THE GAUSS PROBLEM FOR CENTRAL LEAVES

TOMOYOSHI IBUKIYAMA, VALENTIJN KAREMAKER, AND CHIA-FU YU

ABSTRACT. We solve two related Gauss problems. In the arithmetic setting, we consider genera of maximal O-lattices, where O is the maximal order in a definite quaternion $\mathbb{Q}$-algebra, and we list all cases where they have class number 1. We also prove a unique orthogonal decomposition result for more general O-lattices. In the geometric setting, we study the Siegel modular variety $\mathscr{A}_g \otimes \overline{\mathbb{F}}_p$ of genus g, and we list all x in $\mathscr{A}_g \otimes \overline{\mathbb{F}}_p$ for which the corresponding central leaf $\mathscr{C}(x)$ consists of one point, that is, such that x is the unique point in the locus consisting of the points whose associated polarised p-divisible groups are isomorphic to that of x. The solution to the second Gauss problem involves mass formulae, computations of automorphism groups, and a careful analysis of Ekedahl-Oort strata in genus $g = 4$.

1. INTRODUCTION

For a given family of finite sets which typically arise from an arithmetic source and whose cardinalities are naturally called class numbers – for example, the family of ideal class groups indexed by a class of number fields – the Gauss problem asks for the determination of the subfamily in which every member has class number one. As the most famous result, there are 9 imaginary quadratic fields of class number one, due to Heegner and proved independently by Baker and Stark around 1966. Masley and Montgomery [33] determined the cyclotomic fields of class number one; there are 29 of them, cf. Washington [45, Chapter 11] for an exposition and historical background. The family of imaginary abelian fields has been determined by K. Yamamura [46] in 1994. Since then, solving the Gauss problem for normal CM fields has been a major undertaking by various authors. In 2006 the best bound for the degree d of a normal CM field of class number one was given by Lee-Kwon [30], who showed that d satisfies $d \leq 96$ under the Generalised Riemann Hypothesis (GRH). In 2007, Park-Kwon [38] and Park-Yang-Kwon [39] determined all the remaining cases of $d \leq 48$ among all possible values of d in $\{2, 4, \ldots, 48\} \cup \{64, 96\}$. The last two cases have been determined by Hofmann-Sircana [18], who showed that there is no normal CM field of degree $d = 64$ or $d = 96$ of class number one. Besides 172 abelian CM fields determined by Yamamura, there are 55 non-abelian normal CM fields with class number one under GRH.

The present paper solves two related Gauss problems: the first one comes from positive-definite quaternion Hermitian forms and the second one from the reduction modulo some prime p of Siegel modular varieties. For the first Gauss problem, let B be a definite quaternion $\mathbb{Q}$-algebra of discriminant D and let O be a maximal order in B. Let V be a left B-module of rank n, and $f : V \times V \to B$ be a positive-definite quaternion Hermitian form with respect to the canonical involution $x \mapsto \bar{x}$. For each O-lattice L in V denote by $h(L, f)$ the class number of the isomorphism classes in the genus containing L. As the main result of the first, arithmetic, part of this paper, in Theorem 2.9 we determine precisely when $h(L, f) = 1$ for all maximal O-lattices L. For the rank one case, the list of definite quaternion $\mathbb{Z}$-orders of class number one has been determined by Brzezinski [5] in 1995.

2020 *Mathematics Subject Classification.* 14K10 (14K15, 11G10, 11E41, 16H20).

Key words and phrases. Gauss problem, Hermitian lattices, abelian varieties, central leaves, mass formula.

For the second Gauss problem, let p a prime number and let $\mathscr{A}_g$ denote the moduli space over $\overline{\mathbb{F}}_p$ of g-dimensional principally polarised abelian varieties. Let k be an algebraically closed field of characteristic p. For each point $x = [(X_0, \lambda_0)] \in \mathscr{A}_g(k)$, denote by

$$\mathscr{C}(x) := \{[(X, \lambda)] \in \mathscr{A}_g(k) : (X, \lambda)[p^\infty] \simeq (X_0, \lambda_0)[p^\infty]\}$$

the central leaf of $\mathscr{A}_g$ passing through the point x. Our goal is to determine the set of all points x in $\mathscr{A}_g(k)$ such that $\mathscr{C}(x) = \{x\}$.

Let $\mathscr{S}_g \subseteq \mathscr{A}_g$ denote the supersingular locus of $\mathscr{A}_g$, which is the closed subvariety parametrising all supersingular abelian varieties in $\mathscr{A}_g$. For each abelian variety X over k, the a-number of X is defined by

$$a(X) := \dim \mathrm{Hom}(\alpha_p, X), \tag{1}$$

where α_p is the kernel of the Frobenius morphism on the additive group $\mathbb{G}_a$. The a-number of a point x in $\mathscr{A}_g$ is denoted by $a(x)$.

