RIMS Kôkyûroku Bessatsu
B90 (2022), 39–57

Polarized superspecial simple abelian surfaces with real Weil numbers: a survey

By

Jiangwei Xue* and Chia-Fu Yu**

Abstract

In this survey article we describe recent results of explicit formulae for (a) the number of superspecial abelian surfaces over $\mathbb{F}_q$ with real Frobenius endomorphism $\sqrt{q}$ equipped with a polarization module; (b) the type number of each genus of these polarized superspecial abelian surfaces; and (c) the refined class and type numbers of such abelian surfaces with a given automorphism group. These formulae suggest an interesting connection with arithmetic genera of Hilbert modular surfaces.

§ 1. Introduction

The aim of this article is to report recent progress on explicit formulae for variant counting problems for polarized superspecial abelian surfaces in the isogeny class corresponding to a real Weil number. Throughout this article p denotes a prime number. Let $\mathbb{F}_q$ denote the finite field of $q = p^n$ elements, and let π be a Weil q-number. Let $X_\pi/\mathbb{F}_q$ be a simple abelian variety attached to the Galois conjugacy class of the Weil q-number π by the Honda-Tate theorem. The abelian variety X_π is unique up to $\mathbb{F}_q$-isogeny. We denote by

$$\mathrm{Isog}(\pi) := \{\mathbb{F}_q\text{-isom. classes of abelian varieties } X \text{ that are } \mathbb{F}_q\text{-isogenous to } X_\pi\}.$$

Received January 1, 2021. Revised April 7, 2021.
2020 Mathematics Subject Classification(s): 11R52, 11G10
Key Words: *polarized superspecial abelian surfaces, type numbers, totally definite quaternion algebras, refined class numbers.*

*Collaborative Innovation Centre of Mathematics, School of Mathematics and Statistics, Wuhan University, Luojiashan, Wuhan, Hubei, 430072, P.R. China.
e-mail: xue_j@whu.edu.cn
**Institute of Mathematics, Academia Sinica and NCTS, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan.
e-mail: chiafu@math.sinica.edu.tw

Explicit calculation of the size of $\mathrm{Isog}(\pi)$ is an interesting problem; though some special cases are known, many of them are still open. This challenging problem compels us to explore various arithmetic techniques and methods. The problem was first studied by Deuring for elliptic curves and was extended by Waterhouse for abelian varieties. However, explicit formulae for the number of abelian surfaces over $\mathbb{F}_q$ in a (not necessarily simple) isogeny class were only known quite recently. The cases of superspecial abelian surfaces are determined in the works [20, 21, 22, 23] of Tse-Chung Yang and the present authors.

It is also interesting to count abelian varieties equipped with a polarization within a fixed $\mathbb{F}_q$-isogeny class. Problems in this direction are studied by Howe, Ritzenthaler, Achter, Marseglia, and many others; see [1, 7, 9, 10, 13, 24]. Let

$$\mathrm{PPAV}(\pi) := \{\text{prin. pol. abelian varieties } (X,\lambda) \text{ over } \mathbb{F}_q \text{ with } [X]\in \mathrm{Isog}(\pi)\}/\simeq_{/\mathbb{F}_q}.$$

Let $D_\pi := \mathrm{End}^0(X_\pi)$ be the endomorphism algebra of X_π over $\mathbb{F}_q$. Put

$$\begin{aligned}\mathrm{Tp}(\pi) &:= \{\mathrm{End}(X)\,|\,[X]\in \mathrm{Isog}(\pi)\,\}/\simeq \ \ (\text{conjugate by } D_\pi^\times),\\ \mathrm{Tp}^{\mathrm{pp}}(\pi) &:= \{\mathrm{End}(X)\,|\,[X,\lambda]\in \mathrm{PPAV}(\pi)\,\}/\simeq \ \ (\text{conjugate by } D_\pi^\times).\end{aligned}$$

Set

$$\begin{aligned} h(\pi) &:= |\mathrm{Isog}(\pi)|, & h^{\mathrm{pp}}(\pi) &:= |\mathrm{PPAV}(\pi)|,\\ t(\pi) &:= |\mathrm{Tp}(\pi)|, & t^{\mathrm{pp}}(\pi) &:= |\mathrm{Tp}^{\mathrm{pp}}(\pi)|.\end{aligned}$$

We also study refined class numbers with a fixed automorphism group. For any finite group G, let

$$h^{\mathrm{pp}}(\pi, G) := \#\{[X,\lambda]\in \mathrm{PPAV}(\pi)\mid \mathrm{Aut}(X,\lambda)\simeq G\}.$$

If X_π is supersingular, we put

$$\mathrm{Sp}(\pi) := \{[X]\in \mathrm{Isog}(\pi)\,|\, X \text{ is superspecial}\,\},$$

$$\mathrm{PPSp}(\pi) := \{[X,\lambda]\in \mathrm{PPAV}(\pi)\,|\, X \text{ is superspecial}\,\}.$$

In the following, we let π be a real Weil q-number, that is, $\pi = \pm\sqrt{q}$. Then

$$D_\pi \simeq \begin{cases} D_{p,\infty} & \text{if } n \text{ is even},\\ D_{\infty_1,\infty_2} & \text{if } n \text{ is odd},\end{cases}$$

where $D_{p,\infty}$ is the definite quaternion $\mathbb{Q}$-algebra ramified exactly at $\{p,\infty\}$, and D_{∞_1,∞_2} is the definite quaternion F-algebra ramified exactly at the two real places $\{\infty_1,\infty_2\}$ of $F=\mathbb{Q}(\sqrt{p}\,)$.

When $\pi = \pm\sqrt{q}$ with n even, the classical result of Deuring establishes a bijection between the set $\mathrm{Isog}(\pi)$ and the set $\mathrm{Cl}(D_{p,\infty})$ of ideal classes of a maximal order in $D_{p,\infty}$. The class number h of $D_{p,\infty}$ is well known due to Eichler [5] (Deuring and Igusa gave different proofs of this result), and is given by

$$h = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right), \tag{1.1}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. Under the correspondence $\mathrm{Isog}(\pi) \simeq \mathrm{Cl}(D_{p,\infty})$, the type number t of $D_{p,\infty}$ is equal to the number of non-isomorphic endomorphism rings of members $[E]$ in $\mathrm{Isog}(\pi)$. An explicit type formula is also well known due to Deuring [4], which is given by

$$t = \frac{p-1}{24} + \frac{1}{6}\left(1 - \left(\frac{-3}{p}\right)\right) + \begin{cases} h(-p)/4 & \text{if } p \equiv 1 \pmod 4, \\ 1/4 + h(-p)/2 & \text{if } p \equiv 7 \pmod 8, \\ 1/4 + h(-p) & \text{if } p \equiv 3 \pmod 8, \end{cases} \tag{1.2}$$

for $p > 3$, and $t = 1$ for $p = 2, 3$. Here for any square-free integer $d \in \mathbb{Z}$, we write $h(d)$ for the class number of $\mathbb{Q}(\sqrt{d}\,)$.

For $p = 2, 3$, one has $h = 1$ and the unique elliptic curve $[E] \in \mathrm{Isog}(\pi)$ has automorphism group

$$\mathrm{Aut}(E) \simeq \begin{cases} \mathrm{SL}_2(\mathbb{F}_3) \simeq E_{24} & \text{for } p = 2; \\ C_3 \rtimes C_4 \simeq Q_{12} & \text{for } p = 3. \end{cases} \tag{1.3}$$

Here C_n is the cyclic group of order n, E_{24} is the binary tetrahedral group, and Q_{12} is the dicyclic group of order 12. If $p \geq 5$, then for any $[E] \in \mathrm{Isog}(\pi)$, $\mathrm{Aut}(E) \in \{C_2, C_4, C_6\}$. For $p \geq 5$, we have

$$h(\pi, C_2) = \frac{p-1}{12} - \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) - \frac{1}{6}\left(1 - \left(\frac{-3}{p}\right)\right), \tag{1.4}$$

$$h(\pi, C_4) = \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right), \quad h(\pi, C_6) = \frac{1}{2}\left(1 - \left(\frac{-3}{p}\right)\right), \tag{1.5}$$

where $h(\pi, G)$ denotes the number of supersingular elliptic curves $[E] \in \mathrm{Isog}(\pi)$ such that $\mathrm{Aut}(E) \simeq G$. The aim of [26] and some earlier works of the authors is to generalize (1.2)-(1.5) from supersingular elliptic curves to polarized simple superspecial abelian surfaces with Weil q-number $\sqrt{q}$ for an odd power q of p.

