ON COUNTING CERTAIN PRINCIPALLY POLARIZED SUPERSPECIAL ABELIAN SURFACES OVER $\mathbb{F}_p$

JIANGWEI XUE AND CHIA-FU YU

ABSTRACT. This is the survey paper [25] of the joint work in progress. We study the principally polarized superspecial abelian surfaces over the prime finite field $\mathbb{F}_p$ with Frobenius endomorphism π satisfying $\pi^2 = p$. The set of isomorphism classes of such objects is described by a disjoint union of double coset spaces, and the cardinality of each such space is calculated using the Selberg trace formula.

1. INTRODUCTION

Throughout this paper, $p \in \mathbb{N}$ denotes a prime number, and $q \in \mathbb{N}$ a power of p. An algebraic integer $\pi \in \bar{\mathbb{Q}} \subset \mathbb{C}$ is called a Weil q-number if $|\sigma(\pi)| = \sqrt{q}$ for every embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$. By the Honda-Tate Theorem [18, Theorem 1], there is a bijection between the isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of Weil q-numbers. Let X_π be a simple abelian variety over $\mathbb{F}_q$ in the isogeny class corresponding to (the conjugacy class of) a Weil q-number π. Both the dimension $g(\pi) := \dim(X_\pi)$ and the endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_q}(X_\pi) := \mathrm{End}_{\mathbb{F}_q}(X_\pi) \otimes_{\mathbb{Z}} \mathbb{Q}$ are invariants of the isogeny class and can be determined explicitly from π (ibid.). Recall that $\mathrm{End}^0_{\mathbb{F}_q}(X_\pi)$ is a finite-dimensional central division $\mathbb{Q}(\pi)$-algebra.

It is well known [31, 4.1] that for each fixed $g \geq 1$, there are only finitely many g-dimensional abelian varieties over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism. Let $\mathrm{Isog}(\pi)$ be the finite set of isomorphism classes of simple abelian varieties $X/\mathbb{F}_q$ in the isogeny class corresponding to π. Similarly, let $\mathrm{PPAV}(\pi)$ be the set of isomorphism classes of principally polarized abelian varieties $(X, \lambda)/\mathbb{F}_q$ with the $\mathbb{F}_q$-isomorphism class $[X] \in \mathrm{Isog}(\pi)$, which is again finite since it corresponds to a subset of $\mathbb{F}_q$-points in the Siegel moduli scheme $\mathscr{A}_{g(\pi)}$ [3, Theorem 1.4] (see also [9, Part III] and [12]). Therefore, it is natural to ask:

Question. *How to compute the cardinalities* $|\mathrm{Isog}(\pi)|$ *and* $|\mathrm{PPAV}(\pi)|$*?*

In this note, we provide the explicit formulas for $|\mathrm{PPAV}(\pi)|$ in the case $\pi = \pm\sqrt{p}$. The computation relies on that of $|\mathrm{Isog}(\sqrt{p})|$, which was previously calculated in [23]. For simplicity, $h(d)$ denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$ for every square-free integer $d \in \mathbb{Z}$.

Theorem 1.1. *(1)* $|\mathrm{PPAV}(\sqrt{p})| = 1, 1, 2$ *for* $p = 2, 3, 5$*, respectively.*

Date: June 28, 2019.
2010 *Mathematics Subject Classification.* 11G10, 11R52, 11F72.
Key words and phrases. supersingular abelian surfaces, class number formula, trace formula.

(2) For $p \geq 13$ and $p \equiv 1 \pmod 4$, we have

$$|\,\mathrm{PPAV}(\sqrt{p}\,)| = \left(9 - 2\left(\frac{2}{p}\right)\right)\frac{\zeta_F(-1)}{2} + \frac{3h(-p)}{8} + \left(3 + \left(\frac{2}{p}\right)\right)\frac{h(-3p)}{6}. \tag{1.1}$$

(3) For $p \geq 7$ and $p \equiv 3 \pmod 4$, we have

$$|\,\mathrm{PPAV}(\sqrt{p}\,)| = \frac{\zeta_F(-1)}{2} + \left(11 - 3\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-3p)}{6}. \tag{1.2}$$

Here $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, and the special value $\zeta_F(-1)$ of the Dedekind zeta function $\zeta_F(s)$ can be calculated by the Siegel's formula [30, Table 2, p. 70].

The Weil p-numbers $\pm\sqrt{p}$ are exceptional in several ways. Given a Weil q-number π, the number field $\mathbb{Q}(\pi)$ is a CM-field (i.e. a totally imaginary quadratic extension of a totally real field) unless $\pi = \pm\sqrt{q}$. First, suppose that $\pi \neq \pm\sqrt{q}$. From [26, Proposition 2.2], one has

$$|\mathrm{Isog}(\pi)| = N_\pi \cdot h(\mathbb{Q}(\pi)), \tag{1.3}$$

where N_π is a positive integer, and $h(\mathbb{Q}(\pi))$ is the class number of $\mathbb{Q}(\pi)$. It should be mentioned that N_π is highly dependent on π and can be challenging to calculate explicitly in general. See the discussions in [12, §3.2] and [24, §2.4]. The proof of (1.3) relies on a strong approximation argument, which fails for the Weil q-numbers $\pm\sqrt{q}$. The distinction is further amplified in the case $q = p$. If π is a Weil p-number distinct from $\pm\sqrt{p}$, then by [22, Theorem 6.1],

$$\mathrm{End}^0_{\mathbb{F}_p}(X_\pi) = \mathbb{Q}(\pi) \tag{1.4}$$

for every abelian variety X_π in the isogeny class corresponding to π, while (1.4) does not hold for the Weil p-numbers $\pm\sqrt{p}$. Consequently, many theories for abelian varieties over $\mathbb{F}_p$ have to make an exception for the isogeny class corresponding to $\pm\sqrt{p}$. See [2, §1.3] and [12, Theorem 0.3].

Next, suppose that $\pi = \pm\sqrt{q}$. Write $q = p^a$ with $a \in \mathbb{N}$. There are two cases to consider. If a is even, then X_π is a supersingular elliptic curve with $\mathrm{End}^0_{\mathbb{F}_q}(X_\pi) \simeq D_{p,\infty}$, the unique quaternion $\mathbb{Q}$-algebra ramified exactly at p and ∞. It is known [22, Theorem 4.2] that the endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(X_\pi)$ is a maximal order in $\mathrm{End}^0_{\mathbb{F}_q}(X_\pi)$ for every X_π in this case. Fix a maximal order $\mathcal{O}_0$ in $D_{p,\infty}$ and write $a = 2m$. It is a classical result of Deuring and later re-interpreted by Waterhouse [22, Theorem 4.5] that

$$\begin{aligned} |\mathrm{PPAV}(\pm p^m)| &= |\mathrm{Isog}(\pm p^m)| = h(\mathcal{O}_0) \\ &= \frac{p-1}{12} + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right), \end{aligned} \tag{1.5}$$

where $h(\mathcal{O}_0)$ is the class number of $\mathcal{O}_0$; see [20, p. 26].

If a is odd, then X_π is a supersingular abelian surface, and it is even superspecial [10, §1.7] if $a = 1$ (i.e. $q = p$). Similar to the previous case, we have $\mathrm{End}^0_{\mathbb{F}_q}(X_\pi) \simeq D_{\infty_1,\infty_2}$, the unique quaternion $\mathbb{Q}(\sqrt{p}\,)$-algebra ramified exactly at the two infinite places of $\mathbb{Q}(\sqrt{p}\,)$ and splits at all finite places. Therefore, Theorem 1.1 may be regarded as a generalization of (1.5) in the prime field case. Compared with the elliptic curve case, $\mathrm{End}_{\mathbb{F}_q}(X_\pi)$ is no longer necessarily a maximal order in $\mathrm{End}^0_{\mathbb{F}_q}(X_\pi)$ even in the case $a = 1$ [22, Theorem 6.2], which causes new difficulties. The formula for $|\mathrm{Isog}(\sqrt{p^a})|$ with a odd is given in [23, Theorem 1.2] for $a = 1$ and in [26, Theorem 4.4] for a general odd a.