The main result of the second, geometric, part of the paper is the following solution to the Gauss problem.

Theorem A. *(Theorem 5.20) Let $x = [X_0, \lambda_0] \in \mathscr{A}_g(k)$ and $\mathscr{C}(x)$ be the central leaf of $\mathscr{A}_g$ passing through the point x.*

(1) *(Chai [7]) The set $\mathscr{C}(x)$ is finite if and only if X_0 is supersingular, that is, X_0 is isogenous to a product of supersingular elliptic curves.*
(2) *Assume that $x \in \mathscr{S}_g$. Then $\mathscr{C}(x)$ has one element if and only if one of the following three cases holds:*
   (i) *$g = 1$ and $p \in \{2, 3, 5, 7, 13\}$;*
   (ii) *$g = 2$ and $p = 2, 3$;*
   (iii) *$g = 3$, $p = 2$ and $a(x) \geq 2$.*

The result of Chai (cf. Theorem A.(1)) shows that the above two Gauss problems are related. Theorem A.(2)(i) is well-known; Theorem A.(2)(ii) is a result due to the first author [21]. We prove the remaining cases; namely, we show that $|\mathscr{C}(x)| > 1$ for $g \geq 4$, and that when $g = 3$, (iii) lists the only cases such that $|\mathscr{C}(x)| = 1$. When $g = 3$ and $a(x) = 3$ (the *principal genus* case), the class number one result is known due to Hashimoto [15]. Hashimoto first computes an explicit class number formula in the principal genus case and proves the class number one result as a direct consequence.

Our method instead uses mass formulae and the automorphism groups of certain abelian varieties, which is much simpler than proving explicit class number formulae. Mass formulae for dimension $g = 3$ were very recently provided by F. Yobuko and the second and third-named authors [23]. In addition, we perform a careful analysis of the Ekedahl-Oort strata in dimension $g = 4$; in Proposition 5.13 we show precisely how the Ekedahl-Oort strata and Newton strata intersect. It is worth mentioning that we don't use any computers in this paper (unlike most papers that treat the Gauss problem); the only numerical data we use is the well-known table in Subsection 2.3.

In the course of our proof of Theorem A, we define the notion of minimal E-isogenies (Definition 4.13). This generalises the notion of minimal isogenies for supersingular abelian varieties in the sense of Oort [31, Section 1.8]. This new construction of minimal isogenies even shows a new (and stronger) universal property for minimal isogenies since the test object is not required to be an isogeny; see Remark 4.14. We also extend the results of Jordan et al. [22] on abelian varieties isogenous to a power of an elliptic curve to those with a polorisation; see Corollary 4.6 and Theorem 4.22.

We remark on some clear connections between the arithmetic and the geometric setting. By the Albert classification of division algebras, the endomorphism algebra $B = \mathrm{End}^0(A)$ of any simple abelian variety A over any field K is either a totally real field F, a quaternion algebra over F (totally definite or totally indefinite), or a central division algebra over a CM field over F. The results in Subsection 2.1 apply to all these classes of algebras, except for totally indefinite quaternion algebras and non-commutative central division algebras over a CM field. Notably, Theorem 2.1 provides a very general statement about unique orthogonal decomposition of lattices, which enables us to compute the automorphism groups of such lattices via Corollary 2.2. On the geometric side (in Section 4), we obtain general unique decomposition results for abelian varieties which are isomorphic to a power of an elliptic curve (therefore including superspecial abelian varieties), since only these abelian varieties admit a natural description in terms of lattices, as was investigated in [37, 7.12-7.14].

On the other hand, on the geometric side we are mostly interested in supersingular abelian varieties, which are by definition isogenous to a power of a supersingular elliptic curve; hence, the most important algebras for us to study are the definite quaternion $\mathbb{Q}$-algebras $B = \mathrm{End}^0(E)$ for some supersingular elliptic curve E over an algebraic closed field. We specialise to these algebras in the remaining arithmetic parts (Subsections 2.2 and 2.3) and solve the arithmetic Gauss problem for these in Theorem 2.9. And indeed, we solve the geometric Gauss problem for all supersingular abelian varieties, including those which are not directly governed by lattices.