§ 2. Explicit formulae for superspecial abelian surfaces

Now let q be an odd power of p, and let $\mathrm{Sp}(\sqrt{q}\,)$ be the set of isomorphism classes of superspecial abelian surfaces over $\mathbb{F}_q$ in the isogeny class corresponding to the Weil numbers $\pm\sqrt{q}$. As a generalization of (1.1), we have the following explicit formula for $|\operatorname{Sp}(\sqrt{q})|$ (see [22, Theorem 1.2], see also [21, Theorem 1.3]).

Theorem 2.1. *Let $F = \mathbb{Q}(\sqrt{p})$, and O_F be its ring of integers.*
(1) *The cardinality of $\operatorname{Sp}(\sqrt{q})$ depends only on p, and is denoted by $H(p)$.*
(2) *We have $H(p) = 1, 2, 3$ for $p = 2, 3, 5$, respectively.*
(3) *For $p > 5$ and $p \equiv 3 \pmod 4$, one has*

$$H(p) = h(F)\left[\frac{\zeta_F(-1)}{2} + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-2p)}{4} + \frac{h(-3p)}{6}\right],$$

where $h(F)$ is the class number of F and $\zeta_F(s)$ is the Dedekind zeta function of F.
(4) *For $p > 5$ and $p \equiv 1 \pmod 4$, one has*

$$H(p) = \begin{cases} h(F)\left[8\zeta_F(-1) + \frac{1}{2}h(-p) + \frac{2}{3}h(-3p)\right] & \text{for } p \equiv 1 \pmod 8; \\ h(F)\left[\left(\frac{45+\varpi}{2\varpi}\right)\zeta_F(-1) + \left(\frac{9+\varpi}{8\varpi}\right)h(-p) + \frac{2}{3}h(-3p)\right] & \text{for } p \equiv 5 \pmod 8; \end{cases}$$

where $\varpi := [O_F^\times : A^\times] \in \{1, 3\}$ and $A := \mathbb{Z}[\sqrt{p}]$ is the suborder of index 2 in O_F.

Let $\mathcal{T}(\operatorname{Sp}(\sqrt{q}))$ denote the set of isomorphism classes of endomorphism rings of abelian surfaces in $\operatorname{Sp}(\sqrt{q})$. The cardinality of $\mathcal{T}(\operatorname{Sp}(\sqrt{q}))$ again depends only on the prime p ([21, Theorem 1.3]), and is denoted by $T(p)$. We have the following explicit formula for $T(p)$ [27, Theorem 1.2], which generalizes (1.2).

Theorem 2.2. *Let $F = \mathbb{Q}(\sqrt{p})$ and $T(p) := |\mathcal{T}(\operatorname{Sp}(\sqrt{q}))|$.*
(1) *We have $T(p) = 1, 2, 3$ for $p = 2, 3, 5$, respectively.*
(2) *For $p \equiv 3 \pmod 4$ and $p \geq 7$, we have*

$$T(p) = \frac{\zeta_F(-1)}{2} + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-2p)}{4} + \frac{h(-3p)}{6}. \tag{2.1}$$

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

$$T(p) = 8\zeta_F(-1) + \frac{h(-p)}{2} + \frac{2h(-3p)}{3}. \tag{2.2}$$

It follows from Theorems 2.1 and 2.2 that $H(p) = T(p)h(F)$ except for the case where $p \equiv 5 \pmod 8$ and $\varpi = 1$. When $p \equiv 3 \pmod 4$, we actually prove this result first and use it to get formula (2.1). For the case where $p \equiv 1 \pmod 4$, we explain how this coincidence arises in part (1) of Remark 4.3 of [27].

For refined class numbers we restrict ourselves to superspecial abelian surfaces whose endomorphism rings are *maximal* orders.

Let $D = D_{\infty_1,\infty_2}$ be the totally definite quaternion F-algebra ramified only at the two infinite places of F. Fix a maximal O_F-order $\mathbb{O}$ in D. In this case, there is a natural bijection (see [19, Theorem 6.2] and [22, Theorem 6.1.2])

$$\mathrm{Cl}(\mathbb{O}) \simeq \{[X] \in \mathrm{Sp}(\pi) \mid O_F \subset \mathrm{End}(X)\}.$$

For any member $[X] \in \mathrm{Sp}(\pi)$, the reduced automorphism group is defined by $\mathrm{RAut}(X) := \mathrm{Aut}(X)/Z^\times$, where $Z := \mathrm{End}(X) \cap F$. For any finite group G, put

$$h(G) := \#\{[X] \in \mathrm{Sp}(\sqrt{q}\,) \mid O_F \subset \mathrm{End}(X), \mathrm{RAut}(X) \simeq G\}.$$

$$t(G) := \#\{\,\mathrm{End}(X) \mid [X] \in \mathrm{Sp}(\sqrt{q}\,), O_F \subset \mathrm{End}(X), \mathrm{RAut}(X) \simeq G\}/\simeq .$$

The number $t(G)$ is actually the number of $D^\times$-conjugacy classes of maximal O_F-orders $\mathcal{O} \subset D$ such that $\mathcal{O}^\times/O_F^\times \simeq G$, which is the refined type number of D with respect to G.

We have the class-type number relation [27]

$$h(G) = h(F) \cdot t(G), \quad \forall\, G. \tag{2.3}$$

Thus, knowing $t(G)$ amounts to knowing $h(G)$. For any $n \ge 1$, denote by D_n the dihedral group of order $2n$.

Lemma 2.3. *We have*

- $p = 2$, $h(\mathbb{O}) = 1$ *and* $h(S_4) = 1$.
- $p = 3$, $h(\mathbb{O}) = 2$ *and* $h(S_4) = h(D_{12}) = 1$.
- $p = 5$, $h(\mathbb{O}) = 1$ *and* $h(A_5) = 1$.

Theorem 2.4. *Assume $p \ge 7$.*
(1) (Hashimoto [8]) *For $p \equiv 1 \mod 4$, we have*

$$\begin{aligned}
t(C_1) &= \frac{\zeta_F(-1)}{2} - \frac{h(-p)}{8} - \frac{h(-3p)}{12} - \frac{1}{4}\left(\frac{3}{p}\right) - \frac{1}{4}\left(\frac{2}{p}\right) + \frac{1}{2},\\
t(C_2) &= \frac{h(-p)}{4} + \frac{1}{2}\left(\frac{3}{p}\right) + \frac{1}{4}\left(\frac{2}{p}\right) - \frac{3}{4},\\
t(C_3) &= \frac{h(-3p)}{4} + \frac{1}{4}\left(\frac{3}{p}\right) + \frac{1}{2}\left(\frac{2}{p}\right) - \frac{3}{4},\\
t(D_3) &= \frac{1}{2}\left(1 - \left(\frac{3}{p}\right)\right), \quad t(A_4) = \frac{1}{2}\left(1 - \left(\frac{2}{p}\right)\right),
\end{aligned}$$

and $t(G) = 0$ for any group G not in the above list.