2. Method of Calculation

Given an arbitrary Weil q-number π, there are several ways to calculate $|\mathrm{Isog}(\pi)|$ and $|\mathrm{PPAV}(\pi)|$. Kottwitz expresses $|\mathrm{PPAV}(\pi)|$ in terms of orbital integrals in [9, §12]. The method for calculating $|\mathrm{Isog}(\pi)|$ is covered by Lipnowski and Tsimerman in [12, §3], where they also give nice bounds for the size of $\mathrm{Isog}(\pi)$. For the purpose of this note, we follow the method in [26], which is previously developed by the second named author in [29]. While the idea is similar to that of [12, §3], the present method treats both the unpolarized case and the principally polaried case uniformly and expresses the cardinalities as sums of class numbers of linear algebraic groups over $\mathbb{Q}$. The key part of this method works not only over finite fields, but also over any *finitely generated* ground field k (that is, finitely generated over its prime subfield).

Given an abelian variety X over k and a prime number ℓ (not necessarily distinct from the $\mathrm{char}(k)$), we write $X(\ell)$ for the ℓ-divisible group $\varinjlim X[\ell^n]$ associated to X. A $\mathbb{Q}$-*isogeny* $\varphi : X_1 \to X_2$ between two abelian varieties over k is an element $\varphi \in \mathrm{Hom}_k(X_1, X_2) \otimes \mathbb{Q}$ such that $N\varphi$ is an isogeny for some $N \in \mathbb{N}$. Similarly, one defines the notion of $\mathbb{Q}_\ell$-isogenies between ℓ-divisible groups. It is clear that φ induces a $\mathbb{Q}_\ell$-isogeny $\varphi_\ell : X_1(\ell) \to X_2(\ell)$ for each ℓ, and φ_ℓ is an isomorphism for almost all ℓ.

Fix an abelian variety X_0 over k. Two $\mathbb{Q}$-isogenies $\varphi_1 : X_1 \to X_0$ and $\varphi_2 : X_2 \to X_0$ are said to be *equivalent* if there exists an isomorphism $\theta : X_1 \to X_2$ such that $\varphi_2 \circ \theta = \varphi_1$. Let $\mathrm{Qisog}(X_0)$ be the set of equivalence classes of $\mathbb{Q}$-isogenies (X, φ) to X_0. By an abuse of notation, we still write (X, φ) for its equivalence class. Note that $\mathrm{Qisog}(X_0)$ contains a distinguished element (X_0, id_0), where id_0 is the identity map of X_0. For any member $(X_1, \varphi_1) \in \mathrm{Qisog}(X_0)$, we have a bijection

$$\mathrm{Qisog}(X_0) \to \mathrm{Qisog}(X_1), \qquad (X, \varphi) \mapsto (X, \varphi_1^{-1}\varphi). \tag{2.1}$$

Therefore, we may change the base abelian variety X_0 to suit our purpose. Similarly, one defines $\mathrm{Qisog}(X_0(\ell))$ for every prime ℓ.

Let G be the algebraic group over $\mathbb{Q}$ that represents the functor

$$R \mapsto G(R) := (\mathrm{End}_k(X_0) \otimes_{\mathbb{Q}} R)^\times$$

for every commutative $\mathbb{Q}$-algebra R. It is clear that G depends only on the isogeny class of X_0. We have $G(\mathbb{Q}_\ell) = (\mathrm{End}_k(X_0(\ell)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^\times$ by Tate's theorem (due to Tate, Zarhin, Faltings and de Jong). Let $\mathbb{A}_f := \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ be the ring of finite adeles. There is an action of $G(\mathbb{A}_f)$ on $\mathrm{Qisog}(X_0)$ given by the following lemma.

Lemma 2.1 ([26, Lemma 5.2])**.** *For any $(X, \varphi) \in \mathrm{Qisog}(X_0)$ and any $\alpha = (\alpha_\ell) \in G(\mathbb{A}_f)$, there is a unique member $(X', \varphi') \in \mathrm{Qisog}(X_0)$ such that*

$$(X'(\ell), \varphi'_\ell) = (X(\ell), \alpha_\ell \varphi_\ell)$$

in $\mathrm{Qisog}(X_0(\ell))$ for every prime ℓ.

We equip $\mathrm{Qisog}(X_0)$ with the discrete topology. Then the action of $G(\mathbb{A}_f)$ on $\mathrm{Qisog}(X_0)$ is continuous and proper. Indeed, the stabilizer of any $(X, \varphi) \in \mathrm{Qisog}(X_0)$ is an open compact subgroup of $G(\mathbb{A}_f)$.

Definition 2.2. Let $H \subseteq G$ be an algebraic subgroup of G over $\mathbb{Q}$. Two members $(X_i, \varphi_i) \in \mathrm{Qisog}(X_0)$ for $i = 1, 2$ are said to be in the *same H-genus* if there exists $\alpha \in H(\mathbb{A}_f)$ such that $(X_2, \varphi_2) = \alpha(X_1, \varphi_1)$. They are said to be *$H$-isomorphic* if there exists $\alpha \in H(\mathbb{Q})$ such that $(X_2, \varphi_2) = (X_1, \alpha\varphi_1)$.

Proposition 2.3. *Let $\mathscr{G}_H(X_0) \subseteq \mathrm{Qisog}(X_0)$ be the H-genus containing (X_0, id_0), and $\Lambda_H(X_0)$ be the set of H-isomorphism classes within $\mathscr{G}_H(X_0)$. Put $U_H(X_0) := \mathrm{Stab}_{H(\mathbb{A}_f)}(X_0, \mathrm{id}_0)$, the stabilizer of (X_0, id_0) in $H(\mathbb{A}_f)$. Then there is a bijection*

$$\Lambda_H(X_0) \quad \longleftrightarrow \quad H(\mathbb{Q})\backslash H(\mathbb{A}_f)/U_H(X_0),$$

sending the H-isomorphic class $[(X_0, \mathrm{id}_0)]$ to the identity class on the right.

From [16, Theorem 8.1], $\Lambda_H(X_0)$ is a finite set. Proposition 2.3 turns out to be quite versatile. By varying H, it can be used to count abelian varieties with various additional structures. We give two examples below.

First, let us look at the case $H = G$. Two members $(X_i, \varphi_i) \in \mathrm{Qisog}(X_0)$ for $i = 1, 2$ are said to be in the *same genus* if $X_1(\ell)$ is isomorphic to $X_2(\ell)$ for every prime ℓ. It is clear that (X_i, φ_i) for $i = 1, 2$ are in the same genus if and only if there exists $\alpha \in G(\mathbb{A}_f)$ such that $(X_2, \varphi_2) = \alpha(X_1, \varphi_1)$. Similarly, X_1 and X_2 are isomorphic if and only if there exists $\alpha \in G(\mathbb{Q})$ such that $(X_2, \varphi_2) = (X_1, \alpha\varphi_1)$. Therefore, Proposition 2.3 recovers [26, Proposition 5.4] in the case $H = G$.