Finally, for solving the arithmetic Gauss problem, we restrict to maximal lattices for the maximal order O in a definite quaternion $\mathbb{Q}$-algebra B. When $B = \mathrm{End}^0(E)$ and $O = \mathrm{End}(E)$ as above, on the geometric side these lattices correspond to polarised superspecial abelian varieties in either the principal genus or the non-principal genus; see Corollary 4.9. This is how we can reduce our geometric Gauss problem immediately to the lower-dimensional cases ($g \leq 4$). On the other hand, when B is a more general definite $\mathbb{Q}$-algebra, this provides an extension of our geometric Gauss problem from Siegel modular varieties to fake Siegel modular varieties, which are direct generalisations of fake modular curves (that is, Shimura curves).

The structure of the paper is as follows. The arithmetic theory is treated in Section 2, building up to the main result in Theorem 2.9. Theorem 2.1 is the unique orthogonal decomposition result for lattices, and Corollary 2.2 gives its consequence for automorphism groups of such lattices. The geometric theory starts in Section 3, which recalls mass formulae due to the second and third authors as well as other authors. Section 4 treats automorphism groups and provides the geometric analogue of the unique decomposition results in Subsection 2.1, including their consequence for the determination of automorphism groups in Corollary 4.8. Finally, Section 5 solves the geometric Gauss problem for central leaves (Theorem 5.20), using mass formulae for the case $g = 3$ (Subsection 5.2) and explicit computations on Ekedahl-Oort strata for the hardest case $g = 4$ (Subsection 5.3).

1.1. **Acknowledgements.** The first author is supported by JSPS Kakenhi Grant Number JP19K-03424. The second author is supported by the Dutch Research Council (NWO) through grant VI.Veni.192.038. The third author is partially supported by the MoST grant 109-2115-M-001-002-MY3.

2. The arithmetic theory

2.1. **Uniqueness of orthogonal decomposition.**

Let F be a totally real algebraic number field, and let B be either F itself, a CM field over F (i.e., a totally imaginary quadratic extension of F), or a totally definite quaternion algebra

over F (i.e., such that any simple component of $B\otimes\mathbb{R}$ is a division algebra). We may regard B^n as a left B-vector space. As a vector space over F, we see that B^n can be identified with F^{en}, where $e = 1$, 2, or 4 according the choice of B made above. Let O_F be the ring of integers of F. A lattice in B^n is a finitely generated $\mathbb{Z}$-submodule $L \subseteq B^n$ such that $\mathbb{Q}L = B^n$ (i.e., L contains a basis of B^n over $\mathbb{Q}$); it is called an O_F-lattice if $O_F L \subseteq L$. A unitary subring $\mathscr{O}$ of B is called an order of B if it is a lattice in B; $\mathscr{O}$ is called an O_F-order if $\mathscr{O}$ also contains O_F. Any element of $\mathscr{O}$ is integral over O_F.

We fix an order $\mathscr{O}$ of B. Put $V = B^n$ and let $f : V \times V \to B$ be a quadratic form, a Hermitian form, or a quaternion Hermitian form according to whether $B = F$, B is CM, or B is quaternionic. This means that f satisfies

$$\begin{aligned} f(ax, y) &= af(x, y) && \text{for any } x, y \in V, a \in B, \\ f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y) && \text{for any } x_i, y \in V, \\ f(y, x) &= f(x, y)^* && \text{for any } x, y \in V, \end{aligned} \tag{2}$$

where $*$ is the main involution of B over F, that is, the trivial map for F, the complex conjugation for a fixed embedding $B \subseteq \mathbb{C}$ if B is a CM field, or the anti-automorphism of B of order 2 such that $x + x^* = Tr_{B/F}(x)$ for the reduced trace $\mathrm{Tr}_{B/F}$. By the above properties, we have $f(x, x) \in F$ for any $x \in V$. We assume that f is totally positive, that is, for any $x \in V$ and for any embedding $\sigma : F \to \mathbb{R}$, we have $f(x, x)^\sigma > 0$ unless $x = 0$. A lattice $L \subseteq V$ is said to be a left $\mathscr{O}$-lattice if $\mathscr{O}L \subseteq L$. An $\mathscr{O}$-submodule M of an $\mathscr{O}$-lattice L is called an $\mathscr{O}$-sublattice of L; then M is an $\mathscr{O}$-lattice in the B-module BM of possibly smaller rank. We say that a left $\mathscr{O}$-lattice $L \neq 0$ is indecomposable if whenever $L = L_1 + L_2$ and $f(L_1, L_2) = 0$ for some left $\mathscr{O}$-lattices L_1 and L_2, then $L_1 = 0$ or $L_2 = 0$.

For quadratic forms over $\mathbb{Q}$, the following theorem is in [27, p. 169 Theorem 6.7.1] and [28, Satz 27.2]. The proof for the general case is almost the same.