(2) (Li-Xue-Yu [12]) *For* $p \equiv 3 \mod 4$*, we have*

$$t(C_1) = \frac{\zeta_F(-1)}{2} + \left(-7 + 3\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} - \frac{h(-2p)}{4} - \frac{h(-3p)}{12} + \frac{3}{2},$$
$$t(C_2) = \left(2 - \left(\frac{2}{p}\right)\right)\frac{h(-p)}{2} + \frac{h(-2p)}{2} - \frac{5}{2},$$
$$t(C_3) = \frac{h(-3p)}{4} - 1, \quad t(C_4) = \left(3 - \left(\frac{2}{p}\right)\right)\frac{h(-p)}{2} - 1,$$
$$t(D_3) = 1, \quad t(D_4) = 1, \quad t(S_4) = 1,$$

and $t(G) = 0$ *for any group* G *not listed above.*

By Theorem 2.4, there exists a supersingular abelian surface X over $\mathbb{F}_p$ with *non-abelian* reduced automorphism group $\mathrm{RAut}(X)$ if and only if $p \not\equiv 1 \pmod{24}$. Note that $p \equiv 3 \pmod 4$ implies that $p \not\equiv 1 \pmod{24}$.

§ 3. Explicit formulae for polarized superspecial abelian surfaces

In this section we consider superspecial abelian surfaces equipped with a polarization. For simplicity and without loss of generality, we may assume $\pi = \sqrt{p}$, instead of $\sqrt{q}$ for an odd power q of p. Observe that the set $\mathrm{PPSp}(\sqrt{q})$ of isomorphism classes of principally polarized *superspecial* abelian surfaces over $\mathbb{F}_q$ with Frobeninus endomorphism $\pi = \pm\sqrt{q}$ is naturally in bijection with the set of $\mathrm{PPAV}(\sqrt{p})$ of those of principally polarized *supersingular* abelian surfaces over $\mathbb{F}_p$ with $\pi = \pm\sqrt{p}$. Our aim is to compute explicit formulae for $h^{\mathrm{pp}}(\sqrt{p})$, $t^{\mathrm{pp}}(\sqrt{p})$, and refined class numbers $h^{\mathrm{pp}}(\sqrt{p}, G)$. One can also consider an explicit formula for $t^{\mathrm{pp}}(\sqrt{p}, G)$, but this can be deduced from the formula for $t(\sqrt{p}, G)$ and is skipped for simplicity. The followings are new results proved in [26].

Theorem 3.1.
(1) $h^{\mathrm{pp}}(\sqrt{p}) = 1, 1, 2$ *for* $p = 2, 3, 5$*, respectively.*
(2) *For* $p \geq 13$ *and* $p \equiv 1 \pmod 4$*,*

$$h^{\mathrm{pp}}(\sqrt{p}) = \left(9 - 2\left(\frac{2}{p}\right)\right)\frac{\zeta_F(-1)}{2} + \frac{3h(-p)}{8} + \left(3 + \left(\frac{2}{p}\right)\right)\frac{h(-3p)}{6}. \tag{3.1}$$

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

$$h^{\mathrm{pp}}(\sqrt{p}) = \frac{\zeta_F(-1)}{2} + \left(11 - 3\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-3p)}{6}. \tag{3.2}$$

Theorem 3.2. *The type number* $t^{\mathrm{pp}}(\sqrt{p})$ *of* $\mathrm{PPAV}(\sqrt{p})$ *is given as follows:*

(1) $t^{\mathrm{pp}}(\sqrt{p}\,) = 1, 1, 2$ *for* $p = 2, 3, 5,$ *respectively.*

(2) *If* $p \equiv 1 \pmod 4$ *and* $p \geq 13$, *then*

$$t^{\mathrm{pp}}(\sqrt{p}\,) = 8\zeta_F(-1) + \frac{h(-p)}{2} + \frac{2h(-3p)}{3}. \tag{3.3}$$

(3) *If* $p \equiv 3 \pmod 4$ *and* $p \geq 7$, *then*

$$t^{\mathrm{pp}}(\sqrt{p}\,) = \frac{\zeta_F(-1)}{4} + \left(17 - \left(\frac{2}{p}\right)\right)\frac{h(-p)}{16} + \frac{h(-2p)}{8} + \frac{h(-3p)}{12}. \tag{3.4}$$

Recall that for each finite group G,

$$h^{\mathrm{pp}}(\sqrt{p}\,, G) := \#\{[X, \lambda] \in \mathrm{PPAV}(\sqrt{p}\,) : \mathrm{Aut}(X, \lambda) \simeq G\}.$$

For $m \geq 2$, let

$$Q_{4m} := \langle s, t \,|\, s^{2m}, t^2 = s^m, tst^{-1} = s^{-1}\rangle,$$

and call it the dicyclic group of order $4m$. When $m = 2$, $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8.

For $p = 2, 3$, $\mathrm{PPAV}(\sqrt{p}\,) = \{[X, \lambda]\}$ consists of one member, and

$$\mathrm{Aut}(X, \lambda) \simeq \begin{cases} E_{48} & \text{for } p = 2, \\ Q_{24} & \text{for } p = 3, \end{cases}$$

where E_{48} denotes the binary octahedral group. For $p = 5$, $\mathrm{PPAV}(\sqrt{p}\,) = \{[X_1, \lambda_1], [X_{16}, \lambda_{16}]\}$ consists of two members, where $\mathrm{End}(X_1)$ is a maximal order and $\mathrm{End}(X_{16})$ is an order of index 16 in any maximal order containing it. Moreover,

$$\mathrm{Aut}(X_1, \lambda_1) \simeq E_{120} \simeq \mathrm{SL}_2(\mathbb{F}_5), \quad E_{120}/\{\pm 1\} \simeq A_5, \quad \text{and} \quad \mathrm{Aut}(X_{16}, \lambda_{16}) \simeq Q_{12}.$$

The group E_{120} is generally called the binary icosahedral group.

For $p \geq 7$, if $G = \mathrm{Aut}(X, \lambda)$ for some $(X, \lambda) \in \mathrm{PPAV}(\sqrt{p}\,)$, then

$$\begin{aligned} &G \in \{C_2, C_4, C_6, Q_8, Q_{12}, E_{24}\}, \quad \text{and} \\ &G \in \{C_2, C_4, C_6, Q_{12}, E_{24}\}, \quad \text{if } p \equiv 1 \pmod 4. \end{aligned}$$

We have the following explicit formulae for refined class numbers $h^{\mathrm{pp}}(G)$, where we write $h^{\mathrm{pp}}(G)$ for $h^{\mathrm{pp}}(\sqrt{p}\,, G)$.

Theorem 3.3. *Let* $p \geq 7$ *be a prime.*

(1) *If* $p \equiv 1 \pmod 4$, *then*

$$\begin{aligned}
h^{\mathrm{pp}}(C_2) &= \left(9 - 2\left(\frac{2}{p}\right)\right)\frac{\zeta_F(-1)}{2} - \frac{3h(-p)}{8} - \left(3 + \left(\frac{2}{p}\right)\right)\frac{h(-3p)}{12} \\
&\quad - \frac{1}{4}\left(\frac{2}{p}\right) - \frac{1}{2}\left(\frac{p}{3}\right) + \frac{3}{4}, \\
h^{\mathrm{pp}}(C_4) &= \frac{3h(-p)}{4} + \frac{1}{4}\left(\frac{2}{p}\right) + \left(\frac{p}{3}\right) - \frac{5}{4}, \\
h^{\mathrm{pp}}(C_6) &= \frac{1}{4}\left(3 + \left(\frac{2}{p}\right)\right)h(-3p) + \frac{1}{2}\left(\frac{2}{p}\right) + \frac{1}{2}\left(\frac{p}{3}\right) - 1, \\
h^{\mathrm{pp}}(Q_{12}) &= 1 - \left(\frac{p}{3}\right), \quad h^{\mathrm{pp}}(E_{24}) = \frac{1}{2}\left(1 - \left(\frac{2}{p}\right)\right).
\end{aligned}$$

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

$$\begin{aligned}
h^{\mathrm{pp}}(C_2) &= \frac{\zeta_F(-1)}{2} - \left(11 - 3\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} - \frac{h(-3p)}{12} + \frac{1}{4}\left(\frac{2}{p}\right) - \frac{1}{2}\left(\frac{p}{3}\right) + \frac{5}{4}, \\
h^{\mathrm{pp}}(C_4) &= \left(\frac{11}{4} - \frac{3}{4}\left(\frac{2}{p}\right)\right)(h(-p) - 1) - \left(\frac{2}{p}\right) + \left(\frac{p}{3}\right), \\
h^{\mathrm{pp}}(C_6) &= \frac{h(-3p)}{4} - \frac{1}{2}\left(\frac{2}{p}\right) + \frac{1}{2}\left(\frac{p}{3}\right) - 1, \\
h^{\mathrm{pp}}(Q_8) &= 1, \quad h^{\mathrm{pp}}(Q_{12}) = 1 - \left(\frac{p}{3}\right), \quad h^{\mathrm{pp}}(E_{24}) = \frac{1}{2}\left(1 + \left(\frac{2}{p}\right)\right).
\end{aligned}$$

As a convention, if G is any finite group not listed above, then $h^{\mathrm{pp}}(G) = 0$.

