

Note that the prime p is ramified in K with even ramification index, and hence Condition (F) always holds. Therefore,

$$\mathcal{E} = K \quad \text{and} \quad d(\pi) = \frac{1}{2}\,[K : \mathbb{Q}]. \tag{3.5}$$

LEMMA 3.2. *Let K and E be as in (3.4). We have $K = E$ if and only if n is critical at q.*

Proof. Clearly $[K : E] = 1$ or 2. If $\pi \sim -\pi$, then $\pi \mapsto -\pi$ induces a nontrivial automorphism of K with fixed field E. Thus, $\pi \sim -\pi$ if and only if $[K : E] = 2$. By Proposition 2.6, $[K : E] = 1$ if and only if n is critical at q. Note that the lemma also holds when a is even with $K = \mathbb{Q}(\sqrt{q}\,\zeta_n) = \mathbb{Q}(\zeta_n)$. $\square$

LEMMA 3.3. *Suppose that a is odd and $n > 1$ with $4 \nmid n$. Then*

$$d(\pi) = \frac{1}{2}[K : \mathbb{Q}] = \begin{cases} \varphi(n)/2 & \text{if } p \,|\, n \text{ and } p \equiv 1 \pmod 4; \\ \varphi(n) & \text{otherwise.} \end{cases} \tag{3.6}$$

Proof. Since n is odd one has $E = \mathbb{Q}(\zeta_n)$ and $[E : \mathbb{Q}] = \varphi(n)$. We have $\mathfrak{d}_q = p$ or $4p$ according as $p \equiv 1 \pmod 4$ or not. It is easy to see that n is critical at q if and only if $p \equiv 1 \pmod 4$ and $p|n$. The assertion then follows from Lemma 3.2 and (3.5). $\square$

LEMMA 3.4. *Suppose that a is odd and $n = 4k$ with $k \in \mathbb{N}$. Then*

$$d(\pi) = \frac{1}{2}[K : \mathbb{Q}] = \begin{cases} \varphi(n)/4 & \text{if } p \not\equiv 1 \pmod 4,\ 4p \mid n \text{ and } 8p \nmid n; \\ \varphi(n)/2 & \text{otherwise.} \end{cases}$$

Proof. Since $4|n$ we have $[E : \mathbb{Q}] = \varphi(n)/2$. By Lemma 3.2 we have $[K : \mathbb{Q}] = \delta_n \varphi(n)/2$, where $\delta_n = 1$ or 2 depending on whether n is critical at q or not. The lemma follows once we note that $n = 4k$ is never critical when $p \equiv 1 \pmod 4$. $\square$

The following are tables of $d(\pi)$ for $\pi=\sqrt{q}\,\zeta_n$ with $4\nmid n$ and $4|n$, respectively. The symbol $(*)$ denotes the primes satisfying the conditions $p\,|n$ and $p\equiv 1\,(4)$, and $(**)$ denotes the primes satisfying the three conditions $p\not\equiv 1 \pmod 4$, $4p\mid n$ and $8p\nmid n$. For the sake of completeness, the case $n=1$ is included and also marked with a $\natural$ to make a distinction.

n odd	$1^\natural$	3	5	7	9	11	13	15	rest
$\varphi(n)$	1	2	4	6	6	10	12	8	>8
$(*)$	$\emptyset$	$\emptyset$	$p=5$	$\emptyset$	$\emptyset$	$\emptyset$	$p=13$	$p=5$	
$d(\pi)$	2	2	$2\ (p=5)$ $4\ (p\neq 5)$	6	6	10	$6\ (p=13)$ $12\ (p\neq 13)$	$4\ (p=5)$ $8\ (p\neq 5)$	>4

$n=4k$	4	8	12	16	20	24	28
$\varphi(n)$	2	4	4	8	8	8	12
$(**)$	$\emptyset$	2	3	$\emptyset$	$\emptyset$	2	7
$d(\pi)$	1	$1\ (p=2)$ $2\ (p\neq 2)$	$1\ (p=3)$ $2\ (p\neq 3)$	4	4	$2\ (p=2)$ $4\ (p\neq 2)$	$3\ (p=7)$ $6\ (p\neq 7)$

$n=4k$	32	36	40	44	48	56	60
$\varphi(n)$	16	12	16	20	16	24	16
$(**)$	$\emptyset$	$p=3$	$p=2$	$p=11$	$\emptyset$	$p=2$	$p=3$
$d(\pi)$	8	$3\ (p=3)$ $6\ (p\neq 3)$	$4\ (p=2)$ $8\ (p\neq 2)$	$5\ (p=11)$ $10\ (p\neq 11)$	8	$6\ (p=2)$ $12\ (p\neq 2)$	$4\ (p=3)$ $8\ (p\neq 3)$

It is easy to see that when $4|n$ and either $n=52$ or $n>60$, the value $\varphi(n)>16$ and hence $d(\sqrt{q}\,\zeta_n)>4$.

Proposition 3.5. *Suppose that $q=p^a$ is an odd power of p.*

(1) $W_q^{\rm ss}(1)$ consists of

$$\sqrt{q}\,\zeta_4,\ \pm\sqrt{q}\,\zeta_8\ (p=2),\ \pm\sqrt{q}\,\zeta_{12}\ (p=3).$$

(2) $W_q^{\rm ss}(2)$ consists of

$$\sqrt{q}\,,\ \sqrt{q}\,\zeta_3,\ \pm\sqrt{q}\,\zeta_5\ (p=5),\ \sqrt{q}\,\zeta_8\ (p\neq 2),\ \sqrt{q}\,\zeta_{12}\ (p\neq 3),\ \pm\sqrt{q}\,\zeta_{24}\ (p=2).$$

(3) $W_q^{\rm ss}(3)$ consists of $\pm\sqrt{q}\,\zeta_{28}$ if $p=7$, or $\pm\sqrt{q}\,\zeta_{36}$ if $p=3$.

(4) $W_q^{\rm ss}(4)$ consists of

$$\sqrt{q}\,\zeta_5\ (p\neq 5),\ \pm\sqrt{q}\,\zeta_{15}\ (p=5),\ \sqrt{q}\,\zeta_{16},$$
$$\sqrt{q}\,\zeta_{20},\ \sqrt{q}\,\zeta_{24}\ (p\neq 2),\ \pm\sqrt{q}\,\zeta_{40}\ (p=2),\ \pm\sqrt{q}\,\zeta_{60}\ (p=3).$$

4. Supersingular elliptic curves over finite fields

4.1. Isogeny classes over finite fields. Let $\mathcal{I}sog_q$ denote the set of isogeny classes of abelian varieties over $\mathbb{F}_q$, where $q=p^a$ is a power of the prime number p. Let $\mathbb{Z}W_q$ be the free abelian group (written multiplicatively) generated by the set W_q of conjugacy classes of Weil q-numbers. A nontrivial element $\pi\in\mathbb{Z}W_q$ can be put in the form $\pi_1^{m_1}\times\cdots\times\pi_r^{m_r}$ for some $r\in\mathbb{N}$, where each $\pi_i\in W_q$, $\pi_i\not\sim\pi_j$ if $i\neq j$, and $m_i\neq 0$ for all $1\le i\le r$. Such an element is called a *multiple Weil q-number* if $m_i>0$ for all i, and the set of all these elements is denoted by MW_q. Put $X_\pi:=\prod_i X_{\pi_i}^{m_i}$, where X_{π_i} is the

simple abelian variety (up to isogeny) over $\mathbb{F}_q$ corresponding to π_i. The Honda-Tate theorem naturally extends to a bijection $MW_q \simeq \mathcal{I}sog_q$ which sends each $\pi \in MW_q$ to the isogeny class $[X_\pi] \in \mathcal{I}sog_q$ of X_π.
For each $\pi \in MW_q$, we define its *dimension* as

$$d(\pi) := \dim X_\pi = \sum_{i=1}^{r} m_i d(\pi_i).$$

Let $\mathrm{Isog}(\pi) = \mathrm{Isog}(X_\pi)$ denote the set of $\mathbb{F}_q$-isomorphism classes of abelian varieties isogenous to X_π over $\mathbb{F}_q$, and denote $H(\pi) := |\mathrm{Isog}(\pi)|$. Let $MW_q^{\mathrm{ss}} \subset MW_q$ be the subset of supersingular multiple Weil q-numbers, i.e. those $\pi \in MW_q$ whose corresponding abelian varieties X_π are supersingular. For any integer $d \geq 1$, let $MW_q(d)$ (resp. $MW_q^{\mathrm{ss}}(d)$) denote the subset consisting of all elements π in MW_q (resp. in MW_q^{ss}) of dimension d. Let $S_d(\mathbb{F}_q)$ (resp. $\mathrm{Sp}_d(\mathbb{F}_q)$) be the set of isomorphism classes of d-dimensional supersingular (resp. superspecial) abelian varieties over $\mathbb{F}_q$. When $\pi \in MW_q^{\mathrm{ss}}$, we let $\mathrm{Sp}(\pi) \subset \mathrm{Isog}(\pi)$ be the subset consisting of superspecial isomorphism classes and denote $H_{sp}(\pi) := |\mathrm{Sp}(\pi)|$. Thus,

$$|S_d(\mathbb{F}_q)| = \sum_{\pi \in MW_q^{\mathrm{ss}}(d)} H(\pi), \quad |\mathrm{Sp}_d(\mathbb{F}_q)| = \sum_{\pi \in MW_q^{\mathrm{ss}}(d)} H_{\mathrm{sp}}(\pi). \tag{4.1}$$

4.2. Supersingular elliptic curves. We compute the number $|S_1(\mathbb{F}_q)|$ of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_q$, where $q = p^a$ as before. The method is based almost entirely on the results of Waterhouse [21], except certain details need to be cleared up (compare with [21, Theorem 4.5]).

Proposition 4.1. *Let π be the Frobenius endomorphism of an elliptic curve E_0 over $\mathbb{F}_q$, and $K := \mathbb{Q}(\pi)$. Assume that $\pi \notin \mathbb{Q}$ so that K is an imaginary quadratic field. Equivalently, the central K-algebra $\mathrm{End}^0(E_0)$ of the elliptic curve E_0 is assumed to be commutative and thus necessarily an imaginary quadratic field.*

1. *Any endomorphism ring $R = \mathrm{End}(E)$ of an elliptic curve E in the isogeny class $[E_0]$ of E_0 contains π and is maximal at p, that is, $R \otimes \mathbb{Z}_p$ is the maximal order in $K \otimes \mathbb{Q}_p$. Conversely, any order R of K satisfying these two properties occurs as an endomorphism ring of an elliptic curve in this isogeny class.*
2. *Suppose that $R \subset K$ is a quadratic order as in (1). Then the Picard group $\mathrm{Pic}(R)$ of R acts freely on the set $[E_0]_R \subset [E_0]$ of isomorphism classes of elliptic curves in $[E_0]$ with endomorphism ring R. Moreover, the number N of orbits is 2 if p is inert in K and a is even, and $N = 1$ otherwise.*

Proof. Statement (1) is [21, Theorem 4.2]. We give a proof of the second part of Statement (2) since it differs from [21, Theorem 4.5] in some cases. We assert that the statement of [21, Theorem 5.1] for principal abelian varieties is directly applicable to this situation. Namely, the number of orbits here

is also given by $N = \prod_{v|p} N_v$, where v runs through the set of all places of K over p, and each N_v is the number described as follows. Let e_v and f_v be the ramification index and residue degree of v, respectively, and set $g_v = \gcd(f_v, a)$ and $m_v := g_v \operatorname{ord}_v(\pi)/a$. Note that m_v is an integer since $\operatorname{End}^0(E_0)$ is commutative and thus $f_v \operatorname{ord}_v(\pi)/a \in \mathbb{N}$. Then N_v is the number of all g_v-tuples $(n_1, \dots, n_{g_v})$ of integers satisfying $0 \le n_j \le e_v$ and $\sum_{j=1}^{g_v} n_j = m_v$. In the present situation $\operatorname{End}^0(E_0) = K$ is commutative and R is maximal at p. As in the proof of [21, Theorem 5.1], to find the number of orbits for the action of $\operatorname{Pic}(R)$ on $[E_0]_R$, one needs to classify the Tate-modules $T_\ell E$ at all primes $\ell \ne p$ and the Dieudonné modules at the prime p of $E \in [E_0]_R$. The number of orbits is then the product of the number of isomorphism classes of the above modules at each prime.
The Tate-module $T_\ell E$ of each $E \in [E_0]_R$ at a prime $\ell \ne p$ is naturally an R_ℓ-module with $R_\ell = R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Since $R[1/p]$ is a quadratic order, any fractional $R[1/p]$-ideal I whose order ring equals $R[1/p]$ must be locally free over $R[1/p]$. Particularly, there is only one isomorphism class of the prime-to-p Tate modules of E for all $E \in [E_0]_R$. Thus, N is equal to the number of isomorphism classes of Dieudonné modules occurring in the isogeny class $[E_0]$, which is equal to $\prod_v N_v$ as given in the proof of [21, Theorem 5.1].
Now it is easy to compute the number N of orbits. Notice $N_v \ne 1$ only when $g_v > 1$. For our case with $[K : \mathbb{Q}] = 2$ this occurs only when p is inert in K and a is even. In this case there is only one place v over p, $g_v = 2$ and $e_v = 1$. Then $N = N_v$ is the number of pairs (n_1, n_2) with $0 \le n_1, n_2 \le 1$ and $n_1 + n_2 = 1$, which is 2. □

Remark 4.2. In [21, Theorem 5.1] the assumption that the endomorphism ring $R = \operatorname{End}(A)$ is the maximal order can be replaced by the weaker assumption that R is both Gorenstein and maximal at p. Indeed, any proper R-lattice of rank one over a Gorenstein order R is locally free [5, Theorem 37.16 p. 789], so the same proof of [21, Theorem 5.1] applies.

Remark 4.3. Suppose that a is even and p is inert in the imaginary quadratic field $K = \mathbb{Q}(\pi)$ so that $N = 2$. By the classification of Waterhouse ([21, Lemma, p.537], see also Proposition 3.1), this occurs only for supersingular Weil q-numbers π where

$$\pi \sim \pm p^{a/2}\zeta_3,\ p \equiv 2 \pmod 3 \quad \text{or} \quad \pi \sim p^{a/2}\zeta_4,\ p \equiv 3 \pmod 4. \tag{4.2}$$

Then by part (1) of Proposition 4.1, $\operatorname{End}(E) = O_K$ for any elliptic curve E in the isogeny class corresponding to π. Since $h(O_K) = 1$, part (2) of Proposition 4.1 implies that a complete set of representatives of $\operatorname{Sp}(\pi)$ consists a pair of elliptic curves of the form $\{E, E^{(p)}\}$, where $E^{(p)} := E \otimes_{\mathbb{F}_q, \sigma_p} \mathbb{F}_q$, and $\sigma_p \in \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is the Frobenius automorphism of $\mathbb{F}_q/\mathbb{F}_p$. These two elliptic curves are distinguished by the actions of O_K on the respective 1-dimensional Lie-algebras $\operatorname{Lie}(E)$ and $\operatorname{Lie}(E^{(p)})$ over $\mathbb{F}_q$, which are given by distinct embeddings $O_K/(p) \simeq \mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_q$. This establishes a natural bijection $\operatorname{Sp}(\pi) \simeq \operatorname{Hom}(O_K/(p), \mathbb{F}_q)$ for every π in (4.2).