Theorem 2.1. *Assumptions and notation being as above, any left $\mathscr{O}$-lattice $L \subseteq B^n$ has a finite orthogonal decomposition*

$$L = L_1 \perp \cdots \perp L_r$$

for some indecomposable left $\mathscr{O}$-sublattices L_i. The set of lattices $\{L_i\}_{1\le i\le r}$ is uniquely determined by L.

Proof of Theorem 2.1. Any non-zero $x \in L$ is called primitive if there are no y,$z \in L$ such that $y \neq 0$, $z \neq 0$, and $x = y + z$ with $f(y, z) = 0$. First we see that any $0 \neq x \in L$ is a finite sum of primitive elements of L. If x is not primitive, then we have $x = y + z$ with $0 \neq y$, $z \in L$ with $f(y, z) = 0$. So we have $f(x, x) = f(y, y) + f(z, z)$ and hence

$$\mathrm{Tr}_{F/\mathbb{Q}}(f(x, x)) = \mathrm{Tr}_{F/\mathbb{Q}}(f(y, y)) + \mathrm{Tr}_{F/\mathbb{Q}}(f(z, z)).$$

Since f is totally positive, we have $\mathrm{Tr}_{F/\mathbb{Q}}(f(x, x)) = \sum_{\sigma:F\to\mathbb{R}} f(x, x)^\sigma = 0$ if and only if $x = 0$. So we have $\mathrm{Tr}_{F/\mathbb{Q}}(f(y, y)) < \mathrm{Tr}_{F/\mathbb{Q}}(f(x, x))$. If y is not primitive, we continue the same process. We claim that this process terminates after finitely many steps. Since $L \neq 0$ is a finitely generated $\mathbb{Z}$-module, $f(L, L)$ is a non-zero finitely generated $\mathbb{Z}$-module. So the module $\mathrm{Tr}_{F/\mathbb{Q}}(f(L, L))$ is a fractional ideal of $\mathbb{Z}$ and we have $\mathrm{Tr}_{F/\mathbb{Q}}(f(L, L)) = e\mathbb{Z}$ for some $0 < e \in \mathbb{Q}$. This means that $\mathrm{Tr}_{F/\mathbb{Q}}(f(x, x)) \in e\mathbb{Z}_{>0}$ for any $x \in L$. So after finitely many iterations, $\mathrm{Tr}_{F/\mathbb{Q}}(f(y, y))$ becomes 0 and the claim is proved.

We say that primitive elements x, $y \in L$ are connected if there are primitive elements z_1, z_2, …, $z_r \in L$ such that $x = z_0$, $y = z_r$, and $f(z_{i-1}, z_i) \neq 0$ for $i = 1,\ldots, r$. This is an equivalence relation. We denote by K_λ ($\lambda \in \Lambda$) the set of equivalence classes of primitive elements in L. By definition, elements of K_λ and K_κ for $\lambda \neq \kappa$ are orthogonal. We denote by L_λ the left

$\mathscr{O}$-module spanned by elements of K_λ. Then we have

$$L = \perp_{\lambda\in\Lambda} L_\lambda.$$

Since $F\mathscr{O} = B$, we see that $V_\lambda = FL_\lambda$ is a left B-vector space and L_λ is an $\mathscr{O}$-lattice in V_λ. Since $\dim_B \sum_{\lambda\in\Lambda} V_\lambda = n$, we see that Λ is a finite set. Hence any primitive element in L_λ belongs to K_λ. Indeed, if $y \in L_\lambda \subseteq L$ is primitive, then $y \in K_\mu$ for some $\mu \in \Lambda$, but if $\lambda \neq \mu$, then $y \in K_\mu \subseteq L_\mu$, so $y = 0$, a contradiction. Now if $L_\lambda = N_1 \perp N_2$ for some left $\mathscr{O}$-modules $N_1 \neq 0$, $N_2 \neq 0$, then whenever $x + y$ with $x \in N_1$, $y \in N_2$ is primitive, we have $x = 0$ or $y = 0$. So if $0 \neq x \in N_1$ is primitive and if $f(x, z_1) \neq 0$ for some primitive element $z_1 \in L_\lambda$, then $z_1 \in N_1$. Repeating the process, any $y \in K_\lambda$ belongs to N_1, so $N_1 = L_\lambda$, so L_λ is indecomposable. Now if $L = \perp_{\kappa\in K} M_\kappa$ for other indecomposable lattices, then any primitive element x of L is contained in some M_κ by definition of primitivity. By the same reasoning as before, if $x \in M_\kappa$ is primitive, then any primitive $y \in L$ connected to x belongs to M_κ. This means that there is a injection $\iota : \Lambda \to K$ such that $L_\lambda \subseteq M_{\iota(\lambda)}$. Since