Next, we study polarized abelian varieties. Let $X^\vee$ be the dual abelian variety of X. A $\mathbb{Q}$-isogeny $\lambda : X \to X^\vee$ is said to be a $\mathbb{Q}$-*polarization* if $N\lambda$ is a polarization for some $N \in \mathbb{N}$. For each ℓ, the $\mathbb{Q}$-polarization λ induces a $\mathbb{Q}_\ell$-quasipolarization of $X(\ell)$ (see [14, §1] and [10, §5.9]). An isomorphism (resp. $\mathbb{Q}$-isogeny) from a $\mathbb{Q}$-polarized abelian variety (X_1, λ_1) to another (X_2, λ_2) is an isomorphism (resp. $\mathbb{Q}$-isogeny) $\varphi : X_1 \to X_2$ such that

$$\lambda_1 = \varphi^*\lambda_2 := \varphi^\vee \circ \lambda_2 \circ \varphi. \tag{2.2}$$

Fix a $\mathbb{Q}$-polarized abelian variety (X_0, λ_0). Once again two $\mathbb{Q}$-isogenies $\varphi_i : (X_i, \lambda_i) \to (X_0, \lambda_0)$ for $i = 1, 2$ are said to be *equivalent* if there exists an isomorphism $\theta : (X_1, \lambda_1) \to (X_2, \lambda_2)$ such that $\varphi_1 = \varphi_2 \circ \theta$. We define $\mathrm{Qisog}(X_0, \lambda_0)$ to be the set of equivalence classes of all $\mathbb{Q}$-isogenies (X, λ, φ) to (X_0, λ_0). The forgetful map $(X, \lambda, \varphi) \mapsto (X, \varphi)$ induces a bijection:

$$F(\lambda_0) : \mathrm{Qisog}(X_0, \lambda_0) \to \mathrm{Qisog}(X_0), \tag{2.3}$$

whose inverse is given by $(X, \varphi) \mapsto (X, \varphi^*\lambda_0, \varphi)$. Let $G^1 \subseteq G$ be the algebraic subgroup over $\mathbb{Q}$ that represents the functor

$$R \mapsto G^1(R) := \{g \in (\mathrm{End}_k(X_0) \otimes_{\mathbb{Q}} R)^\times \mid g^\vee \circ \lambda_0 \circ g = \lambda_0\} \tag{2.4}$$

for every commutative $\mathbb{Q}$-algebra R.

Two members $(X_i, \lambda_i, \varphi_i) \in \mathrm{Qisog}(X_0, \lambda_0)$ for $i = 1, 2$ are said to be in the *same genus* if $(X_1(\ell), \lambda_{1,\ell})$ is isomorphic to $(X_2(\ell), \lambda_{2,\ell})$ for every prime ℓ. As before, one shows that $(X_i, \lambda_i, \varphi_i)$ are in the same genus if and only if (X_i, φ_i) are in the same G^1-genus, and (X_i, λ_i) are isomorphic if and only if (X_i, φ_i) are G^1-isomorphic. Therefore, when $H = G^1$, Proposition 2.3 recovers a partial case of [26, Theorem 5.8].

Lemma 2.4 ([26, Remark 5.7])**.** *Let $\mathscr{G}(X_0, \lambda_0) \subseteq \mathrm{Qisog}(X_0, \lambda_0)$ be the genus containing $(X_0, \lambda_0, \mathrm{id}_0)$. Assume that λ_0 is an integral polarization on X_0, i.e. not just a $\mathbb{Q}$-polarization. Then λ is a integral polarization on X for every member $(X, \lambda, \varphi) \in \mathscr{G}(X_0, \lambda_0)$. If moreover λ_0 is principal, then so is λ.*

Let us return to the finite field case. Assume that $k = \mathbb{F}_q$, and π is a Weil q-number. It is possible that $\mathrm{PPAV}(\pi) = \emptyset$ (see [8, Theorem 1]). Suppose that this is not the case so that there is something to count. Combining Lemma 2.4 and Proposition 2.3, we may compute $|\mathrm{PPAV}(\pi)|$ in the following steps:

(1) Separate $\mathrm{PPAV}(\pi)$ into $\mathbb{Q}$-isogeny classes.
(2) For each $\mathbb{Q}$-isogeny class in $\mathrm{PPAV}(\pi)$, separate it further into genera (Note that the notation of *genus* need not depend on the $\mathbb{Q}$-isogeny φ). This amounts to classifying principal quasi-polarized ℓ-divisible groups of certain kind for each prime ℓ.
(3) By the above discussion, the cardinality of genus in $\mathrm{PPAV}(\pi)$ represented by a member (X_0, λ_0) is equal to the class number

$$|G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{G^1}(X_0)|. \tag{2.5}$$

(4) Varying (X_0, λ_0) genus by genus, we obtain $|\mathrm{PPAV}(\pi)|$ by summing up all such class numbers.

In subsequent sections, we apply these steps to the Weil p-number $\pi = \sqrt{p}$.

3. Classification of $\mathbb{Q}$-isogeny classes and genera

From now on, we fix the Weil p-number $\pi = \sqrt{p}$ and work over the prime finite field $\mathbb{F}_p$. In particular, all isogenies, polarizations ect. are defined over $\mathbb{F}_p$. As mentioned in the Introduction, every $X/\mathbb{F}_p$ in the isogeny class corresponding to $\pi = \sqrt{p}$ is a superspecial abelian surface with

$$\mathrm{End}^0_{\mathbb{F}_p}(X) = D_{\infty_1,\infty_2}, \tag{3.1}$$

the unique quaternion $\mathbb{Q}(\sqrt{p})$-algebra ramified exactly at the two infinite places of $\mathbb{Q}(\sqrt{p})$ and unramified at all finite places. For simplicity, we set

$$F = \mathbb{Q}(\sqrt{p}) \quad \text{and} \quad D = D_{\infty_1,\infty_2}. \tag{3.2}$$

The ring of integers of F is denoted by O_F.

3.1. **The uniqueness of $\mathbb{Q}$-isogeny class and nonemptiness of** $\mathrm{PPAV}(\sqrt{p})$**.** Since D is totally definite over F, there is a unique positive involution on D, namely, the canonical involution $x \mapsto \bar{x} := \mathrm{Tr}(x) - x$ (see [13, Theorem 2, §21]). It follows that the Rosati involution induced by any polarization λ on X coincides with the canonical involution. Let (X_0, λ_0) be a member in $\mathrm{PPAV}(\sqrt{p})$, whose nonemptiness is guaranteed by Lemma 3.2 below. The group G^1 in (2.4) is just the group of reduced norm one, that is, for any commutative $\mathbb{Q}$-algebra R,

$$G^1(R) = \{g \in (D \otimes_{\mathbb{Q}} R)^\times \mid \mathrm{Nr}(g) = \bar{g}g = 1\}. \tag{3.3}$$

In particular, we have

$$U_{G^1}(X_0) = \widehat{\mathcal{O}}^1 := \{x \in \widehat{\mathcal{O}} := \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \mid \mathrm{Nr}(x) = 1\}, \quad \text{where } \mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(X_0). \tag{3.4}$$

Lemma 3.1. *For any two $\mathbb{Q}$-polarized abelian surfaces $(X_i, \lambda_i)/\mathbb{F}_p$ with X_i in the isogeny class corresponding to $\pi = \sqrt{p}$, there exists a $\mathbb{Q}$-isogeny $\varphi : X_1 \to X_2$ such that $\varphi^*\lambda_2 = \lambda_1$.*

This lemma can be reduced to [28, Corollary 10.3]. It shows that there is a unique $\mathbb{Q}$-isogeny class of $\mathbb{Q}$-polarized abelian varieties for the Weil number $\pi = \sqrt{p}$.

Lemma 3.2. $\mathrm{PPAV}(\sqrt{p}) \neq \emptyset$*.*

Proof. Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve with Frobenius endomorphism $\pi_E = p$, and λ_E be the canonical principal polarization on E. We define

$$(Y, \lambda_Y) := \mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E, \lambda_E). \tag{3.5}$$

Then $[(Y, \lambda_Y)] \in \mathrm{PPAV}(\sqrt{p})$. Alternatively, one may apply [8, Theorem 5]. □

In fact, more can be said about (Y, λ_Y) in (3.5). By functoriality, we have

$$\mathrm{End}_{\mathbb{F}_{p^2}}(E) \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{p}] \subseteq \mathrm{End}_{\mathbb{F}_p}(Y). \tag{3.6}$$

These two rings differ only at the prime p by [7, Remark 4, §2.1]:

$$\mathrm{End}_{\mathbb{F}_{p^2}}(E) \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{p}][1/p] \simeq \mathrm{End}_{\mathbb{F}_p}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]. \tag{3.7}$$