We return to the calculation of $|\,\mathrm{Sp}_1(\mathbb{F}_q)|$ by the counting method. The isogeny classes of supersingular elliptic curves over $\mathbb{F}_q$ are completely listed by the following Weil numbers

$$\begin{aligned} &W_q^{\mathrm{ss}}(1)=\{\sqrt{q}\,\zeta_4,\ \pm\sqrt{q}\,\zeta_8\ (p=2),\ \pm\sqrt{q}\,\zeta_{12}\ (p=3)\,\},\quad \text{for } a \text{ odd};\\ &W_q^{\mathrm{ss}}(1)=\{\pm\sqrt{q}\,,\ \pm\sqrt{q}\,\zeta_3\ (p\not\equiv 1\,(3)),\ \sqrt{q}\,\zeta_4\ (p\not\equiv 1\,(4))\,\},\quad \text{for } a \text{ even}. \end{aligned} \tag{4.3}$$

For each Weil q-number $\pi\in W_q^{\mathrm{ss}}(1)$, let R_0 be the smallest quadratic order in $K=\mathbb{Q}(\pi)$ which contains π and is maximal at p. It is easy to see that R_0 is the maximal order except when $\pi=\sqrt{q}\,\zeta_4$, $p\equiv 3 \pmod 4$ and a is odd. In the latter case $R_0=\mathbb{Z}[\sqrt{-p}\,]$ and we have by Proposition 4.1 that

$$H(\sqrt{q}\,\zeta_4)=\begin{cases} h(O_K) & \text{for } p=2 \text{ or } p\equiv 1 \pmod 4;\\ h(R_0)+h(O_K) & \text{for } p\equiv 3 \pmod 4. \end{cases} \tag{4.4}$$

For the other cases, the order R_0 is maximal and we have

$$H(\pi)=N\cdot h(O_K) \tag{4.5}$$

where $N=2$ if p is inert in K and a is even, and $N=1$ otherwise. Recall that for a square free $m\in\mathbb{Z}$, the class number of $\mathbb{Q}(\sqrt{m}\,)$ is denoted by $h(\sqrt{m}\,)$. Suppose first that a is odd. For $p=2$, we have

$$|\,\mathrm{Sp}_1(\mathbb{F}_q)|=H(\sqrt{q}\,\zeta_4)+2H(\sqrt{q}\,\zeta_8)=h(\sqrt{-2}\,)+2h(\sqrt{-1}\,)=3. \tag{4.6}$$

For $p=3$, we have

$$\begin{aligned} |\,\mathrm{Sp}_1(\mathbb{F}_q)| &= H(\sqrt{q}\,\zeta_4)+2H(\sqrt{q}\,\zeta_{12})\\ &= h(\mathbb{Z}[\sqrt{-3}\,])+h(\sqrt{-3}\,)+2h(\sqrt{-3}\,)=4. \end{aligned} \tag{4.7}$$

For $p>3$, we have by [26, Theorem 1.1] that

$$\begin{aligned} |\,\mathrm{Sp}_1(\mathbb{F}_q)| &= H(\sqrt{q}\,\zeta_4)\\ &= \begin{cases} h(\sqrt{-p}\,) & \text{for } p\equiv 1 \pmod 4;\\ 2h(\sqrt{-p}\,) & \text{for } p\equiv 7 \pmod 8 \ (2 \text{ splits in } \mathbb{Q}(\sqrt{-p}\,))\ ;\\ 4h(\sqrt{-p}\,) & \text{for } p\equiv 3 \pmod 8 \ (2 \text{ is inert in } \mathbb{Q}(\sqrt{-p}\,)). \end{cases} \end{aligned} \tag{4.8}$$

Since $\left(\frac{2}{p}\right)=1$ for $p\equiv 1,7 \pmod 8$ and $\left(\frac{2}{p}\right)=-1$ for $p\equiv 3,5 \pmod 8$, we can rewrite (4.8) as

$$|\,\mathrm{Sp}_1(\mathbb{F}_q)|=\begin{cases} h(\sqrt{-p}\,) & \text{for } p\equiv 1 \pmod 4;\\ \left(3-\left(\frac{2}{p}\right)\right)h(\sqrt{-p}\,) & \text{for } p\equiv 3 \pmod 4. \end{cases} \tag{4.9}$$

Suppose now that a is even. By (4.3), we have

$$|\,\mathrm{Sp}_1(\mathbb{F}_q)|=2H(\sqrt{q}\,)+2\delta_3(p)H(\sqrt{q}\,\zeta_3)+\delta_4(p)H(\sqrt{q}\,\zeta_4), \tag{4.10}$$

where $\delta_m(p)=1,0$ according as $p\not\equiv 1 \pmod m$ or not for $m=3,4$. It is well known that $H(\sqrt{q}\,)$ is equal to the class number $h(B_{p,\infty})$ of the quaternion

$\mathbb{Q}$-algebra $B_{p,\infty}$ ramified only at p and ∞. Thus,

$$H(\sqrt{q}\,) = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right). \tag{4.11}$$

By Proposition 4.1, we have

$$\delta_3(p)H(\sqrt{q}\,\zeta_3) = \begin{cases} 1 & \text{for } p = 3; \\ 2 & \text{for } p \equiv 2 \pmod 3; \\ 0 & \text{for } p \equiv 1 \pmod 3; \end{cases} \tag{4.12}$$

and get $\delta_3(p)H(\sqrt{q}\,\zeta_3) = 1 - \left(\frac{-3}{p}\right)$. Similarly, we have $\delta_4(p)H(\sqrt{q}\,\zeta_4) = 1 - \left(\frac{-4}{p}\right)$. Using (4.10) and (4.11), we get

$$\begin{aligned} |\operatorname{Sp}_1(\mathbb{F}_q)| &= \frac{p-1}{6} + \frac{2}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right) \\ &\quad + 2\left(1 - \left(\frac{-3}{p}\right)\right) + \left(1 - \left(\frac{-4}{p}\right)\right) \\ &= \frac{p-1}{6} + \frac{8}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{3}{2}\left(1 - \left(\frac{-4}{p}\right)\right). \end{aligned} \tag{4.13}$$

From (4.6), (4.7), (4.9) and (4.13), we obtain an explicit formula for the number $|\operatorname{Sp}_1(\mathbb{F}_q)|$ of supersingular elliptic curves over $\mathbb{F}_q$.

PROPOSITION 4.4. *Suppose $q = p^a$ is a power of the prime number p.*

(1) If a is odd, then

$$|\operatorname{Sp}_1(\mathbb{F}_q)| = \begin{cases} 3, 4 & \textit{for } p = 2, 3, \textit{ respectively;} \\ h(\sqrt{-p}\,) & \textit{for } p \equiv 1 \pmod 4; \\ \left(3 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}\,) & \textit{for } p \equiv 3 \pmod 4 \textit{ and } p > 3. \end{cases} \tag{4.14}$$

(2) If a is even, then

$$|\operatorname{Sp}_1(\mathbb{F}_q)| = \frac{p-1}{6} + \frac{8}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{3}{2}\left(1 - \left(\frac{-4}{p}\right)\right). \tag{4.15}$$

REMARK 4.5. From the formulas above we observe a phenomenon that the number $|\operatorname{Sp}_1(\mathbb{F}_q)|$ depends only on the parity of the exponent a of $q = p^a$. We have already seen in Section 2 that the classification of supersingular isogeny classes depends only on the parity of a. More explicitly, if the exponents a and a' of q and q' respectively have the same parity, then a bijective correspondence between supersingular isogeny classes over $\mathbb{F}_q$ and those over $\mathbb{F}_{q'}$ can be given by matching $\pi \in W_q^{\mathrm{ss}}(1)$ with $\pi' = (-p)^{(a'-a)/2}\pi$ (see Remark 6.8). The parity phenomenon of $|\operatorname{Sp}_1(\mathbb{F}_q)|$ arises because there is a bijection $\operatorname{Sp}(\pi) \simeq \operatorname{Sp}(\pi')$ for all pairs (π, π') as above. Indeed, if π and π' are of the form in (4.2), then a canonical bijection $\operatorname{Sp}(\pi) \simeq \operatorname{Sp}(\pi')$ is given by identifying both with $\operatorname{Hom}(O_K/(p), \mathbb{F}_q)$ as in Remark 4.3. For the remaining cases, first suppose that $K = \mathbb{Q}(\pi) = \mathbb{Q}(\pi')$ is imaginary quadratic. Then the endomorphism rings occurring for both isogeny classes are the same by Proposition 4.1. We partition $\mathrm{Sp}(\pi)$ into $\coprod_R \mathrm{Sp}(\pi, R)$, where R runs over all possible endomorphism rings, and $\mathrm{Sp}(\pi, R) \subseteq \mathrm{Sp}(\pi)$ consists of those members with endomorphism ring R. Every $\mathrm{Sp}(\pi, R)$ is a principal homogeneous space of $\mathrm{Pic}(R)$. Thus a $\mathrm{Pic}(R)$-equivariant bijection between $\mathrm{Sp}(\pi, R)$ and $\mathrm{Sp}(\pi', R)$ is established whenever a base point is chosen respectively in each of them. Lastly, suppose that $\mathbb{Q}(\pi) = \mathbb{Q}(\pi') = \mathbb{Q}$. Then $\pi^{a'} = (\pi')^a = p^{aa'/2}$. So we have canonical bijections $\mathrm{Sp}(\pi) \simeq \mathrm{Sp}(\pi^{a'}) \simeq \mathrm{Sp}(\pi')$ by extending both base fields to $\mathbb{F}_{p^{aa'}}$ ([21, Remark, p. 542]). Equivalently, the bijection $\mathrm{Sp}(\pi) \simeq \mathrm{Sp}(\pi')$ can be obtained by matching the j-invariants.

5. Superspecial abelian surfaces over $\mathbb{F}_p$

In this section we assume that the ground field is the prime field $\mathbb{F}_p$; abelian varieties and their morphisms are all defined over $\mathbb{F}_p$ unless otherwise stated.

5.1. Supersingular abelian varieties over $\mathbb{F}_p$. We describe a result which allows us to count supersingular and superspecial abelian varieties over $\mathbb{F}_p$, based on a result of Waterhouse [21, Theorem 6.1 (3)] (see also [26, Theorem 3.1] for an extension to non-simple isogenies).

Let X_0 be a fixed supersingular abelian variety over $\mathbb{F}_p$ and let $\pi = \pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$ be a multiple Weil p-number corresponding to the isogeny class $[X_0]$. One has $X_0 \sim \prod_{i=1}^r X_i^{m_i}$, where each X_i with $1 \le i \le r$ is a simple abelian variety with Frobenius endomorphism π_i. The endomorphism algebra $\mathcal{E} = \mathrm{End}^0(X_0)$ of X_0 is equal to $\prod_{i=1}^r \mathrm{Mat}_{m_i}(\mathrm{End}^0(X_i))$. Let $\pi_0 \in \mathrm{End}(X_0)$ be the Frobenius endomorphism. The $\mathbb{Q}$-subalgebra $K = \mathbb{Q}(\pi_0) \subset \mathcal{E}$ generated by π_0 is semi-simple and coincides with the center of $\mathcal{E}$. One has $K = \prod_i K_i$ and $\pi_0 = (\pi_1, \dots, \pi_r)$, where $K_i = \mathbb{Q}(\pi_i)$. Let $\mathcal{R} := \mathbb{Z}[\pi_0, p\pi_0^{-1}] \subset K$ and $\mathcal{R}_{sp} := \mathcal{R}[\pi_0^2/p] \subset K$. Clearly π_0^2/p is an integral element of finite multiplicative order, and $p/\pi_0 = \pi_0 \cdot (\pi_0^2/p)^{-1}$, so $\mathcal{R}_{sp} = \mathbb{Z}[\pi_0, \pi_0^2/p] \subseteq O_K$, where $O_K = \prod_i O_{K_i}$ is the maximal order K. Observe that the Tate module $T_\ell(X_0)$ (for any prime $\ell \ne p$), as a $\mathbb{Z}_\ell[\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)]$-module, is nothing but an $\mathcal{R}_\ell$-module, and the (covariant) Dieudonné module $M(X_0)$ is simply an $\mathcal{R}_p$-module, where $\mathcal{R}_\ell = \mathcal{R} \otimes \mathbb{Z}_\ell$ and $\mathcal{R}_p = \mathcal{R} \otimes \mathbb{Z}_p$.

Proposition 5.1. *Let $\pi = \pi_1^{m_1} \times \dots \pi_r^{m_r}$, and K, $\mathcal{R}$ and $\mathcal{R}_{sp}$ be as above. Assume that K has no real place, that is, none of π_i is conjugate to $\sqrt{p}$, and set $V := \prod_{i=1}^r K_i^{m_i}$.*

1. *There is a natural bijection between the set* $\mathrm{Isog}(\pi)$ *and the set of isomorphism classes of $\mathcal{R}$-lattices in V.*
2. *Under the above map the subset* $\mathrm{Sp}(\pi)$ *is in bijection with the set of isomorphism classes of $\mathcal{R}_{sp}$-lattices in V.*

Proof. Set $\Lambda := \prod_{i=1}^r O_{K_i}^{m_i} \subset V$, and view V and Λ as a K-module and an $\mathcal{R}$-lattice, respectively. We choose an identification $V \otimes_\mathbb{Q} \mathbb{Q}_\ell = T_\ell(X_0) \otimes \mathbb{Q}_\ell$ for primes $\ell \ne p$ and $V \otimes_\mathbb{Q} \mathbb{Q}_p = M(X_0) \otimes \mathbb{Q}_p$ such that $\Lambda_\ell = T_\ell(X_0)$ for almost all primes ℓ. Under this identification, any $\mathcal{R}$-lattice Λ' in V gives rise to a unique quasi-isogeny $\varphi : X \to X_0$ such that $\varphi_*(T_\ell(X)) = \Lambda' \otimes \mathbb{Z}_\ell$ for $\ell \neq p$ and $\varphi_*(M(X)) = \Lambda' \otimes \mathbb{Z}_p$. Two lattices Λ_1 and Λ_2 are isomorphic as $\mathcal{R}$-modules if and only if there is an element $g \in \mathrm{GL}_K(V)$ such that $\Lambda_2 = g\Lambda_1$. Two quasi-isogenies are isomorphic if and only if they differ by an element in $\mathcal{E}^\times$. Our assumption ensures that $\mathrm{GL}_K(V) \simeq \mathcal{E}^\times$. Then the above correspondence induces the desired bijection (also see [26, Theorem 3.1] for a detailed proof). Note that the abelian variety X in $[X_0]$ as above is superspecial if and only if $\pi_0^2 M(X) = pM(X)$, or equivalently, $M(X)$ is a $(\mathcal{R}_{sp})_p$-lattice in $M(X_0) \otimes \mathbb{Q}_p$. That is, X is superspecial if and only if the corresponding $\mathcal{R}$-module is $\mathcal{R}_{sp}$-stable. The statement (2) then follows from (1). □

REMARK 5.2. Let $\pi = \pi_1^{e_1}$ be a multiple supersingular Weil p-number with $\pi_1 = \pm\sqrt{p}\,\zeta_n$ and n critical at p. Then by Lemma 3.2, $K = \mathbb{Q}(\pi_1) = \mathbb{Q}(\zeta_m)$ and $O_K = \mathbb{Z}[\zeta_m]$, where m is defined in (3.3). Since $\mathcal{R}_{sp} = \mathcal{R}[\pi_1^2/p] \ni \zeta_m$, it follows that $\mathcal{R}_{sp}$ coincides with the maximal order O_K in this case.