§ 4. On the proofs

We explain the ideas of the proof of Theorem 3.1.

§ 4.1. Decomposition into genera

The notion of genera for abelian varieties with or without additional structures appears in [28, 29], and is investigated further in [24]. If $x = X_0$ is an abelian variety over $\mathbb{F}_q$, we define a group scheme G_x over $\mathbb{Z}$ as follows: for any commutative ring R, $G_x(R) := (\mathrm{End}(X_0) \otimes R)^\times$. If $\underline{x} = (X_0, \lambda_0)$ is a polarized abelian variety over $\mathbb{F}_q$, we define a group scheme $G_{\underline{x}}$ over $\mathbb{Z}$ similarly:

$$G_{\underline{x}}(R) := \{g \in (\mathrm{End}(X_0) \otimes R)^\times : g^t \lambda g = \lambda\}$$

for any commutative ring R.

Definition 4.1. (1) Let X_1 and X_2 be two abelian varieties over $\mathbb{F}_q$. They are said to be isogenous, denoted by $X_1 \sim X_2$, if there exists a quasi-isogeny $\alpha : X_1 \to X_2$ over $\mathbb{F}_q$. They are said to be *in the same genus* if $X_1 \sim X_2$ and $X_1[\ell^\infty] \simeq X_2[\ell^\infty]$ over $\mathbb{F}_q$ for all primes ℓ including p. The *genus* of X_1, denoted by $\mathcal{G}(X_1)$, consists of all abelian varieties $X_2/\mathbb{F}_q$ which are in the same genus as X_1.

(2) Two polarized abelian varieties (X_1, λ_1) and (X_2, λ_2) over $\mathbb{F}_q$ are said to be *isogenous*, denoted by $(X_1, \lambda_1) \sim (X_2, \lambda_2)$, if there exists a quasi-isogeny $\alpha : X_1 \to X_2$ over $\mathbb{F}_q$ such that $\alpha^*\lambda_2 = \lambda_1$. They are said to be *in the same genus* if $(X_1, \lambda_1) \sim (X_2, \lambda_2)$ and $(X_1, \lambda_1)[\ell^\infty] \simeq (X_2, \lambda_2)[\ell^\infty]$ for all primes ℓ. The *genus* of (X_1, λ_1), denote by $\mathcal{G}(X_1, \lambda_1)$, consists of all polarized abelian varieties $(X_2, \lambda_2)/\mathbb{F}_q$ which are in the same genus as (X_1, λ_1).

Proposition 4.2. *Let $x = X_0$ be an abelian variety over $\mathbb{F}_q$, and let $\Lambda(x)$ be the set of isomorphism classes of members in the genus $\mathcal{G}(x)$ of X_0. Let $\underline{x} = (X_0, \lambda_0)$ be a polarized abelian variety over $\mathbb{F}_q$, and let $\Lambda(\underline{x})$ be the set of isomorphism classes of members in the genus $\mathcal{G}(\underline{x})$ of (X_0, λ_0). Then there are natural bijections:*

$$\Lambda(x) \simeq G_x(\mathbb{Q})\backslash G_x(\mathbb{A}_f)/G_x(\hat{\mathbb{Z}}),$$

$$\Lambda(\underline{x}) \simeq G_{\underline{x}}(\mathbb{Q})\backslash G_{\underline{x}}(\mathbb{A}_f)/G_{\underline{x}}(\hat{\mathbb{Z}}).$$

In general, one has

$$\mathrm{Isog}(\pi) = \coprod_{i=1}^{r} \Lambda(x_i), \quad \mathrm{PPAV}(\pi) = \coprod_{i=1}^{r'} \Lambda(\underline{x}_i).$$

Therefore, $h(\pi) = |\,\mathrm{Isog}(\pi)|$ is a sum of certain class numbers of G_{x_i} and $h^{\mathrm{pp}}(\pi) = |\mathrm{PPAV}(\pi)|$ is a sum of certain class numbers of $G_{\underline{x}_i}$.

§ 4.2. The unpolarized case $\mathrm{Isog}(\sqrt{p}\,)$.

From now on, let $\pi = \sqrt{p}$, and $D = D_{\infty_1,\infty_2}$. One has

$$\mathrm{Isog}(\sqrt{p}\,) = \begin{cases} \Lambda_1 \coprod \Lambda_8 \coprod \Lambda_{16}, & \text{if } p \equiv 1 \pmod 4; \\ \Lambda_1 & \text{otherwise.} \end{cases}$$

For each $i \in \{1, 8, 16\}$, we have $\Lambda_i \simeq D^\times\backslash \widehat{D}^\times/\widehat{\mathcal{O}}_i^\times$, where $\mathcal{O}_i \subset D$ is an order satisfying

$$\text{there exists } [X] \in \Lambda_i \quad \text{with} \quad \mathcal{O}_i \simeq \mathrm{End}(X). \tag{4.1}$$

Such orders can easily be described locally at each prime ℓ using Tate's theorem. The subscript $i \in \{1, 8, 16\}$ is chosen so that $\mathcal{O}_i$ has index i in any maximal order containing it. Particularly, $\mathcal{O}_1$ is maximal.

In this case, one has $|\Lambda_1| = h(\mathcal{O}_1) = h(D)$ and $h(D) = h(F)t(D)$, where $t(D)$ is the type number of the quaternion algebra D. For $p \geq 7$, one has

$$t(D) = \frac{\zeta_F(-1)}{2} + \frac{h(-p)}{8} + \frac{h(-3p)}{6}, \quad \text{for } p \equiv 1 \pmod 4,$$

$$t(D) = \frac{\zeta_F(-1)}{2} + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-2p)}{4} + \frac{h(-3p)}{6}, \quad \text{for } p \equiv 3 \pmod 4,$$

which is due to Peters, Kitaoka and Ponomarev; see [11, 14].

Let d_F be the discriminant of $F = \mathbb{Q}(\sqrt{p})$, which is equal to p or $4p$ depending on whether $p \equiv 1 \pmod 4$ or not. Several people have also observed that

$$t(D) = H^+(d_F), \tag{4.2}$$

where $H^+(d_F)$ is the proper class number of even positive definite quaternary quadratic forms over $\mathbb{Z}$ of discriminant d_F.

§ 4.3. The polarized case PPAV($\sqrt{p}$).