Recall that $\mathrm{End}_{\mathbb{F}_{p^2}}(E)$ is always a maximal $\mathbb{Z}$-order in $\mathrm{End}^0_{\mathbb{F}_{p^2}}(E) \simeq D_{p,\infty}$, the unique quaternion $\mathbb{Q}$-algebra ramified exactly at $\{p, \infty\}$. On the other hand, if $p \not\equiv 1 \pmod 4$, then $O_F = \mathbb{Z}[\sqrt{p}]$, and $\mathrm{End}_{\mathbb{F}_p}(Y)$ is a maximal O_F-order in $\mathrm{End}^0_{\mathbb{F}_p}(Y) \simeq D$ by [22, Theorem 6.2]. It follows that (3.6) is a strict inclusion in this case. Nevertheless, $\mathrm{End}_{\mathbb{F}_p}(Y)$ is uniquely determined by $\mathrm{End}_{\mathbb{F}_{p^2}}(E)$ thanks to the following lemma (see [11, Lemma 2.11]):

Lemma 3.3. *Let $p \in \mathbb{N}$ be an arbitrary prime number. For every maximal $\mathbb{Z}$-order $\mathcal{O}_0$ in $D_{p,\infty}$, there exists a unique maximal O_F-order $\mathcal{M}(\mathcal{O}_0)$ in $D = D_{p,\infty} \otimes_{\mathbb{Q}} F$ containing $\mathcal{O}_0 \otimes_{\mathbb{Z}} O_F$.*

In general, given a quaternion algebra $\mathbf{B}$ over a number field L, we write $\mathrm{Tp}(\mathbf{B})$ for the finite set of $\mathbf{B}^\times$-conjugacy classes of maximal O_L-orders in $\mathbf{B}$. The $\mathbf{B}^\times$-conjugacy class of a maximal O_L-order $\mathcal{O} \subseteq \mathbf{B}$ is denoted by $[\![\mathcal{O}]\!]$. From Lemma 3.3, there is a well-defined map:

$$\mathcal{M} : \mathrm{Tp}(D_{p,\infty}) \to \mathrm{Tp}(D), \quad [\![\mathcal{O}_0]\!] \mapsto [\![\mathcal{M}(\mathcal{O}_0)]\!]. \tag{3.8}$$

On the other hand, if $p \not\equiv 1 \pmod 4$, we have a canonical map

$$\Psi : \mathrm{PPAV}(\sqrt{p}) \to \mathrm{Tp}(D), \qquad (X, \lambda) \mapsto \left[\!\left[\mathrm{End}_{\mathbb{F}_p}(X)\right]\!\right]. \tag{3.9}$$

From [22, Theorem 3.14], every maximal $\mathbb{Z}$-order in $D_{p,\infty}$ is realizable as $\mathrm{End}_{\mathbb{F}_{p^2}}(E)$ for some elliptic curve $E/\mathbb{F}_{p^2}$ with $\pi_E = p$. It follows that

$$\mathrm{img}(\mathcal{M}) \subseteq \mathrm{img}(\Psi) \qquad \text{if} \quad p \not\equiv 1 \pmod 4. \tag{3.10}$$

Example 3.4. For $p = 3$, we have $|\mathrm{Tp}(D)| = 2$ by [11, Theorem 1.6], so

$$\mathrm{Tp}(D) = \{[\![\mathbb{O}_1]\!], [\![\mathbb{O}_2]\!]\}, \quad \text{with} \quad \mathbb{O}_1^\times/O_F^\times \simeq D_{12}, \quad \mathbb{O}_2^\times/O_F^\times \simeq S_4.$$

On the other hand, $|\mathrm{Tp}(D_{3,\infty})| = 1$, and we can show that $\mathrm{img}(\mathcal{M}) = \{[\![\mathbb{O}_1]\!]\}$. It will be shown in Lemma 4.1 that $\mathrm{img}(\Psi)$ is a proper subset of $\mathrm{Tp}(D)$, so we have $\mathrm{img}(\Psi) = \{[\![\mathbb{O}_1]\!]\}$.

3.2. **The genera.** For simplicity, let $A = \mathbb{Z}[\sqrt{p}]$. Note that

$$[O_F : A] = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 4; \\ 1 & \text{otherwise.} \end{cases} \tag{3.11}$$

For each prime ℓ, we use a subscript ℓ to indicate ℓ-adic completion. For example, A_ℓ denotes the ℓ-adic completion of A, i.e. $A_\ell = A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.

In general, let k be a perfect field of characteristic $p > 0$, and X be an abelian variety over k. For each prime $\ell \neq p$, the Tate module $T_\ell(X) = \varprojlim X[\ell^n]$ is a free $\mathbb{Z}_\ell$-module of rank $2\dim(X)$ with a continuous action by $\mathrm{Gal}(k_s/k)$, where k_s is a separable closure of k. The ℓ-divisible group $X(\ell)$ is uniquely determined by $T_\ell(X)$, and vice versa. Similarly, the p-divisible group $X(p)$ is uniquely determined by its (covariant) Dieudonné module $M(X)$. A polarization λ on X induces a Weil pairing at each prime:

$$e_{\lambda,\ell} : T_\ell(X) \times T_\ell(X) \to \mathbb{Z}_\ell(1), \qquad \forall \ell \neq p, \tag{3.12}$$

$$e_{\lambda,p} : M(X) \times M(X) \to W, \tag{3.13}$$

where $\mathbb{Z}_\ell(1) = \varprojlim \boldsymbol{\mu}_{\ell^n}(k_s)$, and $W = W(k)$ denotes the ring of Witt vectors over k. The Weil pairings are alternating, nondegenerate, and satisfy the following conditions:

(i) $e_{\lambda,\ell}$ is $\mathrm{Gal}(k_s/k)$-equivariant;
(ii) $e_{\lambda,p}(\mathcal{F}x, y) = e_{\lambda,p}(x, \mathcal{V}y)^\sigma$ for all $x, y \in M(X)$.

Here $\mathcal{F}$ and $\mathcal{V}$ denote respectively the Frobenious and Verschiebung map on $M(X)$, and σ the Frobenious automorphism of W. The polarization λ is principal if and only if the Weil pairings are perfect at every prime.

Now we return to the case that $k = \mathbb{F}_p$, and X is an abelian surface in the isogeny class corresponding to $\pi = \sqrt{p}$. At every prime $\ell \neq p$, the Galois action equips $T_\ell(X)$ with an $A_\ell := \mathbb{Z}_\ell[\sqrt{p}\,]$-module structure. Similarly, at the prime p, we have $W(\mathbb{F}_p) = \mathbb{Z}_p$, and the Dieudonné module $M(X)$ is nothing but a torsion-free $\mathbb{Z}_p[\sqrt{p}\,]$-module with $\mathrm{rank}_{\mathbb{Z}_p} M(X) = 4$. Without lose of generality, we set $T_p(X) = M(X)$ and ℓ is no longer necessarily distinct from p.

Recall that two members X_i for $i = 1, 2$ in $\mathrm{Isog}(\sqrt{p}\,)$ are in the same genus if $X_1(\ell) \simeq X_2(\ell)$ for every prime ℓ, or equivalently, $T_\ell(X_1) \simeq T_\ell(X_2)$ as A_ℓ-modules for every prime ℓ. From (3.11), $A_\ell = O_{F_\ell}$ holds in all cases except when $p \equiv 1 \pmod 4$ and $\ell = 2$. When $\ell \neq 2$, we have

$$T_\ell(X) \simeq O_{F_\ell}^2 \tag{3.14}$$

for every member $X \in \mathrm{Isog}(\sqrt{p}\,)$.

First suppose that $p \not\equiv 1 \pmod 4$. Then (3.14) holds for $\ell = 2$ as well. It follows that $\mathrm{Isog}(\sqrt{p}\,)$ forms a single genus in this case, which we denote[1] by Λ_1^{un}. Since $\mathrm{End}_{\mathbb{F}_p}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \mathrm{End}_{A_\ell}(T_\ell(X)) \simeq \mathrm{Mat}_2(O_{F_\ell})$ for every ℓ, we see that $\mathrm{End}(X)$ is a maximal order in $\mathrm{End}^0(X) \simeq D$.

Next, suppose that $p \equiv 1 \pmod 4$. By the above discussion, two members of $\mathrm{Isog}(\sqrt{p}\,)$ belong to the same genus if and only if their Tate modules at $\ell = 2$ are isomorphic as A_2-modules. Since $[O_{F_2} : A_2] = 2$, we have three different isomorphism classes of $T_2(X)$ as listed in Table 3.1, and hence three different genera $\Lambda_{16}^{\mathrm{un}}, \Lambda_8^{\mathrm{un}}$ and Λ_1^{un}. Here the subscript i in Λ_i^{un} for $i > 1$ measures the index of $\mathrm{End}_{\mathbb{F}_p}(X) \otimes \mathbb{Z}_2$ in a maximal O_{F_2}-order containing it.