5.2. PROOF OF THE MAIN THEOREM. By Section 3, we list the sets $W_p^{\mathrm{ss}}(1)$ and $W_p^{\mathrm{ss}}(2)$ of supersingular Weil p-numbers of dimension 1 or 2 as follows:

$$\begin{aligned} W_2^{\mathrm{ss}}(1) &= \{\sqrt{2}\,\zeta_4, \pm\sqrt{2}\,\zeta_8\}, \\ W_3^{\mathrm{ss}}(1) &= \{\sqrt{3}\,\zeta_4, \pm\sqrt{3}\,\zeta_{12}\}, \\ W_p^{\mathrm{ss}}(1) &= \{\sqrt{p}\,\zeta_4\}, \quad p \geq 5; \end{aligned} \tag{5.1}$$

and

$$\begin{aligned} W_2^{\mathrm{ss}}(2) &= \{\sqrt{2}\,, \sqrt{2}\,\zeta_3, \sqrt{2}\,\zeta_{12}, \pm\sqrt{2}\,\zeta_{24}\}, \\ W_3^{\mathrm{ss}}(2) &= \{\sqrt{3}\,, \sqrt{3}\,\zeta_3, \sqrt{3}\,\zeta_8\}, \\ W_5^{\mathrm{ss}}(2) &= \{\sqrt{5}\,, \sqrt{5}\,\zeta_3, \sqrt{5}\,\zeta_8, \sqrt{5}\,\zeta_{12}, \pm\sqrt{5}\,\zeta_5\}, \\ W_p^{\mathrm{ss}}(2) &= \{\sqrt{p}\,, \sqrt{p}\,\zeta_3, \sqrt{p}\,\zeta_8, \sqrt{p}\,\zeta_{12}\}, \quad p \geq 7. \end{aligned} \tag{5.2}$$

Consider the case $\pi \in W_p^{\mathrm{ss}}(2)$ or $\pi = \pi_1 \times \pi_2$ with $\pi_1, \pi_2 \in W_p^{\mathrm{ss}}(1)$. By (4.1) we have

$$|\mathrm{Sp}_2(\mathbb{F}_p)| = \sum_{\pi \in W_p^{\mathrm{ss}}(2)} H_{sp}(\pi) + \sum_{\pi_1, \pi_2 \in W_p^{\mathrm{ss}}(1)} H_{sp}(\pi_1 \times \pi_2). \tag{5.3}$$

The number $H_{sp}(\sqrt{p}\,) = H(\sqrt{p}\,)$ has been calculated in [22], so this case will be excluded from our discussion. We refer to [5, Section 37] for the definition of a Bass order. Note that when $\pi = \pi_1 \times \pi_1$, $\mathcal{R}_{sp}$ is an order in the quadratic field $\mathbb{Q}(\pi_1)$, and such orders are well known to be Bass. It will be shown in Section 7.2 that $\mathcal{R}_{sp}$ is a Bass order for all π considered (i.e. $\pi \in MW_p^{\mathrm{ss}}(2)$). Thus, when the K-module V is free of rank one (i.e. in the case where $\pi \neq \pi_1 \times \pi_1$), Proposition 5.1 gives

$$H_{sp}(\pi) = \sum_{\mathcal{R}_{sp} \subset B \subset O_K} h(B). \tag{5.4}$$

In the case when V is free of higher rank (in fact, rank 2 when $\pi = \pi_1 \times \pi_1$), one can use the results of Borevič and Faddeev on lattices over orders of cyclic index to compute $H_{sp}(\pi)$ (cf. [5, Section 37, p. 789]).
In the following, the notation $B_{\pi,j}$ (or B_j for short) with $j \in \mathbb{N}$, will stand for an order B of K with $\mathcal{R}_{sp} \subset B \subset O_K$ and $[O_K : B] = j$. The dependence of K, $\mathcal{R}_{sp}$ and B_j on the choice of the Weil p-number π should be understood though it is omitted from the notation. For any two square-free integers $d > 1$ and $j \geq 1$, we write $K_{d,j}$ for the CM field $\mathbb{Q}(\sqrt{d}, \sqrt{-j})$. For a finite collection of algebraic numbers $\alpha_1, \dots, \alpha_n$, the notation $h(\alpha_1, \dots, \alpha_n)$ denotes the class number of the number field $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Particularly, $h(\sqrt{d}, \sqrt{-j})$ and $h(K_{d,j})$ have the same meaning.

CASE $\pi = \pi_1 \times \pi_1$. For $\pi_1 = \pm\sqrt{2}\,\zeta_8$, one has $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{R}_{sp} = \mathcal{R} = O_K$, and $H_{sp}(\pi) = H(\pi) = 1$. For $\pi_1 = \pm\sqrt{3}\,\zeta_{12}$, one has $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{R}_{sp} = \mathcal{R} = O_K$, and $H_{sp}(\pi) = H(\pi) = 1$.
For $\pi_1 = \sqrt{-p}$, we have $K = \mathbb{Q}(\sqrt{-p})$, $\mathcal{R}_{sp} = \mathcal{R}$ and $[O_K : \mathcal{R}_{sp}] = 2$ or 1 depending on $p \equiv 3 \pmod 4$ or not. In this case we have $H_{sp}(\pi) = 1, 3$ for $p = 2, 3$, respectively, and

$$H_{sp}(\pi) = \begin{cases} h(\sqrt{-p}) & \text{for } p \equiv 1 \pmod 4; \\ \left(4 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}) & \text{for } p \equiv 3 \pmod 4 \text{ and } p > 3; \end{cases} \tag{5.5}$$

see [26, Theorem 1.1]. Therefore, the contribution of the self-product cases is given by
(5.6)

$$\sum_{\pi_1 \in W_p^{ss}(1)} H_{sp}(\pi_1 \times \pi_1) = \begin{cases} 3, 5 & \text{for } p = 2, 3, \text{ respectively}; \\ h(\sqrt{-p}) & \text{for } p \equiv 1 \pmod 4; \\ \left(4 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}) & \text{for } p \equiv 3 \pmod 4 \text{ and } p > 3. \end{cases}$$

CASE $\pi = \pi_1 \times \pi_2$, $\pi_1 \neq \pi_2$. This occurs only when $p = 2$ or 3. The following are class numbers of B with $\mathcal{R}_{sp} \subset B \subset O_K$ obtained in Section 7.3.

$\pi = \pi_1 \times \pi_2$	K	$[O_K : \mathcal{R}_{sp}]$	$\mathcal{R}_{sp} \subset B \subset O_K$	$h(B)$
$\sqrt{2}\,\zeta_4 \times \pm\sqrt{2}\,\zeta_8$	$\mathbb{Q}(\sqrt{-2}) \times \mathbb{Q}(\sqrt{-1})$	2	$\mathcal{R}_{sp}$, O_K	1, 1
$\sqrt{2}\,\zeta_8 \times -\sqrt{2}\,\zeta_8$	$\mathbb{Q}(\sqrt{-1}) \times \mathbb{Q}(\sqrt{-1})$	8	$\mathcal{R}_{sp}, B_4, B_2, O_K$	1, 1, 1, 1
$\sqrt{3}\,\zeta_4 \times \pm\sqrt{3}\,\zeta_{12}$	$\mathbb{Q}(\sqrt{-3}) \times \mathbb{Q}(\sqrt{-3})$	6	$\mathcal{R}_{sp}, B_3, B_2, O_K$	1, 1, 1, 1
$\sqrt{3}\,\zeta_{12} \times -\sqrt{3}\,\zeta_{12}$	$\mathbb{Q}(\sqrt{-3}) \times \mathbb{Q}(\sqrt{-3})$	12	$\mathcal{R}_{sp}, B_4, B_3, O_K$	1, 1, 1, 1

The orders B_j are listed here for the convenience of the reader:

$$B_2 = \mathbb{Z}[(1+\zeta_4, 0), (\zeta_4, \zeta_4)] \qquad \text{for } \pi = \sqrt{2}\,\zeta_8 \times -\sqrt{2}\,\zeta_8;$$

$$B_2 = \mathbb{Z}[\sqrt{-3}] \times \mathbb{Z}[\zeta_6] \qquad \text{for } \pi = \sqrt{3}\,\zeta_4 \times \pm\sqrt{3}\,\zeta_{12};$$

$$B_3 = \mathbb{Z}[(\sqrt{-3}, 0), (\zeta_6, \zeta_6)] \qquad \text{for } \pi = \sqrt{3}\,\zeta_4 \times \pm\sqrt{3}\,\zeta_{12} \text{ or } \sqrt{3}\,\zeta_{12} \times -\sqrt{3}\,\zeta_{12};$$

$$B_4 = \mathbb{Z}[(2, 0), (\zeta_{2p}, \zeta_{2p})] \qquad \text{for } \pi = \sqrt{p}\,\zeta_{4p} \times -\sqrt{p}\,\zeta_{4p} \text{ and } p = 2, 3.$$

The contribution of other non-simple cases is

$$\sum_{\pi_1\neq\pi_2} H_{sp}(\pi_1\times\pi_2)=\begin{cases}2\times 2+4=8 & \text{for } p=2;\\ 2\times 4+4=12 & \text{for } p=3.\end{cases} \tag{5.7}$$

CASE $\pi \in W_p^{\mathrm{ss}}(2)$. We have $\pi \in \{\pm\sqrt{2}\,\zeta_{24}, \pm\sqrt{5}\,\zeta_5, \sqrt{p}\,\zeta_8\ (p\neq 2), \sqrt{p}\,\zeta_3, \sqrt{p}\,\zeta_{12}\ (p\neq 3)\}$. For $\pi=\pm\sqrt{p}\,\zeta_n$ with $(p,n)=(5,5)$ or $(2,24)$, we have $\mathcal{R}_{sp}=O_K$ by Remark 5.2 since n is critical at p. For $\pi=\sqrt{p}\,\zeta_8$ with $p\neq 2$, we have $K=\mathbb{Q}(\sqrt{p}\,\zeta_8)=\mathbb{Q}(\sqrt{-1},\sqrt{2p})$ and $\mathcal{R}_{sp}=\mathbb{Z}[(\sqrt{2p}+\sqrt{-2p})/2,\sqrt{-1}]$, which is the maximal order in K by Exercise 42(b) of [13, Chapter 2]. Therefore,

$$H_{sp}(\pm\sqrt{2}\,\zeta_{24})=H_{sp}(\pm\sqrt{5}\,\zeta_5)=1,\quad h(\sqrt{p}\,\zeta_8)=h(\sqrt{2p},\sqrt{-1}),\quad p\neq 2. \tag{5.8}$$

For $\pi=\sqrt{p}\,\zeta_3$, we have $K=\mathbb{Q}(\sqrt{p},\sqrt{-3})$ and $\mathcal{R}_{sp}=\mathbb{Z}[\sqrt{p},\zeta_3]$. The suborders $B\subseteq O_K$ containing $\mathbb{Z}[\sqrt{p}]$ with the property $[B^\times:\mathbb{Z}[\sqrt{p}]^\times]>1$ are classified in [23]. We list the suporders of $\mathcal{R}_{sp}$ in O_K and their class numbers in the following table.

$\pi=\sqrt{p}\,\zeta_3$	$[O_K:\mathcal{R}_{sp}]$	$\mathcal{R}_{sp}\subset B\subset O_K$	$h(B)$
$p=2$	1	O_K	1
$p=3$	3	$\mathcal{R}_{sp},\ O_K$	$1,1$
$p\equiv 3 \pmod 4,\ p\neq 3$	1	O_K	$h(K)$
$p\equiv 1 \pmod 4$	4	$\mathcal{R}_{sp},\ O_K$	$\varpi_p\, h(K), h(K)$

Thus,

$$H_{sp}(\sqrt{p}\,\zeta_3)=\begin{cases}1,2 & \text{for } p=2,3, \text{ respectively};\\ (\varpi_p+1)h(\sqrt{p},\sqrt{-3}) & \text{for } p\equiv 1 \pmod 4;\\ h(\sqrt{p},\sqrt{-3}) & \text{for } p\equiv 3 \pmod 4 \text{ and } p>3.\end{cases} \tag{5.9}$$

For $\pi=\sqrt{p}\,\zeta_{12}$ $(p\neq 3)$, we have $K=\mathbb{Q}(\sqrt{-p},\sqrt{-3})$ and $\mathcal{R}_{sp}=\mathbb{Z}[\sqrt{p}\,\zeta_{12},\zeta_6]=\mathbb{Z}[\sqrt{-p},\zeta_6]$. We have the following results from Section 7.4.

$\pi=\sqrt{p}\,\zeta_{12}\ (p\neq 3)$	$[O_K:\mathcal{R}_{sp}]$	$\mathcal{R}_{sp}\subset B\subset O_K$	$h(B)$
$p=2$	1	O_K	1
$p\equiv 1 \pmod 4$	1	O_K	$h(K)$
$p\equiv 3 \pmod 4$	4	$\mathcal{R}_{sp}, O_K$	$\varpi_{3p}\, h(K), h(K)$

Thus,

$$H_{sp}(\sqrt{p}\,\zeta_{12})=\begin{cases}1 & \text{for } p=2;\\ h(\sqrt{-p},\sqrt{-3}) & \text{for } p\equiv 1 \pmod 4;\\ (\varpi_{3p}+1)h(\sqrt{-p},\sqrt{-3}) & \text{for } p\equiv 3 \pmod 4\ (p\neq 3).\end{cases} \tag{5.10}$$

The following are the class numbers of the fields $K=\mathbb{Q}(\sqrt{p}\,\zeta_n)$ for $n\in\{3,8,12\}$ and $p\in\{2,3,5\}$. They are checked using the Magma algebra system [2].