We have the decomposition into genera:

$$\mathrm{PPAV}(\sqrt{p}) = \begin{cases} \Lambda_1^{\mathrm{pp}} \coprod \Lambda_{16}^{\mathrm{pp}}, & \text{if } p \equiv 1 \pmod 4; \\ \Lambda_1^{\mathrm{pp}}, & \text{if } p \equiv 3 \pmod 4 \text{ or } p = 2. \end{cases} \tag{4.3}$$

For each $i \in \{1, 16\}$, fix an order $\mathcal{O}_i \subset D$ such that

$$\text{there exists } [X, \lambda] \in \Lambda_i^{\mathrm{pp}} \quad \text{with} \quad \mathcal{O}_i \simeq \mathrm{End}(X). \tag{4.4}$$

Then there is a bijection

$$\Lambda_i^{\mathrm{pp}} \simeq D^1 \backslash \widehat{D}^1 / \widehat{\mathcal{O}}_i^1 \tag{4.5}$$

where $\widehat{D}^1 := \mathrm{Ker}(N : \widehat{D}^\times \to \widehat{F}^\times)$, and $D^1, \widehat{\mathcal{O}}_i^1 \subset \widehat{D}^1$ are norm one subgroups in $D^\times$ and in $\widehat{\mathcal{O}}_i^\times$, respectively.

Let us take a closer look at condition (4.4) for $i = 1$. Fix a maximal order $\mathbb{O}_0$ satisfying (4.4). The set $\mathrm{Tp}(D)$ of types of maximal orders of D can be expressed as

$$\mathrm{Tp}(D) \simeq D^\times \backslash \widehat{D}^\times / \mathcal{N}(\widehat{\mathbb{O}}_0),$$

where $\mathcal{N}(\widehat{\mathbb{O}}_0)$ is the normalizer of $\widehat{\mathbb{O}}_0$ in $\widehat{D}^\times$. Denote

$$\Psi : \Lambda_1^{\mathrm{pp}} \to \mathrm{Tp}(D), \quad [X, \lambda] \mapsto [\mathrm{End}(X)]. \tag{4.6}$$

For the moment, suppose that $p \equiv 3 \pmod 4$. Then the Gauss genus group $\mathrm{Pic}_+(O_F)/\mathrm{Pic}_+(O_F)^2$ can be canonically identified with the multiplicative group $\{\pm 1\}$. The surjective norm map

$$\mathrm{Tp}(D) \simeq D^\times \backslash \widehat{D}^\times / \mathcal{N}(\widehat{\mathbb{O}}_0) \xrightarrow{N} F_+^\times \backslash \widehat{F}^\times / (\widehat{F}^\times)^2 \widehat{O}_F^\times = \{\pm 1\} \tag{4.7}$$

induces a decomposition

$$\mathrm{Tp}(D) = \mathrm{Tp}^+(D) \coprod \mathrm{Tp}^-(D),$$

where $\mathrm{Tp}^+(D)$ and $\mathrm{Tp}^-(D)$ are the fibers of $+1$ and -1, respectively. It can be shown that a maximal order $\mathcal{O} \subset D$ satisfies (4.4) if and only if $[\mathcal{O}] \in \mathrm{Tp}^+(D)$. Therefore,

$$t^{\mathrm{pp}}(\sqrt{p}) = |\mathrm{Tp}^+(D)| \qquad \text{when } p \equiv 3 \pmod 4. \tag{4.8}$$

Chan and Peters [3] made the following improvement of (4.2). When $p \equiv 3 \pmod 4$, the quaternary quadratic forms in question are separated into two genera since the Gauss genus group $\mathrm{Pic}_+(O_F)/\mathrm{Pic}_+(O_F)^2$ has order 2 in this case. Changing the notation slightly, write γ^+ for the principal Gauss genus and γ^- the non-principal one. Chan and Peters showed that there is a way to label the two genera of quaternary quadratic forms by γ^+ and γ^- respectively such that

$$H^+(4p) = H^+(4p, \gamma^+) + H^+(4p, \gamma^-), \qquad \text{and} \tag{4.9}$$

$$\begin{aligned} H^+(4p, \gamma^+) &= |\mathrm{Tp}^+(D)| \\ &= \frac{\zeta_F(-1)}{4} + \left(17 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{16} + \frac{h(-2p)}{8} + \frac{h(-3p)}{12}, \end{aligned} \tag{4.10}$$

$$\begin{aligned} H^+(4p, \gamma^-) &= |\mathrm{Tp}^-(D)| \\ &= \frac{\zeta_F(-1)}{4} + \left(9 - 9\left(\frac{2}{p}\right)\right) \frac{h(-p)}{16} + \frac{h(-2p)}{8} + \frac{h(-3p)}{12}. \end{aligned} \tag{4.11}$$

Combining with (4.8) we obtain a new relation

$$t^{\mathrm{pp}}(\sqrt{p}) = H^+(4p, \gamma^+) \qquad \text{when } p \equiv 3 \pmod 4. \tag{4.12}$$

For notation, we put $t(D, \gamma^+) := |\mathrm{Tp}^+(D)|$ and $t(D, \gamma^-) := |\mathrm{Tp}^-(D)|$.

We return to the general case where p is arbitrary.

Lemma 4.3. (1) *If $p \not\equiv 3 \pmod 4$, then the map $\Psi : \Lambda_1^{\mathrm{pp}} \xrightarrow{\sim} \mathrm{Tp}(D)$ is a bijection.*

(2) *If $p \equiv 3 \pmod 4$, then $\Psi : \Lambda_1^{\mathrm{pp}} \twoheadrightarrow \mathrm{Tp}^+(D)$ is a two-to-one cover ramified over the subset*

$$\{[\mathbb{O}] \in \mathrm{Tp}^+(D) : N(\mathbb{O}^\times) = O_{F,+}^\times\}.$$

Part (1) of the lemma implies that when $p \equiv 1 \pmod 4$, condition (4.4) is no more stronger than condition (4.1) (as far as maximal orders are concerned). Moreover, in this case

$$|\Lambda_1^{\mathrm{pp}}| = |\mathrm{Tp}(D)| = \frac{h(\mathbb{O}_0)}{h(F)} = \frac{\zeta_F(-1)}{2} + \frac{h(-p)}{8} + \frac{h(-3p)}{6}.$$

Similar results hold for $i = 16$ as well, so we have

$$|\Lambda_{16}^{\mathrm{pp}}| = |\mathrm{Tp}(\mathcal{O}_{16})| = \frac{h(\mathcal{O}_{16})}{h(A)}, \quad \text{where} \quad A = \mathbb{Z}[\sqrt{p}\,].$$

This gives

$$|\Lambda_{16}^{\mathrm{pp}}| = \left(8 - 2\left(\frac{2}{p}\right)\right) \frac{\zeta_F(-1)}{2} + \frac{h(-p)}{4} + \left(2 + \left(\frac{2}{p}\right)\right) \frac{h(-3p)}{6}.$$

Combining the above formulas, we obtain

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

This completes the proof for the case $p \equiv 1 \pmod 4$.

§ 4.4. The case $p \equiv 3 \pmod 4$: the class number formula of the norm one group.

For this part we use the Selberg trace formula. In our initial proof, we calculate the orbital integrals in the elliptic terms directly. The approach we explain here uses the formulae for norm-one class numbers and spinor class numbers of quaternion algebras in [25]. That simplifies and shortens the direct compuations.

From the previous section, the task of computing $h^{\mathrm{pp}}(\sqrt{p}\,)$ when $p \equiv 3 \pmod 4$ is separated into two steps:

1. find an explicit maximal order $\mathbb{O}_0$ in $D = D_{\infty_1,\infty_2}$ satisfying (4.4);
2. compute the class number $h^1(\mathbb{O}_0) := |D^1 \backslash \widehat{D}^1 / \widehat{\mathbb{O}}_0^1|$.

Combining (4.3) and (4.5), we get $h^{\mathrm{pp}}(\sqrt{p}\,) = h^1(\mathbb{O}_0)$.