Next, we classify the genera in $\mathrm{PPAV}(\sqrt{p}\,)$, consider the forgetful map

$$\mathrm{PPAV}(\sqrt{p}\,) \to \mathrm{Isog}(\sqrt{p}\,), \qquad (X, \lambda) \mapsto X. \tag{3.15}$$

Recall that two members $(X_i, \lambda_i)_{i=1,2}$ of $\mathrm{PPAV}(\sqrt{p}\,)$ are in the same genus if $(X_1(\ell), \lambda_{1,\ell})$ is isomorphic to $(X_2(\ell), \lambda_{2,\ell})$ for every prime ℓ. Clearly, if $(X_i, \lambda_i)_{i=1,2}$ lie in the same genus in $\mathrm{PPAV}(\sqrt{p}\,)$, then the X_i's lie in the same genus in $\mathrm{Isog}(\sqrt{p}\,)$. If $p \equiv 1 \pmod 4$, we define[2] $\Lambda_i^{\mathrm{pp}} \subseteq \mathrm{PPAV}(\sqrt{p}\,)$ to be the pre-image of Λ_i^{un}

[1] Here the superscript "un" means "unpolarized".
[2] Here the superscript "pp" means "principally polarized".

TABLE 3.1. Three genera in the case $p \equiv 1 \pmod 4$

$T_2(X)$	A_2^2	$A_2 \oplus O_{F_2}$	$(O_{F_2})^2$
genera	$\Lambda_{16}^{\mathrm{un}}$	Λ_8^{un}	Λ_1^{un}
$\mathrm{End}_{\mathbb{F}_p}(X) \otimes \mathbb{Z}_2$	$\mathrm{Mat}_2(A_2)$	$\begin{pmatrix} A_2 & 2O_{F_2} \\ O_{F_2} & O_{F_2} \end{pmatrix}$	$\mathrm{Mat}_2(O_{F_2})$

under (3.15) for $i \in \{1, 8, 16\}$. As before, if $p \not\equiv 1 \pmod 4$, then we define $\Lambda_1^{\mathrm{pp}} = \mathrm{PPAV}(\sqrt{p})$.

Lemma 3.5. *Suppose that $p \equiv 1 \pmod 4$. Then $\Lambda_8^{\mathrm{pp}} = \emptyset$, while neither $\Lambda_{16}^{\mathrm{pp}}$ nor Λ_1^{pp} is empty.*

Proof. If $\lambda : X \to X^\vee$ is a principal polarization, then $\mathrm{End}_{\mathbb{F}_p}(X)$ is stable under the Rosati involution $a \mapsto a' := \lambda^{-1} \circ a^\vee \circ \lambda$. Recall that the Rosati involution coincides with the canonical involution. Meanwhile, it is clear from Table 3.1 that $\mathrm{End}_{\mathbb{F}_p}(X) \otimes \mathbb{Z}_2$ is not stable under the canonical involution for any $X \in \Lambda_8^{\mathrm{un}}$. It follows that $\Lambda_8^{\mathrm{pp}} = \emptyset$.

To show that $\Lambda_{16}^{\mathrm{pp}} \neq \emptyset$, note that (Y, λ_Y) defined in (3.5) lies in $\Lambda_{16}^{\mathrm{pp}}$ because of (3.7). Then one shows that there is an isogeny $Y \to X \in \Lambda_1^{\mathrm{un}}$ along which $2\lambda_Y$ descends to a principal polarization on X. Thus $\Lambda_1^{\mathrm{un}} \neq \emptyset$ as well. $\square$

Lemma 3.6. *For every prime p, Λ_1^{pp} forms a single genus. The same holds for $\Lambda_{16}^{\mathrm{pp}}$ if $p \equiv 1 \pmod 4$.*

Proof. For every member $X \in \Lambda_1^{\mathrm{un}}$ and every prime ℓ, $T_\ell(X)$ is a free O_{F_ℓ}-module of rank 2. Set $T_\ell := O_{F_\ell}^2$. One shows that up to isomorphism, there is a unique alternating $\mathbb{Z}_\ell$-linear perfect pairing

$$e_\ell : T_\ell \times T_\ell \to \mathbb{Z}_\ell \qquad \text{such that} \tag{3.16}$$

$$e_\ell(ax, y) = e_\ell(x, ay) \qquad \forall a \in O_{F_\ell},\ x, y \in T_\ell. \tag{3.17}$$

It follows that Λ_1^{pp} forms a single genus. The proof for $\Lambda_{16}^{\mathrm{pp}}$ can be carried out similarly, except that one replaces $O_{F,\ell}$ by A_ℓ, and makes use of the fact that A is a Gorenstein order [6, Section 37]. $\square$

In summary, we have

$$\mathrm{PPAV}(\sqrt{p}) = \begin{cases} \Lambda_1^{\mathrm{pp}} \cup \Lambda_{16}^{\mathrm{pp}} & \text{if } p \equiv 1 \pmod 4; \\ \Lambda_1^{\mathrm{pp}} & \text{otherwise,} \end{cases} \tag{3.18}$$

where each Λ_i^{pp} forms a single genus.

4. THE CALCULATIONS

We keep the notation and assumptions of the previous section. Our goal is to work out an explicit formula for $|\mathrm{PPAV}(\sqrt{p})|$. Combining Proposition 2.3 with (3.18), one sees that $|\mathrm{PPAV}(\sqrt{p})|$ is either a class number or the sum of two class numbers of the form $|G^1(\mathbb{Q}) \backslash G^1(\mathbb{A}_f)/U_{G^1}(X_0)|$, where G^1 is given in (3.3) and $U_{G^1}(X_0)$ in (3.4)). One standard method of calculating such class numbers is the Selberg trace formula [15, §5], and indeed we take this approach in the case $p \equiv 3 \pmod 4$ and $p \geq 7$. Meanwhile, some analysis on the endomorphism rings reduces the calculation in the case $p \not\equiv 3 \pmod 4$ to that of type numbers. It also sheds light on the $p \equiv 3 \pmod 4$ case from another perspective.

4.1. **The group action on Λ_1^{pp} and Gauss genera.** Let $F_+^\times$ be the group of totally positive elements of $F^\times$, and $O_{F,+}^\times := F_+^\times \cap O_F^\times$. We write $\mathrm{Pic}^+(O_F)$ for the narrow class group of F, which is naturally identifiable with $\widehat{F}^\times/(F_+^\times \widehat{O}_F^\times)$. By [4, Definition 14.29], the Gauss genus group $\mathfrak{g}_F$ is the quotient group $\mathrm{Pic}^+(O_F)/\mathrm{Pic}^+(O_F)^2$, where $\mathrm{Pic}^+(O_F)^2$ denotes the subgroup of $\mathrm{Pic}^+(O_F)$ consisting of square ideal classes. It is well known [4, Theorem 14.34] that $|\mathfrak{g}_F| = 2^{t-1}$, where t is the number of primes that are ramified in $F/\mathbb{Q}$, so in our case

$$|\mathfrak{g}_F| = |\mathrm{Pic}^+(O_F)/\mathrm{Pic}^+(O_F)^2| = \begin{cases} 1 & \text{if } p \not\equiv 3 \pmod 4; \\ 2 & \text{if } p \equiv 3 \pmod 4). \end{cases} \tag{4.1}$$

Fix a member $(X_0, \lambda_0) \in \Lambda_1^{\mathrm{pp}}$ and let $\mathbb{O}_0 = \mathrm{End}_{\mathbb{F}_p}(X_0)$. Since $D = D_{\infty_1,\infty_2}$ splits at all finite places of F, the normalizer $\mathcal{N}(\widehat{\mathbb{O}}_0)$ of $\widehat{\mathbb{O}}$ in $\widehat{D}^\times$ coincides with $\widehat{F}^\times\widehat{\mathbb{O}}_0^\times$. It follows that there is a natural identification $\mathrm{Tp}(D) \simeq D^\times\backslash\widehat{D}^\times/(\widehat{F}^\times\widehat{\mathbb{O}}_0^\times)$. This leads to a commutative diagram as follows.