$h(K)$	$p=2$	$p=3$	$p=5$
$\mathbb{Q}(\sqrt{p}\,\zeta_3)=\mathbb{Q}(\sqrt{p},\sqrt{-3}\,)$	1	1	1
$\mathbb{Q}(\sqrt{p}\,\zeta_8)=\mathbb{Q}(\sqrt{2p},\sqrt{-3}\,)$	1	2	2
$\mathbb{Q}(\sqrt{p}\,\zeta_{12})=\mathbb{Q}(\sqrt{-p},\sqrt{-3}\,)$	1	1	2

We collect the contribution of simple cases. For $p=2$, we have

$$H_{sp}(\sqrt{2}\,\zeta_3)+H_{sp}(\sqrt{2}\,\zeta_{12})+2H_{sp}(\sqrt{2}\,\zeta_{24})=1+1+2=4. \tag{5.11}$$

For $p=3$, we have

$$H_{sp}(\sqrt{3}\,\zeta_3)+H_{sp}(\sqrt{3}\,\zeta_8)=1+2=3. \tag{5.12}$$

For $p=5$, we have

$$H_{sp}(\sqrt{5}\,\zeta_3)+H_{sp}(\sqrt{3}\,\zeta_8)+H_{sp}(\sqrt{5}\,\zeta_{12})+2H_{sp}(\sqrt{5}\,\zeta_5)=1+2+2+2=7. \tag{5.13}$$

For $p\geq 7$, we have

$$\begin{aligned}\sum_{\pi\neq\sqrt{p}\,\in W_p^{\mathrm{ss}}(2)} H_{sp}(\pi) &= H_{sp}(\sqrt{p}\,\zeta_3)+H_{sp}(\sqrt{p}\,\zeta_8)+H_{sp}(\sqrt{p}\,\zeta_{12})\\ &=\begin{cases}(\varpi_p+1)h(K_{p,3})+h(K_{2p,1})+h(K_{3p,3}), & \text{for } p\equiv 1 \pmod 4;\\ h(K_{p,3})+h(K_{2p,1})+(\varpi_{3p}+1)h(K_{3p,3}), & \text{for } p\equiv 3 \pmod 4.\end{cases}\end{aligned} \tag{5.14}$$

Let $\Delta(p)$ be the number of isomorphism classes of superspecial abelian surfaces whose Frobenius endomorphism not equal to $\pm\sqrt{p}$. Then we have

$$\Delta(p)=\sum_{\pi\in W_p^{\mathrm{ss}}(2),\pi\neq\sqrt{p}} H_{sp}(\pi)+\sum_{\pi_1\times\pi_2,\pi_1\neq\pi_2} H_{sp}(\pi_1\times\pi_2)+\sum_{\pi_1\in W_p^{\mathrm{ss}}(1)} H_{sp}(\pi_1\times\pi_1). \tag{5.15}$$

Collecting the results (5.6), (5.7), (5.11) (5.12), (5.13) and (5.14), we obtain the following result.

Theorem 5.3.

(1) The number $\Delta(p)$ is $15, 20, 9$ for $p=2,3,5$, respectively.

(2) For $p>5$ and $p\equiv 1 \pmod 4$, we have

$$\Delta(p)=(\varpi_p+1)h(K_{p,3})+h(K_{2p,1})+h(K_{3p,3})+h(\sqrt{-p}\,), \tag{5.16}$$

where ϖ_p is defined in (1.2).

(3) For $p>5$ and $p\equiv 3 \pmod 4$, we have

$$\Delta(p)=h(K_{p,3})+h(K_{2p,1})+(\varpi_{3p}+1)h(K_{3p,3})+\left(4-\left(\frac{2}{p}\right)\right)h(\sqrt{-p}\,), \tag{5.17}$$

where ϖ_{3p} is defined in (1.2).

Theorem 1.2 then follows from Theorems 1.1 and 5.3.

Remark 5.4. Based on our computation we observe that the endomorphism ring of a superspecial abelian surface over $\mathbb{F}_p$ may be a non-maximal order, or even non-maximal at p. For example, when $p=3$ and $\pi=\sqrt{3}\,\zeta_3$, the order $\mathcal{R}_{sp}$, which occurs as the endomorphism ring of a superspecial abelian surface [21, Theorem 6.1], has index 3 in the maximal order.

5.3. ASYMPTOTIC BEHAVIOR OF $|\operatorname{Sp}_2(\mathbb{F}_p)|$. We now determine the asymptotic behavior of the size of $\operatorname{Sp}_2(\mathbb{F}_p)$ as the prime p goes to infinity. For simplicity, let $F = \mathbb{Q}(\sqrt{p})$. By Theorem 1.2, $|\operatorname{Sp}_2(\mathbb{F}_p)|$ is expressed as a linear combination of $\zeta_F(-1)h(F)$, $h(\sqrt{-p})$, and class numbers of certain biquadratic CM fields. The term $c\zeta_F(-1)h(\sqrt{p})$ (for a suitable constant c) comes from the contribution of the isogeny class corresponding to the Weil p-number $\pi = \sqrt{p}$. More precisely, it arises from the mass part in the Eichler class number formula for the calculation of $H(\sqrt{p})$. We recall from Theorem 1.1 that the mass part for $p > 5$ is

$$\text{Mass}(p) = \begin{cases} \frac{1}{2}\zeta_F(-1)h(F) & \text{for } p \equiv 3 \pmod 4; \\ 8\zeta_F(-1)h(F) & \text{for } p \equiv 1 \pmod 8; \\ \frac{1}{2}(15\varpi_p + 1)\zeta_F(-1)h(F) & \text{for } p \equiv 5 \pmod 8. \end{cases} \tag{5.18}$$

In [22, Theorem 6.3.1] we showed that the mass part $\text{Mass}(p)$ is the main term of $H(\sqrt{p})$. It is expected that $\text{Mass}(p)$ is also the main term of $|\operatorname{Sp}_2(\mathbb{F}_p)|$. This is true and we have the following asymptotic formula for the size of $\operatorname{Sp}_2(\mathbb{F}_p)$.

PROPOSITION 5.5. *We have*

$$\lim_{p\to\infty} \frac{|\operatorname{Sp}_2(\mathbb{F}_p)|}{\text{Mass}(p)} = 1.$$

Proof. It is enough to show that $\lim_{p\to\infty} h(\sqrt{-p})/h(F)\zeta_F(-1) = 0$, and for all the biquadratic CM-fields $K_{d,j}$ appearing in the formula of $|\operatorname{Sp}_2(\mathbb{F}_p)|$,

$$\lim_{p\to\infty} h(K_{d,j})/h(F)\zeta_F(-1) = 0.$$

The above limit has been verified for the pairs (d, j) with $d = p$ and $j = 1, 2, 3$ in [22, Theorem 6.3.1], and it remains to consider the pairs $(2p, 1)$ and $(3p, 3)$. Recall that the discriminant of F is denoted by $\mathfrak{d}_F$, which is either p or $4p$. Using the functional equation and the trivial inequality $\zeta_F(2) > 1$, we have $\zeta_F(-1) > c_1(\mathfrak{d}_F)^{3/2}$ for a constant $c_1 > 0$. For any CM-field K, let $h^-(K)$ be the relative class number of K defined as $h(K)/h(K^+)$, where K^+ is the maximal totally real subfield of K. By [8, Lemma 4], when K ranges over a sequence of CM-fields with bounded degree and $\mathfrak{d}_K \to \infty$, we have

$$\lim_{\mathfrak{d}_K\to\infty} (\log h^-(K))/(\log \sqrt{\mathfrak{d}_K/\mathfrak{d}_{K^+}}) = 1. \tag{5.19}$$

In particular, applying this to the quadratic imaginary fields $\mathbb{Q}(\sqrt{-p})$, we obtain that $h(\sqrt{-p})/\zeta_F(-1) \to 0$ as $p \to \infty$.
Assume $(d, j) = (2p, 1)$ or $(3p, 3)$. One calculates that $\mathfrak{d}_{K_{d,j}}/\mathfrak{d}_{K^+_{d,j}} \le 32p$. Let ϵ_d be the fundamental unit of the quadratic real field $\mathbb{Q}(\sqrt{d})$. By Siegel's theorem [9, Theorem 15.4, Chapter 12], the growth of $h(K^+_{d,j}) = h(\sqrt{d})$ satisfies the following formula

$$\lim_{d\to\infty} \frac{\log(h(\sqrt{d}) \log \epsilon_d)}{\log \sqrt{d}} = 1.$$

Note that ϵ_d is bounded below by $(1+\sqrt{5})/2$ for all d. Recall that $h(K_{d,j}) = h^-(K_{d,j})h(\sqrt{d})$. Combining these bounds yields that $h(K_{d,j})/\zeta_F(-1) \to 0$ as p goes to infinity. □

6. Galois cohomology and Superspecial abelian varieties

6.1. Galois cohomology and conjugacy classes. We refer to [15, Section I.5] for the definition of nonabelian Galois cohomology. Let $\Gamma_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ be the absolute Galois group of $\mathbb{F}_q$, and G a group with discrete topology on which $\Gamma_{\mathbb{F}_q}$ acts continuously. Let σ_q be the arithmetic Frobenius automorphism of $\overline{\mathbb{F}}_q$, which raises each element of $\overline{\mathbb{F}}_q$ to its q-th power. The group $\Gamma_{\mathbb{F}_q}$ is isomorphic to the profinite group $\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ with canonical generator σ_q. Each 1-cocycle $(a_\sigma)_{\sigma\in\Gamma_{\mathbb{F}_q}}$ is uniquely determined by its value $x = a_{\sigma_q} \in G$ at σ_q. An element of G is called a *1-cocycle element* if it arises from a 1-cocycle in this way. We will identify the set of 1-cocycles $Z^1(\Gamma_{\mathbb{F}_q}, G)$ with the subset of 1-cocycle elements of G. Two 1-cocycle elements $x, y \in Z^1(\Gamma_{\mathbb{F}_q}, G)$ define the same cohomology class if and only if they are σ_q-conjugate (denoted by $x \sim_{\sigma_q} y$), i.e., there exists $z \in G$ such that $x = z^{-1}y\sigma_q(z)$. Write $[x]_{\sigma_q}$ for the σ_q-conjugacy class of $x \in G$, and $B(G)$ for the set of all σ_q-conjugacy classes of G. Then

$$H^1(\Gamma_{\mathbb{F}_q}, G) = \{[x]_{\sigma_q} \in B(G) \mid x \in Z^1(\Gamma_{\mathbb{F}_q}, G)\} \subseteq B(G).$$

If the action of $\Gamma_{\mathbb{F}_q}$ on G is trivial, then $B(G)$ is reduced to the set $\mathrm{Cl}(G)$ of (the usual) conjugacy classes of G. Define $\mathrm{Cl}_0(G) := \{[x] \in \mathrm{Cl}(G) \mid x \text{ is of finite order}\} \subseteq \mathrm{Cl}(G)$.

Lemma 6.1. *Assume that the action of $\Gamma_{\mathbb{F}_q}$ on G factors through a finite quotient $\mathrm{Gal}(\mathbb{F}_{q^N}/\mathbb{F}_q)$. We have*

$$Z^1(\Gamma_{\mathbb{F}_q}, G) = \{x \in G \mid x\sigma_q(x)\cdots\sigma_q^{N-1}(x) \text{ is of finite order}\}.$$

In particular, if the action of $\Gamma_{\mathbb{F}_q}$ on G is trivial, then $H^1(\Gamma_{\mathbb{F}_q}, G) = \mathrm{Cl}_0(G)$.

Proof. This follows directly from Exercise 2 of [15, Section I.5.1]. □

6.2. Abelian varieties over finite fields and twisted forms. Let X_0 be an abelian variety over $\mathbb{F}_q$ with Frobenius endomorphism $\pi_{X_0} \in \mathrm{End}_{\mathbb{F}_q}(X_0)$. Set $\overline{X}_0 = X_0 \otimes \overline{\mathbb{F}}_q$, and $G = \mathrm{Aut}(\overline{X}_0)$. The Galois group $\Gamma_{\mathbb{F}_q}$ acts on $\mathrm{End}(\overline{X}_0)$ as follows (see [24, Lemma 3.3])

$$\sigma_q(x) = \pi_{X_0} x \pi_{X_0}^{-1}, \quad \forall\, x \in \mathrm{End}(\overline{X}_0), \tag{6.1}$$

where the conjugation by π_{X_0} is taken inside $\mathrm{End}^0(\overline{X}_0)$. As $\mathrm{End}(\overline{X}_0)$ is a free $\mathbb{Z}$-module of finite rank, the action of $\Gamma_{\mathbb{F}_q}$ factors through a finite quotient $\mathrm{Gal}(\mathbb{F}_{q^N}/\mathbb{F}_q)$, and hence $(\pi_{X_0})^N$ is central in $\mathrm{End}(\overline{X}_0)$.

Recall that an $(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-*form* of X_0 is an abelian varieties X over $\mathbb{F}_q$ such that $\overline{X} := X \otimes \overline{\mathbb{F}}_q$ is $\overline{\mathbb{F}}_q$-isomorphic to $\overline{X}_0$. Let $E(\overline{\mathbb{F}}_q/\mathbb{F}_q, X_0)$ be the set of $\mathbb{F}_q$-isomorphism classes of $(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-forms of X_0. By [15, Section III.1.3], there is a canonical bijection of pointed sets

$$\theta : E(\overline{\mathbb{F}}_q/\mathbb{F}_q, X_0) \xrightarrow{\sim} H^1(\Gamma_{\mathbb{F}_q}, G), \tag{6.2}$$

sending the $\mathbb{F}_q$-isomorphism class of X_0 to the trivial class. The map θ is induced from mapping each $\overline{\mathbb{F}}_q$-isomorphism $f : \overline{X}_0 \to \overline{X}$ to the 1-cocycle element $x = f^{-1}\sigma_q(f) \in G$. The injectivity of θ follows purely from cohomological formalism, and the surjectivity is a consequence of Weil's Galois descent.

An isomorphism f of abelian varieties as above induces an isomorphism

$$\alpha_f : \mathrm{End}(\overline{X}) \simeq \mathrm{End}(\overline{X}_0), \quad y \mapsto f^{-1}yf. \tag{6.3}$$

The Frobenius endomorphisms π_{X_0} and π_X are related by the following commutative diagram (see [24, (3.2)]):

$$\begin{tikzcd} \overline{X}_0 \arrow[r, "f"] \arrow[d, "\pi_{X_0}"'] & \overline{X} \arrow[d, "\pi_X"] \\ \overline{X}_0 \arrow[r, "\sigma_q(f)"] & \overline{X}. \end{tikzcd} \tag{6.4}$$

We compute

$$\alpha_f(\pi_X) = f^{-1}\pi_X f = f^{-1}\sigma_q(f)\pi_{X_0} = x\pi_{X_0}. \tag{6.5}$$

Note that for $x, y, z \in G$,

$$x = z^{-1}y\sigma_q(z) \iff x\pi_{X_0} = z^{-1}(y\pi_{X_0})z.$$

Hence there is a well-defined injective map

$$\Pi : B(G) \hookrightarrow \mathrm{End}(\overline{X}_0)/G, \quad [x]_{\sigma_q} \mapsto [x\pi_{X_0}], \tag{6.6}$$

where $\mathrm{End}(\overline{X}_0)/G$ denotes the set of orbits of $\mathrm{End}(\overline{X}_0)$ under the right action of G by conjugation. In a sense, the image of $H^1(\Gamma_{\mathbb{F}_q}, G)$ under Π consists of the conjugacy classes of Frobenius endomorphisms of members of $E(\overline{\mathbb{F}}_q/\mathbb{F}_q, X_0)$.