The first step is relatively easy. Let $E/\mathbb{F}_{p^2}$ be an elliptic curve with $[E] \in \mathrm{Isog}(p)$, and λ_E be the canonical principal polarization of E. Take $(X, \lambda_X) := \mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E, \lambda_E)$, the Weil restriction of (E, λ_E) with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$. Then $[X, \lambda_X] \in \mathrm{PPAV}(\sqrt{p}\,)$. For simplicity, put $\mathbb{o} := \mathrm{End}_{\mathbb{F}_{p^2}}(E)$, which is a maximal order in $\mathrm{End}^0_{\mathbb{F}_{p^2}}(E) = D_{p,\infty}$. Similarly, put $\mathbb{O} := \mathrm{End}_{\mathbb{F}_p}(X)$, which is also a maximal order in $\mathrm{End}^0_{\mathbb{F}_p}(X) = D$. By functoriality of the Weil restriction, $\mathbb{o} \otimes O_F$ acts on X. This action identifies $D_{p,\infty} \otimes F$ with D and realizes $\mathbb{o} \otimes O_F$ as a suborder of $\mathbb{O}$.

Now we make the above construction explicit. Since $p \equiv 3 \pmod 4$, there is a unique member $[E_0] \in \mathrm{Isog}(p)$ with $\mathrm{Aut}_{\mathbb{F}_{p^2}}(E_0) \simeq C_6$ by (1.5). Its endomorphism ring is given by

$$\mathbb{o}_0 := \mathrm{End}_{\mathbb{F}_{p^2}}(E_0) = \mathbb{Z}[i, (1+j_p)/2] \subseteq D_{p,\infty}, \tag{4.13}$$

where $1, i, j_p, ij_p$ is a $\mathbb{Q}$-basis of $D_{p,\infty}$ satisfying $i^2 = -1$, $j_p^2 = -p$ and $i \cdot j_p = -j_p \cdot i$. Now put $j := j_p/\sqrt{p} \in D = D_{p,\infty} \otimes \mathbb{Q}(\sqrt{p})$, then $1, i, j, ij$ is the standard basis of $D = \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{p})}\right)$. One easily checks that

$$\mathbb{O}_0 := O_F + O_F\, i + O_F \frac{\sqrt{p}+j}{2} + O_F\, i \cdot \frac{\sqrt{p}+j}{2} \tag{4.14}$$

is the unique maximal order in D containing $\mathbb{o}_0 \otimes O_F$. Therefore, if we put $X_0 = \mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$, then $\mathbb{O}_0 = \mathrm{End}_{\mathbb{F}_p}(X_0)$, and it satisfies (4.4) by our construction.

Now we move on to the next step. To motivate the calculation of the class number $h^1(\mathbb{O}_0)$, let us recall the classical Eichler class number formula. For the moment let F be an arbitrary totally real field, D be a totally definite quaternion F-algebra of reduced discriminant $\mathfrak{d}$, and $\mathcal{O} \subset D$ be an Eichler O_F-order of level $\mathfrak{n}$ in D. The class number $h(\mathcal{O})$ by definition is the cardinality of the double coset space $D^\times \backslash \widehat{D}^\times / \widehat{\mathcal{O}}^\times$. According to [17, Corollary V.2.5], $h(\mathcal{O})$ can be computed by the following formula:

$$h(\mathcal{O}) = \mathrm{Mass}(\mathcal{O}) + \frac{1}{2} \sum_{w(B)>1} h(B)(1 - w(B)^{-1}) \prod_{\mathfrak{p}} m_{\mathfrak{p}}(B), \tag{4.15}$$

Here $\mathrm{Mass}(\mathcal{O})$ is defined in [17, p. 143] and can be computed by the *mass formula* [17, Corollary V.2.3]. The summation is taken over all O_F-orders B such that $B \otimes_{O_F} F$ is a CM-extension of F and $w(B) := [B^\times : O_F^\times] > 1$. Up to isomorphism, there are only finitely many such orders B, so the summation is finite. Lastly, for each finite prime $\mathfrak{p}$ of F, we write $\mathrm{Emb}(B_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}})$ for the set of optimal embeddings of $B_{\mathfrak{p}}$ into $\mathcal{O}_{\mathfrak{p}}$. More explicitly,

$$\mathrm{Emb}(B_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) := \{\varphi_{\mathfrak{p}} : B_{\mathfrak{p}} \hookrightarrow \mathcal{O}_{\mathfrak{p}} \mid \mathcal{O}_{\mathfrak{p}}/\varphi_{\mathfrak{p}}(B_{\mathfrak{p}}) \text{ is } O_{F_{\mathfrak{p}}}\text{-torsion free}\}. \tag{4.16}$$

We define $m_{\mathfrak{p}}(B)$ to be the number of $\mathcal{O}_{\mathfrak{p}}^\times$-conjugacy classes of optimal embeddings of $B_{\mathfrak{p}}$ into $\mathcal{O}_{\mathfrak{p}}$, that is,

$$m_{\mathfrak{p}}(B) := |\mathrm{Emb}(B_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}})/\mathcal{O}_{\mathfrak{p}}^\times|.$$

The formula for $m_{\mathfrak{p}}(\mathcal{O})$ is given by Eichler in the case $\mathfrak{n}$ is square-free and by Hijikata for general $\mathfrak{n}$. For almost all $\mathfrak{p}$, we have $\mathcal{O}_{\mathfrak{p}} \simeq \mathrm{Mat}_2(O_{F_{\mathfrak{p}}})$, which implies that $m_{\mathfrak{p}}(B) = 1$. Thus the product in (4.15) is finite as well. In fact, many results in this article (such as formula (1.1) and Theorem 2.1) are direct consequences of (variants of) Eichler class number formula.

Naturally, one desires a similar formula for the class number $h^1(\mathcal{O}) := |D^1\backslash\widehat{D}^1/\widehat{\mathcal{O}}^1|$. Different from $h(\mathcal{O})$, the value of $h^1(\mathcal{O})$ depends not only on F, $\mathfrak{d}$ and $\mathfrak{n}$, but also more subtly on $\mathcal{O}$ itself. To explain this, let us fix an Eichler order $\mathcal{O}_0$ of level $\mathfrak{n}$ and write $\mathrm{Tp}(\mathcal{O}_0)$ for the set of types of Eichler orders of level $\mathfrak{n}$ in D. Similar to (4.7), we consider the (surjective) reduced norm map

$$\mathrm{Tp}(\mathcal{O}_0) \simeq D^\times\backslash\widehat{D}^\times/\mathcal{N}(\widehat{\mathcal{O}}_0) \xrightarrow{N} F_+^\times\backslash\widehat{F}^\times/N(\mathcal{N}(\widehat{\mathcal{O}}_0)). \tag{4.17}$$

Two Eichler orders $\mathcal{O}$ and $\mathcal{O}'$ of level $\mathfrak{n}$ are said to be in the same *spinor genus* and denoted by $\mathcal{O} \sim \mathcal{O}'$ if their types $[\mathcal{O}]$ and $[\mathcal{O}']$ belong to the same fiber of the norm map in (4.17). This definition does not depend on the choice of $\mathcal{O}_0$. An easy calculation shows that $h^1(\mathcal{O})$ is uniquely determined by the spinor genus of $\mathcal{O}$. Thus to get a class number formula for $h^1(\mathcal{O})$, one must make distinctions of the spinor genera and figure out how such distinctions manifest themselves in the calculation of $h^1(\mathcal{O})$. It is at this critical juncture where *optimal spinor selectivity* comes in.

Let K/F be a CM-extension that is F-embeddable into D, and $B \subset K$ be an O_F-order. We define the symbol

$$\Delta(B,\mathcal{O}) = \begin{cases} 1 & \text{if } \exists\, \mathcal{O}' \text{ such that } \mathcal{O}' \sim \mathcal{O} \text{ and } \mathrm{Emb}(B,\mathcal{O}') \neq \emptyset; \\ 0 & \text{otherwise.} \end{cases} \tag{4.18}$$

Once again, $\mathrm{Emb}(B,\mathcal{O}')$ denotes the set of optimal embeddings of B into $\mathcal{O}'$. From [18, Corollary 30.4.8], there exists an Eichler order $\mathcal{O}_0$ of level $\mathfrak{n}$ in D with $\mathrm{Emb}(B,\mathcal{O}_0) \neq \emptyset$ if and only if $m_\mathfrak{p}(B) \neq 0$ for every finite prime $\mathfrak{p}$. In particular, $\Delta(B,\mathcal{O}) = 0$ if there exists $\mathfrak{p}$ such that $m_\mathfrak{p}(B) = 0$.