$$\begin{tikzcd}
\Lambda_1^{\mathrm{pp}} \arrow[r, "\Psi"] \arrow[d, "\simeq"] & \mathrm{Tp}(D) \arrow[r, two heads, "\Theta"] \arrow[d, "\simeq"] & \mathrm{Pic}^+(O_F)/\mathrm{Pic}^+(O_F)^2 \arrow[d, equal] \\
D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}_0^1 \arrow[r] & D^\times\backslash\widehat{D}^\times/(\widehat{F}^\times\widehat{\mathbb{O}}_0^\times) \arrow[r, two heads, "\mathrm{Nr}"] & \widehat{F}^\times/(F_+^\times\widehat{O}_F^\times\widehat{F}^{\times 2})
\end{tikzcd}$$

Here the leftmost vertical arrow is given by Proposition 2.3, and Ψ is defined in (3.9). We define the map $\Theta : \mathrm{Tp}(D) \to \mathfrak{g}_F$ as follows. Recall that any two maximal orders $\mathbb{O}_1$ and $\mathbb{O}_2$ in D are *linked* [20, §I.4], i.e. there exists an O_F-lattice $I \subset D$ such that $\mathbb{O}_1 = \{x \in D | xI \subseteq I\}$, and $\mathbb{O}_2 = \{x \in D | Ix \subseteq I\}$. Given an element $[\![\mathbb{O}]\!] \in \mathrm{Tp}(D)$, we choose an O_F-lattice I via which $\mathbb{O}$ and $\mathbb{O}_0$ are linked. Then $\Theta([\![\mathbb{O}]\!])$ is defined as the element of $\mathfrak{g}_F$ represented by the fractional O_F-ideal $\mathrm{Nr}(I)$. It is easy to check by definition that $\Theta([\![\mathbb{O}]\!])$ does not depend on the choice of $\mathbb{O}$ nor I. Since the reduced norm map Nr is surjective, so is Θ.

Note that the rows of the commutative diagram are *exact*, in the sense that the first horizontal arrow maps surjectively onto the neutral fiber of the second arrow. The elements of the neutral fiber $\mathrm{Tp}_0(D) := \mathrm{img}(\Psi)$ of Θ will be called the conjugacy classes of maximal orders belonging to the *principal Gauss genus*. If $p \not\equiv 3 \pmod 4$, then $\mathrm{Tp}_0(D) = \mathrm{Tp}(D)$ by (4.1), so this notion is more or less vacuous in this case. If $p \equiv 3 \pmod 4$, then $\mathrm{Tp}_0(D)$ is a proper subset of $\mathrm{Tp}(D)$. We obtain the following result:

Lemma 4.1. *If $p \not\equiv 3 \pmod 4$, then every maximal order is realizable as the endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(X)$ for some $(X, \lambda) \in \Lambda_1^{\mathrm{pp}} \subseteq \mathrm{PPAV}(\sqrt{p})$. If $p \equiv 3 \pmod 4$, then a maximal order is realizable as $\mathrm{End}_{\mathbb{F}_p}(X)$ for some $(X, \lambda) \in \mathrm{PPAV}(\sqrt{p})$ if and only if it belongs to the principal Gauss genus.*

If $p \equiv 3 \pmod 4$, then $\mathrm{Tp}_0(D)$ always contains the image of $\mathcal{M} : \mathrm{Tp}(D_{p,\infty}) \to \mathrm{Tp}(D)$ as shown in (3.10).

There is a natural action of $O_{F,+}^\times$ on Λ_1^{pp} as follows:

$$u \cdot (X, \lambda) = (X, \lambda u) \qquad \forall u \in O_{F,+}^\times,\ (X, \lambda) \in \Lambda_1^{\mathrm{pp}}.$$

Since u is invariant under the canonical involution and totally positive, λu is another principal polarization on X. Let $\mathbb{O} = \mathrm{End}_{\mathbb{F}_p}(X)$ and identify it with a maximal order in D. For any $\alpha \in \mathbb{O}^\times$, we have $\alpha^*\lambda = \alpha^\vee\lambda\alpha = \lambda\bar{\alpha}\alpha$. Taking $\alpha = v \in O_F^\times$, we see that $v^*\lambda = \lambda v^2$, so the subgroup $O_F^{\times 2} \subseteq O_{F,+}^\times$ acts trivially on Λ_1^{pp}. It follows that the action of $O_{F,+}^\times$ on Λ_1^{pp} descends to an action of $\mathfrak{u} := O_{F,+}^\times/O_F^{\times 2}$, and Ψ factors through $\mathfrak{u}\backslash\Lambda_1^{\mathrm{pp}}$. Moreover, (X,λ) is fixed by $\mathfrak{u}$ if and only if the reduced norm map $\mathrm{Nr} : \mathbb{O}^\times \to O_{F,+}^\times$ is surjective.

Let $\varepsilon \in O_F^\times$ be the fundamental unit of F. By [1, §11.5] or [5, Corollary 18.4bis], ε is totally positive (i.e. $\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = 1$) if and only if $p \equiv 3 \pmod 4$. Hence $O_{F,+}^\times = \langle\varepsilon\rangle$ if $p \equiv 3 \pmod 4$, and $O_{F,+}^\times = \langle\varepsilon^2\rangle$ otherwise. On the other hand, $O_F^{\times 2} = \langle\varepsilon^2\rangle$ for all p, so we have

$$|\mathfrak{u}| = \begin{cases} 1 & \text{if } p \not\equiv 3 \pmod 4; \\ 2 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{4.2}$$

The action of $\mathfrak{u}$ can be realized adelically on $D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}_0^1$ as follows. Consider the group

$$\Delta := \{(\alpha,\mu) \in D^\times \times \widehat{\mathbb{O}}_0^\times \mid \mathrm{Nr}(\alpha) = \mathrm{Nr}(\mu)\},$$

which contains $\Delta_1 := O_F^\times(D^1 \times \widehat{\mathbb{O}}_0^1)$ as a normal subgroup. Here $O_F^\times$ embeds diagonally into Δ. The reduced norm map $(\alpha,\mu) \mapsto \mathrm{Nr}(\alpha)$ induces an epimorphism $\mathrm{Nr} : \Delta \twoheadrightarrow O_{F,+}^\times$, and hence an isomorphism

$$\Delta/\Delta_1 \simeq \mathfrak{u}. \tag{4.3}$$

The group Δ acts on $\widehat{D}^1$ as follows:

$$(\alpha,\mu)\cdot g = \alpha g \mu^{-1}, \qquad \forall (\alpha,\mu) \in \Delta,\ g \in \widehat{D}^1.$$

Clearly, we have $\Delta_1\backslash\widehat{D}^1 \simeq D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}_0^1$, so $\Delta\backslash\widehat{D}^1$ may be identified with the orbit space of the induced action of $\mathfrak{u}$ on $D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}_0^1$. On the other hand, $\Delta\backslash\widehat{D}^1$ is just the image of the canonical map

$$D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}_0^1 \to D^\times\backslash\widehat{D}^\times/(\widehat{F}^\times\widehat{\mathbb{O}}_0^\times).$$

Lastly, one checks that the action of $\mathfrak{u}$ on $D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}_0^1$ is compatible with that of $\mathfrak{u}$ on Λ_1^{pp} defined earlier. Summarizing, we obtain the following lemma.