We can also work in the category of abelian varieties up to isogeny and study the $(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-forms of the isogeny class $[X_0]$. Thus we pass from isomorphisms of abelian varieties to quasi-isogenies, and endomorphism rings to endomorphism algebras, etc. Let $E^0(\overline{\mathbb{F}}_q/\mathbb{F}_q, [X_0])$ be the set of $\mathbb{F}_q$-isogeny classes of abelian varieties $[X]$ such that $\overline{X}$ is isogenous to $\overline{X}_0$ over $\overline{\mathbb{F}}_q$, and $G_{\mathbb{Q}} = \mathrm{End}^0(\overline{X}_0)^\times$. Many previous constructions can be carried over. In particular, both (6.4) and (6.5) hold true for any quasi-isogeny $f : \overline{X}_0 \to \overline{X}$, and one obtains a 1-cocycle element $x = f^{-1}\sigma_q(f) \in G_{\mathbb{Q}}$ as before. This gives a canonical injective map

$$\theta : E^0(\overline{\mathbb{F}}_q/\mathbb{F}_q, [X_0]) \hookrightarrow H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}}), \tag{6.7}$$

which fits into a commutative diagram

$$\begin{tikzcd} E(\overline{\mathbb{F}}_q/\mathbb{F}_q, X_0) \arrow[r, "\cong", "\theta"'] \arrow[d] & H^1(\Gamma_{\mathbb{F}_q}, G) \arrow[d] \\ E^0(\overline{\mathbb{F}}_q/\mathbb{F}_q, [X_0]) \arrow[r, "\theta"] & H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}}). \end{tikzcd} \tag{6.8}$$

The left vertical map sends the $\mathbb{F}_q$-isomorphism class of X to its $\mathbb{F}_q$-isogeny class $[X]$, and the right vertical map is induced from the inclusion of $\Gamma_{\mathbb{F}_q}$-groups $G \subset G_{\mathbb{Q}}$. Thus (6.8) endows a geometric meaning for this cohomological map. We complete the picture by showing that the map θ in (6.7) is surjective and thus a bijection of pointed sets as stated in Proposition 1.4. Recall that the action of $\Gamma_{\mathbb{F}_q}$ on $\mathrm{End}^0(\overline{X})$ factors through $\mathrm{Gal}(\mathbb{F}_{q^N}/\mathbb{F}_q)$ for a fixed $N \in \mathbb{N}$. Without lose of generality, assume that X_0 is $\mathbb{F}_{q^N}$-isotypical, i.e., $X_0 \otimes \mathbb{F}_{q^N}$ is isogenous to $(Y_N)^d$, where Y_N is an absolutely simple abelian variety over $\mathbb{F}_{q^N}$ with $\mathrm{End}(Y_N) = \mathrm{End}(\overline{Y}_N)$. Equivalently, we assume that the multiple Weil q-number $\pi_{0,1}^{t_1} \times \cdots \times \pi_{0,u}^{t_u} \in MW_q$ corresponding to the $\mathbb{F}_q$-isogeny class $[X_0]$ satisfies that $\pi_{0,1}^N = \pi_{0,2}^N = \cdots = \pi_{0,u}^N$ after suitable conjugation, and $\mathbb{Q}((\pi_{X_0})^N) \subset \mathrm{End}^0(X_0)$ is a field which coincides with $\mathbb{Q}((\pi_{X_0})^{sN})$ for all $s \in \mathbb{N}$. Then $\mathrm{End}^0(\overline{X}_0) = \mathrm{Mat}_d(\mathrm{End}^0(\overline{Y}_N))$, and $\mathrm{End}^0(\overline{Y}_N)$ is a central division algebra over $\mathbb{Q}((\pi_{X_0})^N)$. For simplicity, let $D = \mathrm{End}^0(\overline{Y}_N)$ and $K_0 = \mathbb{Q}((\pi_{X_0})^N)$. Then $G_{\mathbb{Q}} = \mathrm{End}^0(\overline{X}_0)^\times = \mathrm{GL}_d(D)$.

LEMMA 6.2. *There is a bijection between $H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}})$ and the following subset of $\mathrm{Cl}(G_{\mathbb{Q}})$:*

$$\mathscr{C}(\pi_{X_0}) = \{[\underline{\pi}] \in \mathrm{Cl}(G_{\mathbb{Q}}) \mid \exists M \in \mathbb{N} : \ \underline{\pi}^{NM} = \pi_{X_0}^{NM}\}. \tag{6.9}$$

Proof. Since $\pi_{X_0} \in G_{\mathbb{Q}}$, the map Π in (6.6) defines a bijection

$$\Pi : B(G_{\mathbb{Q}}) \xrightarrow{\sim} \mathrm{Cl}(G_{\mathbb{Q}}), \quad [x]_{\sigma_q} \mapsto [x\pi_{X_0}].$$

Let $\pi_x = x\pi_{X_0}$ for each $x \in G_{\mathbb{Q}}$. Then

$$x\sigma_q(x)\cdots\sigma_q^{N-1}(x) = (x\pi_{X_0})^N(\pi_{X_0})^{-N} = (\pi_x)^N(\pi_{X_0})^{-N}.$$

By Lemma 6.1, $x \in Z^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}})$ if and only if $(\pi_x)^N = (\pi_{X_0})^N\xi$ for some $\xi \in G_{\mathbb{Q}}$ of finite order, or equivalently, $\pi_x^{NM} = (\pi_{X_0})^{NM}$ for some $M \in \mathbb{N}$. $\square$

Any $\underline{\pi} \in G_{\mathbb{Q}}$ with $[\underline{\pi}] \in \mathscr{C}(\pi_{X_0})$ is semisimple, as $\underline{\pi}^{NM} = (\pi_{X_0})^{NM}$ lies in the center of the simple $\mathbb{Q}$-algebra $\mathrm{End}^0(\overline{X}_0)$. The minimal polynomial of $\underline{\pi}$ factorizes as a product of distinct irreducible polynomials over $\mathbb{Q}$:

$$P(t) = \prod_{i=1}^{r} P_i(t) \in \mathbb{Q}[t]. \tag{6.10}$$

For all $\underline{\pi}'$ in the conjugacy class $[\underline{\pi}]$, the $\mathbb{Q}$-subalgebra $K_{\underline{\pi}'} := \mathbb{Q}(\underline{\pi}') \subset \mathrm{End}^0(\overline{X}_0)$ is canonically isomorphic to $K := \mathbb{Q}[t]/(P(t))$ via the map $\underline{\pi}' \mapsto t$. Since $\pi_{X_0}^{NM} = \underline{\pi}^{NM}$, the field $K_0 = \mathbb{Q}(\pi_{X_0}^{NM})$ can be identified with the $\mathbb{Q}$-subalgebra of K generated by t^{NM}, thus providing a K_0-algebra structure on K. By (6.10), K factorizes as a products of number fields

$$K = K_1 \times \cdots \times K_r, \quad \text{with} \quad K_i = \mathbb{Q}[t]/(P_i(t)) \supseteq K_0. \tag{6.11}$$

By an abuse of notation, we regard $\pi_{X_0}^N$ as a Weil q^N-number via a embedding $K_0 \hookrightarrow \overline{\mathbb{Q}}$. Then for each $1 \le i \le r$, the roots of $P_i(t)$ in $\overline{\mathbb{Q}}$ is a conjugacy class of Weil q-numbers such that one of its representative π_i satisfies $\pi_i^{NM} = \pi_{X_0}^{NM}$.

Therefore, given $\underline{\pi} \in \mathscr{C}(\pi_{X_0})$, we find r Weil q-numbers representing distinct conjugacy classes

(6.12)
$$\{\pi_1, \cdots, \pi_r\} \quad \text{with} \quad \pi_i^{NM} = \pi_{X_0}^{NM} \quad \text{for some } M \in \mathbb{N} \text{ and all } 1 \le i \le r.$$

Next, we fix $P(t) \in \mathbb{Q}[t]$ as above, and produce a discrete invariant for every conjugacy class $[\underline{\pi}] \in \mathscr{C}(\pi_{X_0})$ with minimal polynomial $P(t)$. Let $V = D^d$ be the right vector space over D of column vectors. Then $\mathrm{End}_D(V) = \mathrm{Mat}_d(D)$ acts on V from the left by the usual matrix multiplication. We have a canonical K_0-algebra embedding $K \hookrightarrow \mathrm{End}_D(V)$ sending K to K_π. Thus $\underline{\pi}$ endows a faithful (K, D)-bimodule structure on V, denoted by $V_{\underline{\pi}}$. By (6.11), there is a decomposition of V into right D-subspaces:

$$V = \bigoplus_{i=1}^{r} V_i, \quad d_i = \dim_D V_i. \tag{6.13}$$

The action of K_i on V_i gives rise to a K_0-embedding $K_i \hookrightarrow \mathrm{End}_D(V_i) = \mathrm{Mat}_{d_i}(D)$. We study each of the embeddings individually first.

Lemma 6.3. *Let $\pi \in W_q$ be a Weil q-number such that $\pi^{NM} = \pi_{X_0}^{NM}$ for some integer $M \in \mathbb{N}$, and X_π a simple abelian variety over $\mathbb{F}_q$ in the isogeny class corresponding to π. Let $e = e(\pi)$ be the smallest integer such that there is an K_0-embedding $\mathbb{Q}(\pi) \hookrightarrow \mathrm{Mat}_e(D)$. Then $\overline{X}_\pi = X_\pi \otimes \overline{\mathbb{F}}_q$ is isogenous to $(\overline{Y}_N)^e$, and $\mathrm{End}^0(X_\pi)$ is isomorphic to the centralizer C_π of $\mathbb{Q}(\pi)$ in $\mathrm{Mat}_e(D)$.*

Proof. Since $\pi^{NM} = \pi_{X_0}^{NM}$, there exists an isogeny $\overline{X}_\pi \to (\overline{Y}_N)^e$ for some $e \in \mathbb{N}$, which gives an identification of $\mathrm{End}^0(\overline{X}_\pi)$ with $\mathrm{Mat}_e(D) = \mathrm{End}^0((\overline{Y}_N)^e)$ in the same way as (6.3). Thus we obtain a K_0-embedding $\mathbb{Q}(\pi) \hookrightarrow \mathrm{Mat}_e(D)$, and $\mathrm{End}^0(X_\pi)$ is recovered as the $\Gamma_{\mathbb{F}_q}$-invariants of $\mathrm{End}^0(\overline{X}_\pi)$, or equivalently, the centralizer C_π of $\mathbb{Q}(\pi)$ in $\mathrm{Mat}_e(D)$ by (6.1). On the other hand, C_π is also the endomorphism algebra of the $(\mathbb{Q}(\pi), D)$-bimodule D^e. Now the minimality of e follows from the fact that $C_\pi = \mathrm{End}^0(X_\pi)$ is a division algebra. □

Given $e' \in \mathbb{N}$, a K_0-embedding of $\mathbb{Q}(\pi)$ into the simple algebra $\mathrm{Mat}_{e'}(D)$ exists if and only if $e(\pi)$ divides e'. Therefore, every d_i in (6.13) is of the form $m_i e(\pi_i)$ for some positive integer $m_i \in \mathbb{N}$ subjecting to the condition

$$m_1 e(\pi_1) + \cdots + m_r e(\pi_r) = d. \tag{6.14}$$

We shall call the r-tuple $\underline{m} = (m_1, \ldots, m_r)$ the *type* of the (K, D)-bimodule $V_{\underline{\pi}}$ or simply the *type* of $\underline{\pi}$.

Lemma 6.4. *There are natural bijections between the following sets:*

1. *the set of conjugacy classes $[\underline{\pi}] \in \mathscr{C}(\pi_{X_0})$ with minimal polynomial $P(t)$;*
2. *the set of $G_{\mathbb{Q}}$-conjugacy classes of K_0-embedding $K \hookrightarrow \mathrm{End}_D(V)$;*
3. *the set of isomorphism classes of faithful (K, D)-bimodule structures on V;*
4. *the set of r-tuples $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}^r$ satisfying (6.14).*

Proof. The bijection between between (1) and (2) is established by the map sending each K_0-embedding $\phi : K = \mathbb{Q}[t]/(P(t)) \hookrightarrow \mathrm{End}_D(V)$ to $\pi = \phi(t)$. Every faithful (K, D)-bimodule structure on V is given by a K_0-embedding $\phi : K \hookrightarrow \mathrm{End}_D(V)$. Two such embeddings define isomorphic structures if and only if they are conjugate by an element of $G_{\mathbb{Q}}$. Hence (2) is bijective to (3). The proof that (2) is bijective to (4) is similar to that of [16, Proposition 3.2] and is omitted. □

PROPOSITION 6.5. *Each cohomology class $[x]_{\sigma_q} \in H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}})$ determines a unique conjugacy class of multiple Weil q-number $\pi_1^{m_1} \times \cdots \times \pi_r^{m_r} \in MW_q$ such that*

- $\pi_i^{NM} = \pi_{X_0}^{NM}$ *for some $M \in \mathbb{N}$ and all $1 \le i \le r$;*
- $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}^r$ *satisfies (6.14).*

In particular, the map θ in (6.7) is a bijection of pointed sets.

Proof. Given $[x]_{\sigma_q} \in H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}})$, we produce the desired multiple Weil q-number by combing the type $\underline{m} = (m_1, \cdots, m_r)$ of $[\pi_x] \in \mathscr{C}(\pi_{X_0})$ and the set $\{\pi_1, \cdots, \pi_r\}$ determined by $[\pi_x]$ as in (6.12). Let $X = \prod_{i=1}^r (X_{\pi_i})^{m_i}$ be an abelian variety over $\mathbb{F}_q$ corresponding to $\pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$. Then $\overline{X}$ is isogenous to $\overline{X}_0$ by Lemma 6.3 and (6.14). Identify $\mathrm{End}^0(\overline{X})$ with $\mathrm{End}^0(\overline{X}_0)$ via an isogeny $f : \overline{X}_0 \to \overline{X}$ as in (6.3). The conjugacy class of $\alpha_f(\pi_X) \in G_{\mathbb{Q}}$ is independent of the choice of f. By the construction, $\alpha_f(\pi_X)$ is a semisimple element with the same minimal polynomial and type as $\pi_x = x\pi_{X_0}$. It follows from Lemma 6.4 that they must lie in the same conjugacy class of $G_{\mathbb{Q}}$. We conclude that θ is surjective by Lemma 6.2. □

6.3. SUPERSPECIAL ABELIAN VARIETIES AND THE PARITY PROPERTY. We apply the previous construction to the study of superspecial abelian varieties over finite fields. Let E_0 be a supersingular elliptic curve over the prime finite field $\mathbb{F}_p$ whose Frobenius endomorphism π_0 satisfying $\pi_0^2 + p = 0$ (Recall that $\sqrt{-p} \in W_p^{\mathrm{ss}}(1)$ for all p by Proposition 3.5). Let $\mathcal{O} := \mathrm{End}(E_0 \otimes \overline{\mathbb{F}}_p)$ be the endomorphism ring of $E_0 \otimes \overline{\mathbb{F}}_p$; this is a maximal order in the unique quaternion $\mathbb{Q}$-algebra $D = B_{p,\infty}$ ramified exactly at $\{p, \infty\}$. Take $X_0 = E_0^d$ and $\overline{X}_0 := X_0 \otimes \overline{\mathbb{F}}_p$ for $d \ge 1$. Then $\mathrm{End}(\overline{X}_0) = \mathrm{Mat}_d(\mathcal{O})$. In what follows we denote by

$$G := \mathrm{Aut}(\overline{X}_0) = \mathrm{GL}_d(\mathcal{O})$$

the automorphism group of $\overline{X}_0$. Consider $\mathcal{O}$ as a subring of $\mathrm{Mat}_d(\mathcal{O})$ by the diagonal embedding and view π_0 as an element in $\mathrm{Mat}_d(\mathcal{O})$. Then the action of $\Gamma_{\mathbb{F}_p}$ on $G = \mathrm{GL}_d(\mathcal{O})$ is given by

$$\sigma_p(x) = \pi_0 x \pi_0^{-1}, \quad x \in G. \tag{6.15}$$

We will also write $G_{\mathbb{Q}}$ for the group $\mathrm{GL}_d(D)$.
Recall that $\mathrm{Sp}_d(\mathbb{F}_q)$ denotes the set of isomorphism classes of d-dimensional superspecial abelian varieties over $\mathbb{F}_q$. For the classification of superspecial

abelian varieties over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, we have the following result, due to Deligne, Shioda and Ogus (cf. [12, Section 1.6, p. 13]).