Definition 4.4. Suppose that $m_\mathfrak{p}(B) \neq 0$ for every finite prime $\mathfrak{p}$. We say B is *optimally spinor selective* (or *selective* for short) for Eichler orders of level $\mathfrak{n}$ in D if there exists an Eichler order $\mathcal{O}''$ of level $\mathfrak{n}$ such that $\Delta(B,\mathcal{O}'') = 0$.

The assumption of Definition 4.4 guarantees that there exists an Eichler order $\mathcal{O}_0$ of level $\mathfrak{n}$ with $\Delta(B,\mathcal{O}_0) = 1$. If B is selective and $\Delta(B,\mathcal{O}_0') = 1$ for some $\mathcal{O}_0'$, then we say the spinor genus of $\mathcal{O}_0'$ is selected by B.

Factorize the level $\mathfrak{n}$ into a product of prime powers $\prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{n})}$. The optimal spinor selectivity theorem provides an elegant criterion for selectivity in terms of class field theory.

Theorem 4.5. *Let D be a totally definite quaternion algebra over a totally real field F, and let B be an O_F-order of a CM-extension K/F. Suppose that B is optimally embeddable into an Eichler order of level $\mathfrak{n}$ in D. Then B is selective for Eichler orders of level $\mathfrak{n}$ in D if and only if both of the following conditions hold:*

1. both D and K are unramified at all the finite primes of F;

2. if $\mathfrak{p}$ is a finite prime of F with $\nu_{\mathfrak{p}}(\mathfrak{n}) \equiv 1 \pmod 2$, then $\mathfrak{p}$ splits in K.

If B is selective, then exactly half of the spinor genera are selected by B.

In fact, if B is selective, then starting from a known selectivity symbol $\Delta(B, \mathcal{O})$, one can express all other $\Delta(B, \mathcal{O}')$ in terms of $\Delta(B, \mathcal{O})$ and the "relative position" of $\mathcal{O}$ and $\mathcal{O}'$. See [25, Theorem 2.11] for details. A variant of Theorem 4.5 is first proved for *indefinite* quaternion algebras by Arenas et al. [2] and by Voight [18, Theorem 31.1.7] independently. Similar ideas of the proofs in loc. cit. are adapted to extend to *totally definite* quaternion algebras here.

Given a CM-extension K/F, we put $s(\mathfrak{n}, K) = 1$ if K and D satisfy both of the conditions in Theorem 4.5, and $s(\mathfrak{n}, K) = 0$ otherwise. Following [17, §V.2, p. 143], we put

$$M(B) := \frac{h(B)}{w(B)} \prod_{\mathfrak{p}} m_{\mathfrak{p}}(B). \tag{4.19}$$

Now we are ready to state the norm-one class number formula for an Eichler order $\mathcal{O}$ of level $\mathfrak{n}$:

$$h^1(\mathcal{O}) = 2\,\mathrm{Mass}^1(\mathcal{O}) + \frac{1}{4h(F)} \sum_{|\boldsymbol{\mu}(B)|>2} 2^{s(\mathfrak{n},K)} \Delta(B, \mathcal{O})(|\boldsymbol{\mu}(B)| - 2) M(B). \tag{4.20}$$

Here $\boldsymbol{\mu}(B)$ is the group of roots of unity in B, and the summation is over all O_F-orders B such that $B \otimes_{O_F} F$ is a CM-extension of F and $|\boldsymbol{\mu}(B)| > 2$. Write $r = [F : \mathbb{Q}]$. Then $\mathrm{Mass}^1(\mathcal{O})$ can be computed by the following formula:

$$\mathrm{Mass}^1(\mathcal{O}) = \frac{1}{2^r} |\zeta_F(-1)|\, \mathrm{N}(\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{d}} (\mathrm{N}(\mathfrak{p}) - 1) \prod_{\mathfrak{p}|\mathfrak{n}} (1 + \mathrm{N}(\mathfrak{p})^{-1}). \tag{4.21}$$

The proof of (4.20) relies on the Selberg trace formula for compact quotient spaces, namely $D^1 \backslash \widehat{D}^1$ in the present setting. Instead of computing the orbital integrals directly, we take a lengthy and arduous process to regroup the terms and connect them with the spinor trace formula [25, Proposition 2.15] to obtain (4.20).

Finally, we return to the computation of $h^{\mathrm{pp}}(\sqrt{p}\,) = h^1(\mathbb{O}_0)$. In this case $F = \mathbb{Q}(\sqrt{p}\,)$, $D = D_{\infty_1, \infty_2}$, and $\mathfrak{d} = \mathfrak{n} = O_F$. It follows that $\mathrm{Mass}^1(\mathbb{O}_0) = \zeta_F(-1)/4$, and $s(\mathfrak{n}, K) = 1$ if and only if $K = F(\sqrt{-1}\,)$. For $B \subset F(\sqrt{-1}\,)$, the values of $\Delta(B, \mathbb{O}_0)$ can be computed directly using the explicit expression (4.14) of $\mathbb{O}_0$. All other terms in (4.20) are calculated routinely. This yields

$$h^1(\mathbb{O}_0) = \frac{\zeta_F(-1)}{2} + \left(11 - 3\left(\frac{2}{p}\right)\right) \frac{h(-p)}{8} + \frac{h(-3p)}{6}. \tag{4.22}$$

This finishes the explanation of the proof of Theorem 3.1.

Remark 4.6. If $\mathbb{O} \subseteq D$ is a maximal order with $[\mathbb{O}] \in \mathrm{Tp}^-(D)$, i.e. $\mathbb{O} \not\simeq \mathbb{O}_0$, then a similar calculation as above yields that

$$h^1(\mathbb{O}) = \frac{\zeta_F(-1)}{2} + \left(3 - 3\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-3p)}{6}. \tag{4.23}$$

Observe that the second terms in (4.22) and (4.23) are different while the third terms coincide. This is precisely because O_F-orders in $F(\sqrt{-1}\,)$ are selective for maximal orders in D while O_F-orders in $F(\sqrt{-3}\,)$ are non-selective.

§ 5. Connections with Hilbert modular surfaces

Let F be an arbitrary real quadratic field. We regard $F \oplus F$ as the column vector space and let $\mathrm{Mat}_2(F) = \mathrm{End}_F(F \oplus F)$ act on $F \oplus F$ by left multiplication. For any ideal $\mathfrak{a}$ of O_F, let

$$\begin{aligned} \mathrm{SL}(O_F \oplus \mathfrak{a}) &= \{g \in \mathrm{SL}_2(F) \mid g \cdot (O_F \oplus \mathfrak{a}) = O_F \oplus \mathfrak{a}\,\}, \\ \Gamma(O_F \oplus \mathfrak{a}) &= \text{the image of } \mathrm{SL}(O_F \oplus \mathfrak{a}) \text{ in } \mathrm{PSL}_2(F), \\ \Gamma_m(O_F \oplus \mathfrak{a}) &= \text{the Hurwitz-Maass extension of } \Gamma(O_F \oplus \mathfrak{a}). \end{aligned}$$

Let $\mathbb{H}$ be the complex upper half plane. For $\Gamma = \Gamma(O_F \oplus \mathfrak{a})$ or $\Gamma = \Gamma_m(O_F \oplus \mathfrak{a})$, we denote by $(\Gamma\backslash\mathbb{H}^2)^*$ the minimal compactification of $\Gamma\backslash\mathbb{H}^2$, which is obtained by adding all cusps $\Gamma\backslash\mathbb{P}^1(F)$ to $\Gamma\backslash\mathbb{H}^2$. Let Y_Γ be a projective smooth model of $(\Gamma\backslash\mathbb{H}^2)^*$. The *arithmetic genus* of Y_Γ is defined to be

$$\chi(Y_\Gamma) := \sum_{i=0}^{2}(-1)^i \dim H^i(Y_\Gamma, \mathcal{O}_{Y_\Gamma}). \tag{5.1}$$

The arithmetic genus $\chi(Y_\Gamma)$ does not depend on the choice of the smooth model Y_Γ.