Lemma 4.2. *The map Ψ induces a bijection $(\mathfrak{u}\backslash\Lambda_1^{\mathrm{pp}}) \to \mathrm{Tp}_0(D)$ for every prime p. More precisely,*

1. *if $p \not\equiv 3 \pmod 4$, then $\Psi : \Lambda_1^{\mathrm{pp}} \to \mathrm{Tp}(D)$ is bijective;*
2. *if $p \equiv 3 \pmod 4$, then $\Lambda_1^{\mathrm{pp}} \to (\mathfrak{u}\backslash\Lambda_1^{\mathrm{pp}}) \simeq \mathrm{Tp}_0(D)$ is a 2:1 cover ramified over the subset $\{[\![\mathbb{O}]\!] \in \mathrm{Tp}_0(D) \mid \mathrm{Nr}(\mathbb{O}^\times) = O_{F,+}^\times\}$.*

Indeed, if $p \not\equiv 3 \pmod 4$, then $\mathfrak{u}$ is trivial, and $\mathrm{Tp}_0(D) = \mathrm{Tp}(D)$. In particular,

$$|\mathrm{PPAV}(\sqrt{2}\,)| = |\Lambda_1^{\mathrm{pp}}| = |\mathrm{Tp}(D)| = 1 \qquad \text{when} \quad p = 2. \tag{4.4}$$

If $p \equiv 3 \pmod 4$, then $|\mathfrak{u}| = 2$, and a member $(X,\lambda) \in \Lambda_1^{\mathrm{pp}}$ is fixed by $\mathfrak{u}$ if and only if $\mathrm{Nr} : \mathrm{Aut}_{\mathbb{F}_p}(X) \to O_{F,+}^\times$ is surjective. Suppose that $p = 3$ and let $\mathbb{O}_1$ be as in Example 3.4. Since $\mathrm{Nr}(\mathbb{O}_1^\times) = O_{F,+}^\times$, we have

$$|\mathrm{PPAV}(\sqrt{3}\,)| = |\Lambda_1^{\mathrm{pp}}| = |\mathrm{Tp}_0(D)| = 1 \qquad \text{when} \quad p = 3. \tag{4.5}$$

According to Lemma 4.2, we have $|\Lambda_1^{\mathrm{pp}}| = |\mathrm{Tp}(D)|$ when $p \equiv 1 \pmod 4$. Note that $D = D_{\infty_1,\infty_2}$ splits at all finite places of F, and $h(F)$ is odd [5, Corollary 18.4]. From [27, Corollary 3.5], we have

$$|\Lambda_1^{\mathrm{pp}}| = |\mathrm{Tp}(D)| = \frac{h(\mathbb{O}_0)}{h(O_F)}.$$

A similar argument as above also shows that when $p \equiv 1 \pmod 4$,

$$|\Lambda_{16}^{\mathrm{pp}}| = \frac{h(\mathcal{O}_{16})}{h(A)},$$

where $\mathcal{O}_{16} = \mathrm{End}_{\mathbb{F}_p}(X)$ for some $(X,\lambda) \in \Lambda_{16}^{\mathrm{pp}}$, and $A = \mathbb{Z}[\sqrt{p}]$. In particular,

$$|\Lambda_1^{\mathrm{pp}}| = |\Lambda_{16}^{\mathrm{pp}}| = 1 \qquad \text{if } p = 5.$$

Applying the results of [27, §4], we obtain the following proposition.

Proposition 4.3. *Suppose that $p \equiv 1 \pmod 4$ and $p \geq 13$. Then*

$$|\Lambda_1^{\mathrm{pp}}| = \frac{\zeta_F(-1)}{2} + \frac{h(-p)}{8} + \frac{h(-3p)}{6};$$

$$|\Lambda_{16}^{\mathrm{pp}}| = \left(4 - \left(\frac{2}{p}\right)\right)\zeta_F(-1) + \frac{h(-p)}{4} + \left(2 + \left(\frac{2}{p}\right)\right)\frac{h(-3p)}{6}.$$

Therefore, we have

$$\begin{aligned}|\mathrm{PPAV}(\sqrt{p})| &= |\Lambda_1^{\mathrm{pp}}| + |\Lambda_{16}^{\mathrm{pp}}| \\ &= \left(9 - 2\left(\frac{2}{p}\right)\right)\frac{\zeta_F(-1)}{2} + \frac{3h(-p)}{8} + \left(3 + \left(\frac{2}{p}\right)\right)\frac{h(-3p)}{6}.\end{aligned}$$

4.2. **The Selberg trace formula.** Assume that $p \equiv 3 \pmod 4$ and $p \geq 7$. In this case, $\mathrm{Tp}_0(D)$ is a proper subset of $\mathrm{Tp}(D)$. Pick $[\![\mathbb{O}]\!] \in \mathrm{Tp}_0(D)$ so that there exists $(X,\lambda) \in \Lambda_1^{\mathrm{pp}}$ with $\mathbb{O} \simeq \mathrm{End}_{\mathbb{F}_p}(X)$. For example, we may take $\mathbb{O}$ in the image of $\mathcal{M} : \mathrm{Tp}(D_{p,\infty}) \to \mathrm{Tp}(D)$ as in (3.8). Combining Proposition 2.3 with (3.18), we see that

$$|\mathrm{PPAV}(\sqrt{p})| = |\Lambda_1^{\mathrm{pp}}| = |D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}^1|. \tag{4.6}$$

Proposition 4.4. *Suppose that $p \equiv 3 \pmod 4$ and $p \geq 7$. Let $\mathbb{O}$ be a maximal order in $D = D_{\infty_1,\infty_2}$. Then we have*

$$|D^1\backslash\widehat{D}^1/\widehat{\mathbb{O}}^1| = \begin{cases} \dfrac{\zeta_F(-1)}{2} + \left(11 - 3\left(\dfrac{2}{p}\right)\right)\dfrac{h(-p)}{8} + \dfrac{h(-3p)}{6} & \text{if } [\![\mathbb{O}]\!] \in \mathrm{Tp}_0(D); \\[2ex] \dfrac{\zeta_F(-1)}{2} + \left(3 - 3\left(\dfrac{2}{p}\right)\right)\dfrac{h(-p)}{8} + \dfrac{h(-3p)}{6} & \text{otherwise.}\end{cases}$$

The main tool for such calculations is the *Selberg trace formula* (of co-compact type). See [15, §5] for a brief introduction.

For simplicity, write $\mathcal{G} = \widehat{D}^1$, $U = \widehat{\mathbb{O}}^1$ and $\Gamma = D^1$. Then $\mathcal{G}$ is a locally compact unimodular group, and U is an open compact subgroup of $\mathcal{G}$. We normalize the Haar measure dx on $\mathcal{G}$ such that $\mathrm{Vol}(U) = \int_U dx = 1$. Let $\mathcal{H}$ be a closed subgroup of $\mathcal{G}$ and dh a Haar measure on $\mathcal{H}$. There is a unique right $\mathcal{G}$-invariant measure $\frac{dx}{dh}$ on $\mathcal{H}\backslash\mathcal{G}$ characterized by the following integration formula:

$$\int_{\mathcal{G}} f dx = \int_{\mathcal{H}\backslash\mathcal{G}}\int_{\mathcal{H}} f(hg)dh\frac{dx}{dh}, \qquad \forall f \in C_c^\infty(\mathcal{G}).$$

Here $C_c^\infty(\mathcal{G})$ denotes the space of locally constant $\mathbb{C}$-valued functions on $\mathcal{G}$ with compact support.

By [20, §III.1], Γ is discrete cocompact in $\mathcal{G}$. Given $\gamma \in \Gamma$, we write $\{\gamma\}$ for the conjugacy class of γ in Γ, and $\Gamma/\!\sim$ for the set of all conjugacy classes of Γ. Let $\mathbb{1}_U \in C_c^\infty(\mathcal{G})$ be the characteristic function of U. Applying the Selberg trace formula to $\mathbb{1}_U$, we obtain

$$|\Gamma\backslash\mathcal{G}/U| = \sum_{\{\gamma\}\in\Gamma/\sim} \mathrm{Vol}(\Gamma_\gamma\backslash\mathcal{G}_\gamma)\int_{\mathcal{G}_\gamma\backslash\mathcal{G}} \mathbb{1}_U(x^{-1}\gamma x)\frac{dx}{dx_\gamma}, \tag{4.7}$$

where Γ_γ (resp. $\mathcal{G}_\gamma$) denotes the centralizer of γ in Γ (resp. $\mathcal{G}$), and dx_γ is a Haar measure on $\mathcal{G}_\gamma$.