Theorem 6.6. *For any integer $d \geq 2$, there is only one isomorphism class of d-dimensional superspecial abelian varieties over any algebraically closed field of characteristic $p > 0$.*

According to this theorem, any d-dimensional superspecial abelian variety over $\mathbb{F}_q$ is an $(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-form of $X_0 \otimes \mathbb{F}_q$. Thus we obtain a natural bijection by (6.2)

$$H^1(\Gamma_{\mathbb{F}_q}, G) \simeq \mathrm{Sp}_d(\mathbb{F}_q), \quad d > 1, \tag{6.16}$$

which sends the trivial class to the isomorphism class of $X_0 \otimes \mathbb{F}_q$. The set $\mathrm{Sp}_d(\mathbb{F}_q)$ is partitioned into isogeny classes:

$$\mathrm{Sp}_d(\mathbb{F}_q) = \coprod_{\pi \in MW_q^{\mathrm{ss}}(d)} \mathrm{Sp}(\pi). \tag{6.17}$$

Theorem 6.7. *Let $q = p^a$ and $q' = p^{a'}$ be powers of the prime number p such that $a \equiv a' \pmod 2$. For any integer $d \geq 1$, there are natural bijections*

$$H^1(\Gamma_{\mathbb{F}_q}, G) \simeq H^1(\Gamma_{\mathbb{F}_{q'}}, G), \tag{6.18}$$

$$\mathrm{Sp}_d(\mathbb{F}_q) \simeq \mathrm{Sp}_d(\mathbb{F}_{q'}). \tag{6.19}$$

Proof. If $d = 1$, then (6.19) has been proven in Section 4.2; see Proposition 4.4 and Remark 4.5. If $d > 1$, then (6.19) follows from (6.16) and (6.18). Therefore, it remains to prove (6.18).
Since π_0^2 is a central element, the element σ_p^2 acts trivially on G by (6.15). Thus $\sigma_q(x) = \sigma_{q'}(x)$ for all $x \in G$. This together with the canonical isomorphism $\Gamma_{\mathbb{F}_q} \simeq \Gamma_{\mathbb{F}_{q'}}$ (sending $\sigma_q \mapsto \sigma_{q'}$) yields a natural bijection $H^1(\Gamma_{\mathbb{F}_q}, G) \simeq H^1(\Gamma_{\mathbb{F}_{q'}}, G)$. The theorem is proved. □

Remark 6.8. By the same token, we have a natural bijection

$$H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}}) \simeq H^1(\Gamma_{\mathbb{F}_{q'}}, G_{\mathbb{Q}}). \tag{6.20}$$

Thus by Proposition 6.5, there is also a *natural* bijection between the isogeny classes of supersingular abelian varieties over $\mathbb{F}_q$ and those over $\mathbb{F}_{q'}$. This can be made explicit in terms of multiple Weil numbers. The Frobenius endomorphism of $X_0 \otimes \mathbb{F}_q$ is π_0^a. Hence the Frobenius endomorphisms of the isogeny class corresponding to a cohomology class $[x]_{\sigma_q} \in H^1(\Gamma_{\mathbb{F}_q}, G_{\mathbb{Q}})$ is given by the conjugacy class $[x\pi_0^a]$ by (6.5). Without lose of generality, assume that $a - a' = 2s \geq 0$. If $\pi = \pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$ is a multiple Weil q-number determined by $[x]_{\sigma_q}$, then the corresponding multiple Weil q'-number is $\widetilde{\pi} = \widetilde{\pi}_1^{m_1} \times \cdots \times \widetilde{\pi}_r^{m_r}$, with $\widetilde{\pi}_i = (-p)^{-s}\pi_i$ for all $1 \leq i \leq r$.
By the commutative diagram (6.8), the bijection (6.19) preserves isogeny classes in the sense that there is a natural bijection

$$\mathrm{Sp}(\pi) \simeq \mathrm{Sp}(\widetilde{\pi}) \qquad \forall\, \pi \in MW_q^{\mathrm{ss}}(d). \tag{6.21}$$

Corollary 6.9. *Let $q = p^{2s+1}$ be an odd power of p. Let Y_0 be a fixed supersingular abelian variety over $\mathbb{F}_q$ and $\pi = \pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$ the corresponding multiple Weil q-number. Let V and K be as in Proposition 5.1, and set $\mathcal{R}_{sp} := \mathbb{Z}[\widetilde{\pi}_0, p\widetilde{\pi}_0^{-1}] \subset K$, where $\widetilde{\pi}_0 = (-p)^{-s}(\pi_1, \ldots, \pi_r)$. Assume that K has no real place. Then there is a natural bijection between the set $\mathrm{Sp}(\pi)$ of isomorphism classes of superspecial abelian varieties in the isogeny class $[Y_0]$ and the set of isomorphism classes of $\mathcal{R}_{sp}$-lattices in V.*

Proof. This follows from Proposition 5.1 and Theorem 6.7. $\square$

The above theorem provides an approach for computing the size of $\mathrm{Sp}_d(\mathbb{F}_q)$ explicitly in the odd exponent case, subject to the condition that K has no totally real factors. For the rest of this section we shall describe $H^1(\Gamma_{\mathbb{F}_q}, \mathrm{GL}_d(\mathcal{O}))$ (and hence $\mathrm{Sp}_d(\mathbb{F}_q)$) when q is an even power of p.

6.4. A description of $H^1(\Gamma_{\mathbb{F}_q}, \mathrm{GL}_d(\mathcal{O}))$ with even exponent. In what follows we assume that $q = p^a$ is an even power of p and $X_0 = E_0^d \otimes \mathbb{F}_q$ with $d \geq 2$. The Frobenius endomorphism $\pi_{X_0} = (-p)^{a/2}$ lies in the center of $\mathrm{End}(\overline{X}_0) = \mathrm{Mat}_d(\mathcal{O})$. Hence $\Gamma_{\mathbb{F}_q}$ acts trivially on the group $G := \mathrm{GL}_d(\mathcal{O})$ by (6.15). Then it follows from Lemma 6.1 that $H^1(\Gamma_{\mathbb{F}_q}, G)$ can be identified with the set $\mathrm{Cl}_0(G)$ of conjugacy classes of elements in G of finite order. We shall give a lattice description for $\mathrm{Cl}_0(G)$ and hence for $\mathrm{Sp}_d(\mathbb{F}_q)$ by the previous correspondence. See Proposition 6.11 for details.
Suppose $x \in G$ is an element of finite order, which is necessarily semi-simple. The minimal polynomial of x over $\mathbb{Q}$ has the form

$$P_{\underline{n}}(t) = \Phi_{n_1}(t)\Phi_{n_2}(t)\cdots\Phi_{n_r}(t), \quad 1 \leq n_1 < n_2 < \cdots < n_r \tag{6.22}$$

for some r-tuple $\underline{n} = (n_1, \ldots, n_r) \in \mathbb{N}^r$, where $\Phi_m(t) \in \mathbb{Z}[t]$ denotes the m-th cyclotomic polynomial. We define

$$K_{\underline{n}} := \frac{\mathbb{Q}[t]}{\prod_{i=1}^r \Phi_{n_i}(t)} \quad \text{and} \quad A_{\underline{n}} := \frac{\mathbb{Z}[t]}{\prod_{i=1}^r \Phi_{n_i}(t)}.$$

The $\mathbb{Q}$-subalgebras of $\mathrm{End}^0(\overline{X}_0) = \mathrm{Mat}_d(D)$ generated by x and $\pi_x = x\pi_{X_0}$ coincide and are isomorphic to $K_{\underline{n}}$. Moreover, the subring $\mathbb{Z}[x] \subset \mathrm{Mat}_d(\mathcal{O})$ is canonically isomorphic to $A_{\underline{n}}$.
We denote by $C(\underline{n}) \subset \mathrm{Cl}_0(G)$ the set of conjugacy classes of G with minimal polynomial $P_{\underline{n}}(t)$. By Proposition 6.5, each conjugacy class $[x] \in C(\underline{n})$ determines a (conjugacy class of) supersingular multiple Weil q-number $\pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$, where $\pi_i = (-p)^{a/2}\zeta_{n_i}$, and $\underline{m} = (m_1, \cdots, m_r)$ is the type of the faithful $(K_{\underline{n}}, D)$-bimodule structure on $V = D^d$ equipped by $\pi_x \in \mathrm{Mat}_d(D)$. Since $\mathbb{Q}(\pi_x) = \mathbb{Q}(x) \cong K_{\underline{n}}$, the $(K_{\underline{n}}, D)$-bimodule structure on V is also equipped *directly* by $x \in \mathrm{Mat}_d(D)$. Thus $\underline{m}$ is also called the type of $[x]$, as it depends only on the conjugacy class. Recall that a $(K_{\underline{n}}, D)$-bimodule V is said to be type $\underline{m}$ if the decomposition into D-subspaces $V = \oplus_{i=1}^r V_i$ induced from the decomposition $K_{\underline{n}} = \prod_{i=1}^r \mathbb{Q}(\zeta_{n_i})$ satisfies that $\dim_D V_i = m_i e(\pi_i)$ for all $1 \leq i \leq r$, where $e(\pi_i)$ is defined in Lemma 6.3. Since $\dim E_0 = 1$, we have $e(\pi_i) = d(\pi_i)$, the dimension of the Weil number π_i. Note that $d(\pi_i)$ depends only on the

integer n_i as $q = p^a$ is fixed, so we write $d(n_i)$ for it instead. Equation (6.14) becomes

$$m_1 d(n_1) + \cdots + m_r d(n_r) = d. \tag{6.23}$$

A pair of r-tuples $(\underline{n}, \underline{m}) \in \mathbb{N}^r \times \mathbb{N}^r$ with $1 \le n_1 < \cdots < n_r$ is said to be *d-admissible* if the condition (6.23) is satisfied. Let $C(\underline{n}, \underline{m}) \subset C(\underline{n})$ denote the subset of conjugacy classes of type $\underline{m}$. An element $x \in G$ or its conjugacy $[x] \in \mathrm{Cl}(G)$ is said to be type $(\underline{n}, \underline{m})$ if $[x] \in C(\underline{n}, \underline{m})$.

LEMMA 6.10. *Fix a faithful $(K_{\underline{n}}, D)$-bimodule $V = D^d$ of type $\underline{m}$. There is a natural bijection between the set $C(\underline{n}, \underline{m})$ and the set of isomorphism classes of $(A_{\underline{n}}, \mathcal{O})$-lattices in V.*

Proof. Let $M_0 := \mathcal{O}^d \subset V$ be the standard lattice in V. Every element $x \in G$ of type $(\underline{n}, \underline{m})$ gives rise to an $(A_{\underline{n}}, \mathcal{O})$-bimodule structure on M_0. Two elements x, x' determine isomorphism bimodule structures if and only if they are conjugate in G. Therefore, the set $C(\underline{n}, \underline{m})$ is in bijection with the set of isomorphism classes of $(A_{\underline{n}}, \mathcal{O})$-lattices in V that are $\mathcal{O}$-isomorphic to M_0. Since $d \ge 2$, every $\mathcal{O}$-lattice in V is isomorphic to M_0. This follows from a theorem of Eichler [6] that the class number of $\mathrm{Mat}_d(\mathcal{O})$ is 1 for $d \ge 2$ (see also [10, Theorem 2.1]). □

PROPOSITION 6.11. *Let $\mathrm{Cl}_0(G)$ be the set of conjugacy classes of $G = \mathrm{GL}_d(\mathcal{O})$ of finite order with $d \ge 2$. Then*

$$\mathrm{Cl}_0(G) = \coprod_{(\underline{n}, \underline{m})} C(\underline{n}, \underline{m}), \tag{6.24}$$

where $(\underline{n}, \underline{m})$ runs through all d-admissible types. For each fixed $(\underline{n}, \underline{m})$, there are natural bijections between the following sets:

(1) $C(\underline{n}, \underline{m})$, the set of conjugacy classes of type $(\underline{n}, \underline{m})$;
(2) $\mathrm{Sp}(\pi)$, where $\pi = \pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$ and $\pi_i = (-p)^{a/2} \zeta_{n_i}$;
(3) the set of isomorphism classes of $(A_{\underline{n}}, \mathcal{O})$-lattices in the $(K_{\underline{n}}, D)$-bimodule V of type $\underline{m}$.

Proof. The bijection between (1) and (2) is established by combining (6.16) and Proposition 6.5. The bijection between (1) and (3) follows from Lemma 6.10. □

7. ARITHMETIC RESULTS

In this section, we prove the arithmetic results used in Section 5 concerning the order $\mathcal{R}_{sp}$. In the light of (5.4), our goals are two fold: (1) show that $\mathcal{R}_{sp}$ is Bass for every supersingular multiple Weil p-number $\pi \in MW_p^{\mathrm{ss}}(2)$ of dimension 2 distinct from $\pm\sqrt{p}$; (2) classify all suporders of $\mathcal{R}_{sp}$ (i.e., orders in K containing $\mathcal{R}_{sp}$) and calculate their class numbers when π is not of the form $\pi_1 \times \pi_1$ with $\pi_1 \in W_p^{\mathrm{ss}}(1)$ (The case $\pi = \pi_1 \times \pi_1$ has already been treated in Section 5.2).

7.1. Orders in products of number fields. Let $K = \prod_{i=1}^{r} K_i$ be a product of number fields, and $\mathcal{S}$ be an order contained in the maximal order $O_K = \prod_{i=1}^{r} O_{K_i}$. We write $\mathrm{pr}_i : K \to K_i$ for the projection map onto the i-th factor. By a theorem of Borevič and Faddeev [1] (see [5, Section 37, p. 789] or [11, Theorem 2.1]), $\mathcal{S}$ is Bass if and only if $O_K/\mathcal{S}$ is cyclic as an $\mathcal{S}$-module. This leads to the following simple criterion when $r = 2$.

Lemma 7.1. *A suborder $\mathcal{S} \subseteq O_{K_1} \times O_{K_2}$ that projects surjectively onto both factors O_{K_1} and O_{K_2} is Bass.*

Proof. Each O_{K_i} is equipped with an $\mathcal{S}$-module structure via the projection map $\mathrm{pr}_i : \mathcal{S} \to O_{K_i}$. Since $\mathrm{pr}_2(\mathcal{S}) = O_{K_2}$, the natural inclusion $O_{K_1} \hookrightarrow O_{K_1} \times O_{K_2}$ defined by $x \mapsto (x, 0)$ induces an isomorphism of S-modules

$$O_{K_1}/(O_{K_1} \cap \mathcal{S}) \xrightarrow{\simeq} (O_{K_1} \times O_{K_2})/\mathcal{S}. \tag{7.1}$$

The left hand side is a cyclic $\mathcal{S}$-module because $\mathrm{pr}_1(\mathcal{S}) = O_{K_1}$. □

We return to the general case with $r \geq 1$. Let $\mathfrak{a}$ be an O_K-lattice (i.e., a fractional O_K-ideal that contains a $\mathbb{Q}$-basis of K) contained in $\mathcal{S}$. There is a one-to-one correspondence between the orders B intermediate to $\mathcal{S} \subseteq O_K$ and the subrings of $O_K/\mathfrak{a}$ containing $\mathcal{S}/\mathfrak{a}$. By [14, Theorem I.12.12], the class number $h(B)$ can be calculated by

$$h(B) = \frac{h(O_K)[(O_K/\mathfrak{a})^\times : (B/\mathfrak{a})^\times]}{[O_K^\times : B^\times]}, \tag{7.2}$$

where $h(O_K) = \prod_{i=1}^{r} h(O_{K_i})$. A priori, [14, Theorem I.12.12] is only stated for the number field case with $\mathfrak{a}$ being the conductor of B, but the same proof applies in the current setting as well.