Note that if the narrow ideal classes $[\mathfrak{a}]$ and $[\mathfrak{a}']$ are in the same Gauss genus in $\mathrm{Pic}_+(O_F)/\mathrm{Pic}_+(O_F)^2$, then

$$\Gamma(O_F \oplus \mathfrak{a})\backslash\mathbb{H}^2 \simeq \Gamma(O_F \oplus \mathfrak{a}')\backslash\mathbb{H}^2 \text{ and } (\Gamma(O_F \oplus \mathfrak{a})\backslash\mathbb{H}^2)^* \simeq (\Gamma(O_F \oplus \mathfrak{a}')\backslash\mathbb{H}^2)^*.$$

So one can choose smooth models of them such that $Y_{\Gamma(O_F\oplus\mathfrak{a})} \simeq Y_{\Gamma(O_F\oplus\mathfrak{a}')}$. For each class $\gamma \in \mathrm{Pic}_+(O_F)/\mathrm{Pic}_+(O_F)^2$, put $Y(d_F, \gamma) := Y_{\Gamma(O_F\oplus\mathfrak{a})}$, where $\mathfrak{a}$ is an ideal of O_F such that $[\mathfrak{a}] \in \gamma$. Then $\chi(Y(d_F, \gamma))$ only depends on γ. Similarly, we let $Y_m(d_F, \gamma) := Y_{\Gamma_m(O_F\oplus\mathfrak{a})}$.

Now let $F = \mathbb{Q}(\sqrt{p}\,)$. Based on known explicit formulae for $\chi(Y(d_F, \gamma))$ [6, Theorems II.5.8–9], $\chi(Y_m(d_F, \gamma))$ [15, §I.4, p. 13] , $t(D)$ and $H^+(d_F)$ [3, §1], and the explicit formula for $|\Lambda_1^{\mathrm{pp}}|$ (Theorems 3.1), if $p \not\equiv 3 \pmod 4$, we have

$$\chi(Y(d_F, \gamma)) = \chi(Y_m(d_F, \gamma)) = |\Lambda_1^{\mathrm{pp}}| = t(D) = H^+(d_F), \tag{5.2}$$

where $d_F = p$ if $p \equiv 1 \pmod 4$, and $d_F = 8$ if $p = 2$.

If $p \equiv 3 \pmod 4$, then there are two Gauss genera. Let γ^+ denote the principal Gauss genus and γ^- the non-principal one. Based on known explicit formulae loc. cit., Theorem 3.2, and (4.10), (4.11), (4.12), we have

$$\chi(Y(4p, \gamma^-)) = |\Lambda_1^{\mathrm{pp}}|, \tag{5.3}$$

$$\chi(Y_m(4p, \gamma^+)) = t(D, \gamma^-) = H^+(4p, \gamma^+), \tag{5.4}$$

$$\chi(Y_m(4p, \gamma^-)) = t(D, \gamma^+) = H^+(4p, \gamma^-). \tag{5.5}$$

As for current status, the identities $|\Lambda_1^{\mathrm{pp}}| = t(D) = H^+(p)$ for $p \equiv 1 \pmod 4$ and $t(D) = H^+(4p)$ for $p \equiv 3 \pmod 4$ were proved directly without knowing their formulae. For other identities, it remains to discover a better proof .

Acknowledgments

The second author thanks the organizers, Shushi Harashita, Momonari Kudo, and Katsuyuki Takashima, of the RIMS conference "Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties" for their warm invitation and hospitality; he enjoyed the conference very much. This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. Yu is partially supported by the MoST grants 107-2115-M-001-001-MY2 and 109-2115-M-001-002-MY3. They are grateful to the referee for a careful reading and helpful suggestions.

References

[1] Jeff Achter, Salim Ali Altug, Julia Gordon, Wen-Wei Li, and Thomas Rüd. Counting abelian varieties over finite fields via frobenius densities, 2019, `arXiv:1905.11603`.

[2] Manuel Arenas, Luis Arenas-Carmona, and Jaime Contreras. On optimal embeddings and trees. *J. Number Theory*, 193:91–117, 2018.

[3] Wai Kiu Chan and Meinhard Peters. Quaternary quadratic forms and Hilbert modular surfaces. In *Algebraic and arithmetic theory of quadratic forms*, volume 344 of *Contemp. Math.*, pages 85–97. Amer. Math. Soc., Providence, RI, 2004.

[4] Max Deuring. Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. *Jber. Deutsch. Math. Verein.*, 54:24–41, 1950.

[5] Martin Eichler. Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.*, 43(1):102–109, 1938.

[6] Eberhard Freitag. *Hilbert modular forms.* Springer-Verlag, Berlin, 1990.

[7] Jia-Wei Guo, Nai-Heng Sheu, and Chia-Fu Yu. Class numbers of CM algebraic tori, CM abelian varieties and components of unitary Shimura varieties. *arXiv e-prints*, page arXiv:1905.11649, May 2019, `arXiv:1905.11649`. To appear in Nagoya Math. J.

[8] Ki-ichiro Hashimoto. Twisted trace formula of the Brandt matrix. *Proc. Japan Acad. Ser. A Math. Sci.*, 53(3):98–102, 1977.

[9] Everett W. Howe. Kernels of polarizations of abelian varieties over finite fields. *J. Algebraic Geom.*, 5(3):583–608, 1996.

[10] 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.

[11] Yoshiyuki Kitaoka. Quaternary even positive definite quadratic forms of prime discriminant. *Nagoya Math. J.*, 52:147–161, 1973.

[12] Qun Li, Jiangwei Xue, and Chia-Fu Yu. Unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields. *Trans. Amer. Math. Soc.*, 374(8):5349–5403, 2021.

[13] Stefano Marseglia. Computing square-free polarized abelian varieties over finite fields. *Math. Comp.*, 90(328):953–971, 2021.

[14] Paul Ponomarev. Class number formulas for quaternary quadratic forms. *Acta Arith.*, 39(1):95–104, 1981.

[15] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

[16] Marie-France Vignéras. Invariants numériques des groupes de Hilbert. *Math. Ann.*, 224(3):189–215, 1976.

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

[18] John Voight. *Quaternion algebras (v.0.9.23)*, volume 288 of *Graduate Texts in Mathematics*. Springer-Verlag, 2021. Current postprint version available at `https://math.dartmouth.edu/~jvoight/quat-book.pdf`.

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

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

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

[22] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Supersingular abelian surfaces and Eichler's class number formula. *Asian J. Math.*, 23(4):651–680, 2019.

[23] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. On superspecial abelian surfaces over finite fields II. *J. Math. Soc. Japan*, 72(1):303–331, 2020.

[24] Jiangwei Xue and Chia-Fu Yu. Counting abelian varieties over finite fields. *Acta Math. Sin. (Engl. Ser.)*, 37(1):205–228, 2021.

[25] Jiangwei Xue and Chia-Fu Yu. Spinor class number formulas for totally definite quaternion orders. *arXiv e-prints*, page arXiv:1909.11858, Sep 2019, `arXiv:1909.11858`.

[26] Jiangwei Xue and Chia-Fu Yu. Polarized superspecial simple abelian surfaces with real weil numbers, 2020, `arXiv:2009.02729`.

[27] Jiangwei Xue and Chia-Fu Yu. On superspecial abelian surfaces and type numbers of totally definite quaternion algebras. *Indiana Univ. Math. J.*, 70(2):781–808, 2021.

[28] Chia-Fu Yu. Simple mass formulas on Shimura varieties of PEL-type. *Forum Math.*, 22(3):565–582, 2010.
[29] Chia-Fu Yu. Abelian varieties over finite fields as basic abelian varieties. *Forum Math.*, 29(2):489–500, 2017.