Note that γ is central if and only if $\gamma = \pm 1$, in which case the summand in (4.7) corresponding to $\{\gamma\}$ reduces to $\mathrm{Vol}(\Gamma\backslash\mathcal{G})$. By a result of Vignéras [19, Proposition 2], we have

$$\mathrm{Vol}(\Gamma\backslash\mathcal{G}) = \mathrm{Vol}(D^1\backslash\widehat{D}^1) = \frac{1}{4}\zeta_F(-1). \tag{4.8}$$

There are two central elements, which explains the term $\frac{1}{2}\zeta_F(-1)$ in the formulas of Proposition 4.4.

Assume that γ is non-central for the rest of this section. The centralizer of γ in D coincides with $K := F(\gamma)$. Since D is totally definite, K is a CM-extension of F. Using Weil restriction of scalars, we define two algebraic tori over $\mathbb{Q}$:

$$T^K := \mathrm{Res}_{K/\mathbb{Q}}\,\mathbb{G}_{m,K}, \qquad T^F := \mathrm{Res}_{F/\mathbb{Q}}\,\mathbb{G}_{m,F}.$$

The norm map $\mathrm{N}_{K/F}$ induces a homomorphism $T^K \to T^F$, whose kernel is denoted by T^1. The centralizer of γ in the algebraic group G^1 in (3.3) is isomorphic to T^1, so we have

$$\mathcal{G}_\gamma = \widehat{K}^1 := T^1(\mathbb{A}_f) \quad \text{and} \quad \Gamma_\gamma = K^1 := T^1(\mathbb{Q}).$$

Normalize the Haar measure on $\widehat{K}^1$ so that the maximal open compact subgroup $\widehat{O}_K^1$ has volume 1. By [17, Theorem 3], which is attributed to Takashi Ono, we have

$$\mathrm{Vol}(\Gamma_\gamma\backslash G_\gamma) = \mathrm{Vol}(K^1\backslash\widehat{K}^1) = \frac{h(K)}{2^{t-1}|\boldsymbol{\mu}(K)|Q_{K/F}h(F)} \tag{4.9}$$

where t, $\boldsymbol{\mu}(K)$ and $Q_{K/F}$ are as follows:

- t is the number of finite primes ramified in K/F;
- $\boldsymbol{\mu}(K)$ is the group of roots of unity in K;
- $Q_{K/F}$ is the Hasse unit index $[O_K^\times : O_F^\times\boldsymbol{\mu}(K)]$, which takes value either 1 or 2 by [21, Theorem 4.12].

Lastly, note that the integral $\int_{\mathcal{G}_\gamma\backslash\mathcal{G}} \mathbb{1}_U(x^{-1}\gamma x)\frac{dx}{dx_\gamma} = 0$ unless γ is a root of unity. Since $p \geq 7$ and $[K:\mathbb{Q}] = 4$, the multiplicative order of $\gamma \in D^1$ is $3, 4$ or 6. To apply (4.9), we assemble the relevant data in the following table (see [11, §7]):

$\mathrm{ord}(\gamma)$	4	3 or 6
$K = F(\gamma)$	$F(\sqrt{-1}\,)$	$F(\sqrt{-3}\,)$
$h(K)/h(F)$	$h(-p)$	$h(-3p)/2$
t	0	$\frac{3}{2}+\frac{1}{2}\left(\frac{p}{3}\right)$
$\lvert\boldsymbol{\mu}(K)\rvert$	4	6
$Q_{K/F}$	2	1

This somewhat explains the $h(-p)$ and $h(-3p)$ terms in the fomulas of Proposition 4.4. However, there is a key subtlety that cannot be ignored. Indeed, for any two maximal orders $\mathbb{O}$ and $\mathbb{O}'$ belonging to distinct Guass genus (i.e. $[\![\mathbb{O}]\!] \in \mathrm{Tp}_0(D)$ and $[\![\mathbb{O}']\!] \notin \mathrm{Tp}_0(D)$), the groups $\widehat{\mathbb{O}}^1$ and $\widehat{\mathbb{O}}'^1$ are isomorphic. So there is certain *global* obstruction that causes the class numbers to be distinct as in Proposition 4.4. Alas, such arithmetic intricacy goes beyond this simple note, and we refer to our upcoming paper [25] for details.

Acknowledgment

J. Xue is partially supported by the Natural Science Foundation of China grant #11601395. He would like to express his gratitude to Professor Tomoyoshi Ibukiyama, Professor Takao Komastu and Professor Satoshi Wakatsuki for their assistance and hospitality during his visit to Research Institute for Mathematical Sciences (RIMS), Kyoto University. C.-F. Yu is partially supported by the MoST grants 104-2115-M-001-001MY3 and 107-2115-M-001-001-MY2.

References

[1] Şaban Alaca and Kenneth S. Williams. *Introductory algebraic number theory*. Cambridge University Press, Cambridge, 2004.

[2] 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.

[3] Ching-Li Chai. Siegel moduli schemes and their compactifications over **C**. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 231–251. Springer, New York, 1986.

[4] Harvey Cohn. *A classical invitation to algebraic numbers and class fields*. Springer-Verlag, New York-Heidelberg, 1978. With two appendices by Olga Taussky: "Artin's 1932 Göttingen lectures on class field theory" and "Connections between algebraic number theory and integral matrices", Universitext.

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

[6] 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.

[7] Claus Diem and Niko Naumann. On the structure of Weil restrictions of abelian varieties. *J. Ramanujan Math. Soc.*, 18(2):153–174, 2003.

[8] Everett W. Howe, Daniel Maisner, Enric Nart, and Christophe Ritzenthaler. Principally polarizable isogeny classes of abelian surfaces over finite fields. *Math. Res. Lett.*, 15(1):121–127, 2008.

[9] Robert E. Kottwitz. Shimura varieties and λ-adic representations. In *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988)*, volume 10 of *Perspect. Math.*, pages 161–209. Academic Press, Boston, MA, 1990.

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

[11] Qun Li, Jiangwei Xue, and Chia-Fu Yu. Unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields. *ArXiv e-prints*, July 2018, `arXiv:1807.04736`.

[12] Michael Lipnowski and Jacob Tsimerman. How large is $A_g(\mathbb{F}_q)$? *Duke Math. J.*, 167(18):3403–3453, 2018.

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

[14] Frans Oort. Newton polygons and formal groups: conjectures by Manin and Grothendieck. *Ann. of Math. (2)*, 152(1):183–206, 2000.

[15] Arnold K. Pizer. Type numbers of Eichler orders. *J. Reine Angew. Math.*, 264:76–102, 1973.

[16] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[17] Ryuji Sasaki. Some remarks to Ono's theorem on a generalization of Gauss' genus theory. *Nagoya Math. J.*, 111:131–142, 1988.

[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. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287:257–277, 1976.

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

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

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

[23] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Supersingular abelian surfaces and Eichler's class number formula. *ArXiv e-prints*, April 2014, `arXiv:1404.2978`. to appear in The Asian Journal of Mathematics.

[24] 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.

[25] Jiangwei Xue and Chia-Fu Yu. On principally polarized superspecial abelian surfaces over finite fields. In preparation.

[26] Jiangwei Xue and Chia-Fu Yu. Counting abelian varieties over finite fields. *ArXiv e-prints*, January 2018, `arXiv:1801.00229`.

[27] Jiangwei Xue and Chia-Fu Yu. On superspecial abelian surfaces and type numbers of totally definite quaternion algebras. *ArXiv e-prints*, September 2018, `arXiv:1809.04316`.

[28] Chia-Fu Yu. On reduction of Hilbert-Blumenthal varieties. *Ann. Inst. Fourier (Grenoble)*, 53(7):2105–2154, 2003.

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

[30] 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.

[31] Ju. G. Zarhin. Endomorphisms of abelian varieties and points of finite order in characteristic P. *Mat. Zametki*, 21(6):737–744, 1977.

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

Email address: `xue_j@whu.edu.cn`

(Yu) Institute of Mathematics, Academia Sinica, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN.

(Yu) National Center for Theoretical Sciences, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN.

Email address: `chiafu@math.sinica.edu.tw`