Lemma 7.2. *Let $\mathfrak{a} \subset O_K$ be an O_K-lattice. If the natural map $O_K^\times \to (O_K/\mathfrak{a})^\times$ is surjective, then $h(B) = h(O_K)$ for every suborder $B \subseteq O_K$ containing $\mathfrak{a}$.*

Proof. Let $\mathfrak{K}$ be the kernel of $O_K^\times \to (O_K/\mathfrak{a})^\times$. Then $\mathfrak{K} \subseteq B^\times$ and $[O_K^\times : B^\times] = [O_K^\times/\mathfrak{K} : B^\times/\mathfrak{K}]$. We identify $O_K^\times/\mathfrak{K}$ with the image of $O_K^\times \to (O_K/\mathfrak{a})^\times$, and similarly for $B^\times/\mathfrak{K}$. By [22, Lemma 2.7], $B^\times = O_K^\times \cap B$. Hence

$$B^\times/\mathfrak{K} = (O_K^\times/\mathfrak{K}) \cap (B/\mathfrak{a}).$$

When $O_K^\times$ maps surjectively onto $(O_K/\mathfrak{a})^\times$, we have $B^\times/\mathfrak{K} = (O_K/\mathfrak{a})^\times \cap (B/\mathfrak{a}) = (B/\mathfrak{a})^\times$. Therefore, $h(B) = h(O_K)$ by (7.2). □

Lemma 7.3. *Let $\mathcal{S}$ be a suborder of $O_K = \prod_{i=1}^{r} O_{K_i}$, and $\mathfrak{c}_1$ be a nonzero ideal of O_{K_1} contained in $\mathrm{pr}_1(\mathcal{S})$. If $x_1 \in O_{K_1}$ is an element such that $(x_1, 0, \cdots, 0) \in \mathcal{S}$, then $(x_1\mathfrak{c}_1, 0, \cdots, 0)$ is an ideal of O_K contained in $\mathcal{S}$. Similar results hold for all $1 \leq i \leq r$.*

Proof. Clearly $(x_1\mathfrak{c}_1, 0, \cdots, 0)$ is an ideal of O_K. For any element $y_1 \in \mathfrak{c}_1$, we may find $\mathbf{y} \in \mathcal{S}$ such that $\mathrm{pr}_1(\mathbf{y}) = y_1$. Then $(x_1y_1, 0, \cdots, 0) = (x_1, 0, \cdots, 0) \cdot \mathbf{y} \in \mathcal{S}$. □

7.2. THE ORDER $\mathcal{R}_{sp}$ IS BASS WHEN $d(\pi) = 2$. We recall the definition of $\mathcal{R}_{sp}$. Suppose that $\pi = \pi_1^{m_1} \times \cdots \times \pi_r^{m_r}$ is a supersingular multiple Weil p-number with $m_i \in \mathbb{N}$ and $\pi_i \not\sim \pi_j$. Let $K = \prod_i K_i$ with $K_i = \mathbb{Q}(\pi_i)$, and $\pi_0 = (\pi_1, \ldots, \pi_r) \in K$. Then $\mathcal{R}_{sp}$ is defined to be the order $\mathbb{Z}[\pi_0, \pi_0^2/p] \subseteq O_K$. Assume that π has dimension 2 and none of π_i is conjugate to $\sqrt{p}$. The case $\pi = \pi_1^2$ with $\pi_1 \in W_p^{\mathrm{ss}}(1)$ has already been studied in Section 5.2. It remains to treat the following two cases:

(1) $\pi = \pi_1 \times \pi_2$ with both $\pi_1, \pi_2 \in W_p^{\mathrm{ss}}(1)$ and $\pi_1 \not\sim \pi_2$ (the nonisotypic product case);
(2) $\pi = \pi_1 \in W_p^{\mathrm{ss}}(2)$ and $\pi_1 \not\sim \sqrt{p}$ (the nonreal simple case).

The first case occurs only when

$$p = 2, 3, \quad \text{and} \quad \pi = \sqrt{p}\,\zeta_4 \times (\pm\sqrt{p}\,\zeta_{4p}), \quad \text{or} \quad \sqrt{p}\,\zeta_{4p} \times (-\sqrt{p}\,\zeta_{4p}). \tag{7.3}$$

In the second case, the supersingular Weil p-numbers of dimension 2 distinct from $\pm\sqrt{p}$ are

$$\sqrt{p}\,\zeta_3,\ \pm\sqrt{p}\,\zeta_5\ (p = 5),\ \sqrt{p}\,\zeta_8\ (p \neq 2),\ \sqrt{p}\,\zeta_{12}\ (p \neq 3),\ \pm\sqrt{p}\,\zeta_{24}\ (p = 2). \tag{7.4}$$

LEMMA 7.4. *Assume $p = 2$ or 3. If $\pi = \sqrt{p}\,\zeta_4 \times (\pm\sqrt{p}\,\zeta_{4p})$, then*

$$\mathcal{R}_{sp} = \mathbb{Z}[(\sqrt{-p}, 0), (0, 1 + \zeta_{2p})] \subset \mathbb{Q}(\sqrt{-p}) \times \mathbb{Q}(\zeta_{2p}) = K.$$

If $\pi = \sqrt{p}\,\zeta_{4p} \times (-\sqrt{p}\,\zeta_{4p})$, then

$$\mathcal{R}_{sp} = \mathbb{Z}[(2(1 + \zeta_{2p}, 0), (\zeta_{2p}, \zeta_{2p})] \subset \mathbb{Q}(\zeta_{2p}) \times \mathbb{Q}(\zeta_{2p}) = K.$$

Proof. Note that $\sqrt{p}\,\zeta_{4p} = 1 + \zeta_{2p}$ when $p = 2$ or 3. If $\pi = \sqrt{p}\,\zeta_4 \times (\pm\sqrt{p}\,\zeta_{4p})$, then

$$\begin{aligned}\mathcal{R}_{sp} &= \mathbb{Z}[(\sqrt{-p}, \pm\sqrt{p}\,\zeta_{4p}), (-1, \zeta_{2p})] = \mathbb{Z}[(\sqrt{-p}, \pm\sqrt{p}\,\zeta_{4p}), (0, 1 + \zeta_{2p})] \\ &= \mathbb{Z}[(\sqrt{-p}, 0), (0, 1 + \zeta_{2p})].\end{aligned}$$

If $\pi = \sqrt{p}\,\zeta_{4p} \times (-\sqrt{p}\,\zeta_{4p})$, then

$$\begin{aligned}\mathcal{R}_{sp} &= \mathbb{Z}[(\sqrt{p}\,\zeta_{4p}, -\sqrt{p}\,\zeta_{4p}), (\zeta_{2p}, \zeta_{2p})] = \mathbb{Z}[(1 + \zeta_{2p}, -(1 + \zeta_{2p})), (\zeta_{2p}, \zeta_{2p})] \\ &= \mathbb{Z}[(2(1 + \zeta_{2p}), 0), (\zeta_{2p}, \zeta_{2p})].\end{aligned}$$

□

PROPOSITION 7.5. *The order $\mathcal{R}_{sp}$ is a Bass order for every supersingular multiple Weil p-number $\pi \in MW_p^{\mathrm{ss}}(2)$ distinct from $\pm\sqrt{p}$.*

Proof. We only need to consider the cases where π is not of the form π_1^2 with $\pi_1 \in W_p^{\mathrm{ss}}(1)$. Suppose that $\pi = \pm\sqrt{p}\,\zeta_n \in W_p^{\mathrm{ss}}(2)$ is one of the Weil p-numbers listed in (7.4), and m is defined as in (3.3). If n is critical at p, then $\mathcal{R}_{sp}$ equals to the maximal order $\mathbb{Z}[\zeta_m]$ in $K = \mathbb{Q}(\zeta_m)$ by Remark 5.2. Otherwise, $[K : \mathbb{Q}(\zeta_m)] = 2$ and $\mathcal{R}_{sp}$ is a quadratic $\mathbb{Z}[\zeta_m]$-order, and such type of orders are Bass [11, Example 2.3].

If $p = 2, 3$ and $\pi = \sqrt{p}\,\zeta_{4p} \times (-\sqrt{p}\,\zeta_{4p})$, or $p = 2$ and $\pi = \sqrt{2}\,\zeta_4 \times (\pm\sqrt{2}\,\zeta_8)$, then $\mathcal{R}_{sp}$ projects surjectively onto both O_{K_1} and O_{K_2}, and hence $\mathcal{R}_{sp}$ is Bass by Lemma 7.1.

Lastly, suppose that $p = 3$ and $\pi = \sqrt{3}\,\zeta_4 \times (\pm\sqrt{3}\,\zeta_{12})$. Then $\mathrm{pr}_1(\mathcal{R}_{sp}) = \mathbb{Z}[\sqrt{-3}]$, a suborder of index 2 in $O_{K_1} = \mathbb{Z}[\zeta_6]$, while $\mathrm{pr}_2(\mathcal{R}_{sp}) = \mathbb{Z}[\zeta_6] = O_{K_2}$.

So by (7.1), to show that $\mathcal{R}_{sp}$ is Bass, it is enough to prove that $O_{K_1}/(O_{K_1}\cap \mathcal{R}_{sp})$ is a cyclic $\mathcal{R}_{sp}$-module. Note that $O_{K_1}\subset O_{K_1}\times O_{K_2}$ is generated by $(1,0)$ and $(\zeta_6,0)$ over $\mathbb{Z}$, and

$$\mathcal{R}_{sp}(\zeta_6,0)\ni(-1+\sqrt{-3}\,,-1)\cdot(\zeta_6,0)=(1,0)+(\sqrt{-3}\,,0)^2\equiv(1,0) \pmod{O_{K_1}\cap\mathcal{R}_{sp}}.$$

Hence $O_{K_1}/(O_{K_1}\cap\mathcal{R}_{sp})$ is a cyclic $\mathcal{R}_{sp}$-module generated by $(\zeta_6,0)$. $\square$

7.3. Suporders of $\mathcal{R}_{sp}$ and class numbers: the nonisotypic product case. Assume that $p=2$ or 3 and $\pi=\pi_1\times\pi_2$ is a supersingular multiple Weil p-number of dimension 2 listed in (7.3). Using Lemma 7.3 and Lemma 7.4, one may easily find an O_K-lattice $\mathfrak{a}$ contained in $\mathcal{R}_{sp}$ and compute the quotient rings $O_K/\mathfrak{a}$ and $\mathcal{R}_{sp}/\mathfrak{a}$. We obtain the following table (For simplicity, we set $i=\zeta_4=\sqrt{-1}\,$).

$\pi=\pi_1\times\pi_2$	$\mathfrak{a}\subset\mathcal{R}_{sp}$	$O_K/\mathfrak{a}$	$\mathcal{R}_{sp}/\mathfrak{a}$
$\sqrt{2}\,\zeta_4\times\pm\sqrt{2}\,\zeta_8$	$\sqrt{-2}\,O_{K_1}\times(1+i)O_{K_2}$	$(\mathbb{F}_2)^2$	$\mathcal{D}_2$
$\sqrt{2}\,\zeta_8\times-\sqrt{2}\,\zeta_8$	$(2(1+i)O_{K_1})^2$	$(\mathbb{Z}[i]/(1+i)^3)^2$	$\mathcal{D}_8$
$\sqrt{3}\,\zeta_4\times\pm\sqrt{3}\,\zeta_{12}$	$(2\sqrt{-3})O_{K_1}\times\sqrt{-3}\,O_{K_2}$	$\mathbb{F}_4\times(\mathbb{F}_3)^2$	$\mathbb{F}_2\times\mathcal{D}_3$
$\sqrt{3}\,\zeta_{12}\times-\sqrt{3}\,\zeta_{12}$	$(2\sqrt{-3}\,)O_{K_1}\times(2\sqrt{-3}\,)O_{K_2}$	$(\mathbb{F}_4\times\mathbb{F}_3)^2$	$\mathcal{D}_{12}$

Here $\mathcal{D}_2$, $\mathcal{D}_8$, $\mathcal{D}_3$, and $\mathcal{D}_{12}$ denote the diagonal in $(\mathbb{F}_2)^2$, $(\mathbb{Z}[i]/(1+i)^3)^2$, $(\mathbb{F}_3)^2$, and $(\mathbb{F}_4\times\mathbb{F}_3)^2$ respectively.

It is an exercise to show that $O_K^\times$ maps surjectively onto $(O_K/\mathfrak{a})^\times$ in all the above cases. By Lemma 7.2, $h(B)=h(O_K)$ for every order B with $\mathcal{R}_{sp}\subseteq B\subseteq O_K$. Note that $h(O_K)=h(O_{K_1})h(O_{K_2})=1$ since both $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_6]$ have class number 1. We obtain the following proposition.

Proposition 7.6. *Assume that $p=2$ or 3 and $\pi=\pi_1\times\pi_2$ is given in (7.3). Then any suporder B of $\mathcal{R}_{sp}$ has class number* 1.

It remains to list all suporders B of $\mathcal{R}_{sp}$ for each π. We recall the convention in Section 5.2 that a suporder of $\mathcal{R}_{sp}$ with index $j>1$ in O_K is denoted by B_j. Our calculation will show that for those π considered in this subsection, if such an order exists, then it is unique. So there is no ambiguity in this notation if π is clear from the context. We separate into cases.

Case $\pi=\sqrt{2}\,\zeta_4\times\pm\sqrt{2}\,\zeta_8$. Since $[O_K:\mathcal{R}_{sp}]=[O_K/\mathfrak{a}:\mathcal{R}_{sp}/\mathfrak{a}]=2$, there are no other suporders of $\mathcal{R}_{sp}$ besides $\mathcal{R}_{sp}$ and O_K.

Case $\pi=\sqrt{3}\,\zeta_4\times\pm\sqrt{3}\,\zeta_{12}$. We have $[O_K:\mathcal{R}_{sp}]=[\mathbb{F}_4\times(\mathbb{F}_3)^2:\mathbb{F}_2\times\mathcal{D}_3]=6$. There are two rings properly intermediate to the inclusion $\mathbb{F}_2\times\mathcal{D}_3\subset\mathbb{F}_4\times(\mathbb{F}_3)^2$, namely $\mathbb{F}_4\times\mathcal{D}_3$ and $\mathbb{F}_2\times(\mathbb{F}_3)^2$. Under the inclusion-preserving correspondence between suborders of O_K containing $\mathfrak{a}$ and subrings of $O_K/\mathfrak{a}$, we have

$$B_3:=\mathbb{Z}[(\sqrt{-3}\,,0),(\zeta_6,\zeta_6)]=\mathbb{Z}[(1+\zeta_6,0),(0,1+\zeta_6)]\longleftrightarrow\mathbb{F}_4\times\mathcal{D}_3,$$
$$B_2:=\mathbb{Z}[\sqrt{-3}\,]\times\mathbb{Z}[\zeta_6]\longleftrightarrow\mathbb{F}_2\times(\mathbb{F}_3)^2.$$

The remaining two cases are best seen in the light of the following lemma.

Lemma 7.7. *Let R be a commutative ring, and $\mathcal{D}$ be the diagonal of R^2. Every subring S of R^2 containing $\mathcal{D}$ decomposes uniquely as $\mathcal{D} \oplus (I_S, 0)$, where I_S is an ideal of R. In particular, there is an inclusion-preserving bijective correspondence between subrings of R^2 containing $\mathcal{D}$ and ideals of R.*

Proof. Every subring of R^2 containing $\mathcal{D}$ is naturally an R-submodule of R^2. So the intersection $(I_S, 0) := S \cap (R, 0)$ is again an R-submodule of R^2. Equivalently, I_S is an ideal of R. Clearly, we have $S = \mathcal{D} \oplus (I_S, 0)$. Conversely, for any ideal $I \subseteq R$, the direct sum $\mathcal{D} \oplus (I, 0)$ is a subring of R^2. The correspondence is established. □

By Lemma 7.4, if $\pi = \sqrt{p}\,\zeta_{4p} \times -\sqrt{p}\,\zeta_{4p}$ with $p = 2$ or 3, then $O_K = \mathbb{Z}[\zeta_{2p}]^2$, and

$$\mathcal{R}_{sp} = \mathbb{Z}[(2(1+\zeta_{2p}), 0), (\zeta_{2p}, \zeta_{2p})] = \mathcal{D} \oplus (2(1+\zeta_{2p})\mathbb{Z}[\zeta_{2p}], 0).$$

Case $\pi = \sqrt{2}\,\zeta_8 \times -\sqrt{2}\,\zeta_8$. We have $2(1+i)\mathbb{Z}[i] = (1+i)^3\mathbb{Z}[i]$. So by Lemma 7.7, the suborders of O_K properly containing $\mathcal{R}_{sp}$ and distinct from O_K are

$$B_4 := \mathbb{Z}[(i,i), (2,0)] \longleftrightarrow (1+i)^2\mathbb{Z}[i] = 2\mathbb{Z}[i],$$
$$B_2 := \mathbb{Z}[(i,i), (1+i,0)] \longleftrightarrow (1+i)\mathbb{Z}[i].$$

Case $\pi = \sqrt{3}\,\zeta_{12} \times -\sqrt{3}\,\zeta_{12}$. In this case, the ideal $2(1+\zeta_6)\mathbb{Z}[\zeta_6]$ factors as the product of the prime ideals $2\mathbb{Z}[\zeta_6]$ and $\sqrt{-3}\,\mathbb{Z}[\zeta_6]$. The suborders of O_K properly containing $\mathcal{R}_{sp}$ and distinct from O_K are

$$B_4 := \mathbb{Z}[(\zeta_6, \zeta_6), (2,0)] \longleftrightarrow 2\mathbb{Z}[\zeta_6],$$
$$B_3 := \mathbb{Z}[(\zeta_6, \zeta_6), (\sqrt{-3}, 0)] \longleftrightarrow \sqrt{-3}\,\mathbb{Z}[\zeta_6].$$

7.4. Suporders of $\mathcal{R}_{sp}$ and class numbers: the nonreal simple case. Assume that π is a supersingular Weil p-number of dimension 2 listed in (7.4). Only the case $\pi = \sqrt{p}\,\zeta_{12}$ with $p \neq 3$ needs to be studied, as the rest have already been covered in Section 5.2.

If $\pi = \sqrt{p}\,\zeta_{12}$, we have $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-3})$, and $\mathcal{R}_{sp} = \mathbb{Z}[\sqrt{-p}, \zeta_6]$. Since the discriminants of $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-p})$ are coprime, O_K is the compositum of $\mathbb{Z}[\zeta_6]$ and $O_{\mathbb{Q}(\sqrt{-p})}$. If $p = 2$ or $p \equiv 1 \pmod 4$, then $O_{\mathbb{Q}(\sqrt{-p})} = \mathbb{Z}[\sqrt{-p}]$, and $\mathcal{R}_{sp}$ is the maximal order in K. We assume that $p \equiv 3 \pmod 4$ and $p \neq 3$ for the rest of this subsection. Note that $2O_K \subseteq \mathcal{R}_{sp}$, and $\mathcal{R}_{sp}/2O_K = \mathbb{Z}[\zeta_6]/(2) \simeq \mathbb{F}_4$, which embeds into $O_K/2O_K \simeq \mathbb{F}_4 \oplus \mathbb{F}_4$ diagonally. It follows that $\mathcal{R}_{sp}$ and O_K are the only orders in O_K containing $\mathcal{R}_{sp}$. By (7.2), $h(\mathcal{R}_{sp}) = 3h(O_K)/[O_K^\times : \mathcal{R}_{sp}^\times]$. It remains to calculate the index $[O_K^\times : \mathcal{R}_{sp}^\times]$.

Lemma 7.8. *Let p_1 and p_2 be distinct primes with $p_1 \equiv p_2 \equiv 3 \pmod 4$, and ϵ be the fundamental unit of $F = \mathbb{Q}(\sqrt{p_1 p_2})$. Then $\sqrt{-\epsilon} \in K = \mathbb{Q}(\sqrt{-p_1}, \sqrt{-p_2})$, and $O_K^\times = \langle \sqrt{-\epsilon} \rangle \times \boldsymbol{\mu}_K$, the direct product of the free abelian group generated by $\sqrt{-\epsilon}$ and the group $\boldsymbol{\mu}_K$ of roots of unity in K. Moreover, if $\epsilon \in \mathbb{Z}[\sqrt{p_1 p_2}]$, then $\sqrt{-\epsilon}$ lies in the $\mathbb{Z}$-module $\mathbb{Z}\sqrt{-p_1} + \mathbb{Z}\sqrt{-p_2} \subset O_K$; otherwise $\sqrt{-\epsilon} \equiv (\sqrt{-p_1} + \sqrt{-p_2})/2 \pmod{\mathbb{Z}\sqrt{-p_1} + \mathbb{Z}\sqrt{-p_2}}$.*

Proof. By Dirichlet's Unit Theorem, the quotient group $O_K^\times/\boldsymbol{\mu}_K$ is a free abelian group of rank 1 containing $O_F^\times/\{\pm 1\} \cong \langle -\epsilon\rangle$ as a subgroup of finite index. In fact, we have $[O_K^\times/\boldsymbol{\mu}_K : O_F^\times/\{\pm 1\}] \le 2$ by [20, Theorem 4.12] as K is a CM-field with maximal totally real subfield F.
Since both $p_i \equiv 3 \pmod 4$, it follows from [7, (V.1.7)] that the norm $\mathrm{N}_{F/\mathbb{Q}}(\epsilon) = +1$. By [3, Lemma 3], $p_1\epsilon$ is a perfect square in $F^\times$. Write $p_1\epsilon = (x+y\sqrt{p_1p_2}\,)^2$ with $x, y \in \mathbb{Q}$. Then

$$\sqrt{-\epsilon} = \sqrt{p_1\epsilon}\cdot\frac{-1}{\sqrt{-p_1}} = (x+y\sqrt{p_1p_2}\,)\cdot\frac{-1}{\sqrt{-p_1}} \in \mathbb{Q}\sqrt{-p_1} + \mathbb{Q}\sqrt{-p_2} \subset K.$$

In particular, $[O_K^\times/\boldsymbol{\mu}_K : O_F^\times/\{\pm 1\}] \ge 2$. It follows that $[O_K^\times/\boldsymbol{\mu}_K : O_F^\times/\{\pm 1\}] = 2$, and $O_K^\times/\boldsymbol{\mu}_K \cong \langle\sqrt{-\epsilon}\,\rangle$. Hence $O_K^\times = \langle\sqrt{-\epsilon}\,\rangle \times \boldsymbol{\mu}_K$.
By our assumption on p_i, the prime 2 is unramified in O_K. One easily checks that the following statements are equivalent:

(1) $\epsilon \in \mathbb{Z}[\sqrt{p_1p_2}\,] = \mathbb{Z} + 2O_F$;
(2) $\epsilon \equiv 1 \pmod{2O_F}$;
(3) $\sqrt{-\epsilon} \equiv 1 \pmod{2O_K}$;
(4) $\sqrt{-\epsilon} \in \mathbb{Z} + 2O_K$.

By Exercise 42(d) of [13, Chapter 2], a $\mathbb{Z}$-basis of O_K is given by

$$\left\{1,\quad \frac{1+\sqrt{-p_1}}{2},\quad \frac{1+\sqrt{-p_2}}{2},\quad \frac{(1+\sqrt{-p_1}\,)(1+\sqrt{-p_2}\,)}{4}\right\}.$$

It follows that

$$O_K \cap (\mathbb{Q}\sqrt{-p_1} + \mathbb{Q}\sqrt{-p_2}\,) = \mathbb{Z}\sqrt{-p_1} + \mathbb{Z}(\sqrt{-p_1} + \sqrt{-p_2}\,)/2;$$
$$(\mathbb{Z} + 2O_K) \cap (\mathbb{Q}\sqrt{-p_1} + \mathbb{Q}\sqrt{-p_2}\,) = \mathbb{Z}\sqrt{-p_1} + \mathbb{Z}\sqrt{-p_2}\,.$$

Therefore, if $\epsilon \in \mathbb{Z}[\sqrt{p_1p_2}]$, then $\sqrt{-\epsilon} \in \mathbb{Z}\sqrt{-p_1} + \mathbb{Z}\sqrt{-p_2}$. Otherwise $\sqrt{-\epsilon}$ lies in $\mathbb{Z}\sqrt{-p_1} + \mathbb{Z}(\sqrt{-p_1} + \sqrt{-p_2}\,)/2$ but not in $\mathbb{Z}\sqrt{-p_1} + \mathbb{Z}\sqrt{-p_2}$. Hence $\sqrt{-\epsilon} \equiv (\sqrt{-p_1} + \sqrt{-p_2}\,)/2 \pmod{\mathbb{Z}\sqrt{-p_1} + \mathbb{Z}\sqrt{-p_2}\,}$ in this case. □

We return to the assumption that $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-3}\,)$ with $p \equiv 3 \pmod 4$ and $p \ne 3$. Note that $\boldsymbol{\mu}_K = \langle\zeta_6\rangle \subset \mathcal{R}_{sp}^\times$, and $\mathcal{R}_{sp} \cap (\mathbb{Q}\sqrt{-p} + \mathbb{Q}\sqrt{-3}\,) = (\mathbb{Z}\sqrt{-p} + \mathbb{Z}\sqrt{-3}\,)$. Let ϵ be the fundamental unit of $F = \mathbb{Q}(\sqrt{3p}\,)$. If $\epsilon \in \mathbb{Z}[\sqrt{3p}]$, then $\sqrt{-\epsilon} \in \mathcal{R}_{sp}$, and hence $\mathcal{R}_{sp}^\times = O_K^\times$. This holds in particular when $p \equiv 3 \pmod 8$ and $p \ne 3$ as remarked after (1.2). Assume that $p \equiv 7 \pmod 8$ and $\epsilon \notin \mathbb{Z}[\sqrt{3p}]$. Then $(O_F/2O_F)^\times \simeq \mathbb{F}_4^\times$ and $\epsilon^3 \in \mathbb{Z} + 2O_F = \mathbb{Z}[\sqrt{3p}]$. On the other hand, $[(O_K/2O_K)^\times : (\mathcal{R}_{sp}/2O_K)^\times] = [(\mathbb{F}_4^\times)^2 : \mathbb{F}_4^\times] = 3$, so we have $\sqrt{-\epsilon} \notin \mathcal{R}_{sp}$ but $(\sqrt{-\epsilon}\,)^3 \in \mathcal{R}_{sp}$.
In summary, we find that

$$[O_K^\times : \mathcal{R}_{sp}^\times] = [O_F^\times : \mathbb{Z}[\sqrt{3p}\,]^\times] = \begin{cases} 1 & \text{if } \epsilon \in \mathbb{Z}[\sqrt{3p}]; \\ 3 & \text{otherwise.} \end{cases}$$

Therefore, we have $h(\mathcal{R}_{sp}) = \varpi_{3p} h(O_K)$, where $\varpi_{3p} = 3/[O_F^\times : \mathbb{Z}[\sqrt{3p}\,]^\times]$ as defined in (1.2).

Acknowledgements

J. Xue is partially supported by the 1000-plan program for young talents of PRC. He thanks Academia Sinica and NCTS for their hospitality and great working conditions. TC Yang and CF Yu are partially supported by the grants MoST 100-2628-M-001-006-MY4, 103-2811-M-001-142, 104-2115-M-001-001MY3 and 104-2811-M-001-066. The authors thank the referee for careful reading and helpful suggestions.

References

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

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

[4] Tommaso Giorgio Centeleghe and Jakob Stix. Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$. *Algebra Number Theory*, 9(1):225–265, 2015.

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

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

[7] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[8] Kuniaki Horie and Mitsuko Horie. CM-fields and exponents of their ideal class groups. *Acta Arith.*, 55(2):157–170, 1990.

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

[10] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57(2):127–152, 1986.

[11] Lawrence S. Levy and Roger Wiegand. Dedekind-like behavior of rings with 2-generated ideals. *J. Pure Appl. Algebra*, 37(1):41–58, 1985.

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

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

[14] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[15] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[16] Sheng-Chi Shih, Tse-Chung Yang, and Chia-Fu Yu. Embeddings of fields into simple algebras over global fields. *Asian J. Math.*, 18(2):365–386, 2014.

[17] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

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

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

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

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

[22] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Supersingular abelian surfaces and Eichler's class number formula. *arXiv:1404.2978v3*. 29 pp.

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

[24] Chia-Fu Yu. On arithmetic of the superspecial locus. *arXiv:1210.1120v2*. 35 pp.

[25] Chia-Fu Yu. Simple mass formulas on Shimura varieties of PEL-type. *Forum Math.*, 22(3):565–582, 2010.

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

[27] Chia-Fu Yu. Endomorphism algebras of QM abelian surfaces. *J. Pure Appl. Algebra*, 217(5):907–914, 2013.

[28] Don Zagier. On the values at negative integers of the zeta-function of a real quadratic field. *Enseignement Math. (2)*, 22(1-2):55–95, 1976.

Jiangwei Xue
Collaborative Innovation Centre of Mathematics
School of Mathematics and Statistics
Wuhan University
Luojiashan
Wuhan, Hubei 430072 P.R. China.
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
tsechung@math.sinica.edu.tw

Chia-Fu Yu
Institute of Mathematics
Academia Sinica and NCTS
Astronomy-Mathematics
Building No. 1, Sec. 4
Roosevelt Road
Taipei 10617
TAIWAN
chiafu@math.sinica.edu.tw