$$L = \perp_{\lambda\in\Lambda} L_\lambda \subseteq \perp_{\lambda\in\Lambda} M_{\iota(\lambda)} \subseteq L$$

we have $L_\lambda = M_{\iota(\lambda)}$ and ι is a bijection. □

Corollary 2.2. *Assumptions and notation being as before, suppose that L has an orthogonal decomposition*

$$L = \perp_{i=1}^{r} M_i$$

where $M_i = \perp_{j=1}^{e_i} L_{ij}$ for some indecomposable left $\mathscr{O}$-lattices L_{ij} such that L_{ij} and $L_{ij'}$ are isometric for any j, j', but L_{ij} and $L_{i'j'}$ are not isometric for $i \neq i'$. Then we have

$$\mathrm{Aut}(L) \cong \prod_{i=1}^{r} \mathrm{Aut}(L_{i1})^{e_i} \cdot S_{e_i}$$

where S_{e_i} is the symmetric group on e_i letters and $\mathrm{Aut}(L_{i1})^{e_i} \cdot S_{e_i}$ is a semi-direct product where S_{e_i} normalises $\mathrm{Aut}(L_{i1})^{e_i}$.

Proof. By Theorem 2.1, we see that for any element $\epsilon \in \mathrm{Aut}(L)$, there exists $\tau \in S_{e_i}$ such that $\epsilon(L_{i1}) = L_{i\tau(1)}$, so the result follows. □

Remark 2.3. The proof of Theorem 2.1 also works in the following more general setting: $B = \prod_i B_i$ is a finite product of $\mathbb{Q}$-algebras B_i, where B_i is either a totally real field F_i, a CM field over F_i, or a totally definite quaternion algebra over F_i. Denote by $*$ the main involution on B and $F = \prod_i F_i$ the subalgebra fixed by $*$. Let $\mathscr{O}$ be any order in B, and let V be a faithful left B-module equipped with a totally positive Hermitian form f, which satisfies the conditions in (2) and is totally positive on each factor in $V = \oplus V_i$ with respect to $F = \prod_i F_i$.

2.2. **Quaternionic unitary groups and mass formulae.**

For the rest of this section, we let B be a definite quaternion $\mathbb{Q}$-algebra central over $\mathbb{Q}$ with discriminant D and let O be a maximal order in B. Then $D = q_1 \cdots q_t$ is a product of an odd number t of primes. The canonical involution on B is denoted by $x \mapsto \bar{x}$. Let (V, f) be a positive-definite quaternion Hermitian space over B of rank n. By definition, $f : V \times V \to B$ is a $\mathbb{Q}$-bilinear form such that

(i) $f(ax, y) = af(x, y)$ and $f(x, ay) = f(x, y)\bar{a}$,
(ii) $f(y, x) = \overline{f(x, y)}$, and
(iii) $f(x, x) \geq 0$ and $f(x, x) = 0$ only when $x = 0$,

for all $a \in B$ and $x, y \in V$. The isomorphism class of (V, f) over B is uniquely determined by $\dim_B V$. We denote by $G = G(V, f)$ the group of all similitudes on (V, f); namely,

$$G = \{\alpha \in \mathrm{GL}_B(V) : f(x\alpha, y\alpha) = n(\alpha)f(x, y) \quad \forall\, x, y \in V\ \},$$

where $n(\alpha) \in \mathbb{Q}^\times$ is a scalar depending only on α. For each prime p, we write $O_p := O \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $V_p := V \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and let $G_p = G(V_p, f_p)$ be the group of all similitudes on the local quaternion Hermitian space (V_p, f_p).

Two O-lattices L_1 and L_2 are said to be equivalent, denoted $L_1 \sim L_2$, if there exists an element $\alpha \in G$ such that $L_2 = L_1\alpha$; the equivalence of two O_p-lattices is defined analogously. Two O-lattices L_1 and L_2 are said to be in the same genus if $(L_1)_p \sim (L_2)_p$ for all primes p. The norm $N(L)$ of an O-lattice L is defined to be the two-sided fractional O-ideal generated by $f(x, y)$ for all $x, y \in L$. If L is maximal among the O-lattices having the same norm $N(L)$, then it is called a maximal O-lattice. The notion of maximal O_p-lattices in V_p is defined analogously. Then an O-lattice L is maximal if and only if the O_p-lattice $L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is maximal for all prime numbers p.

For each prime p, if $p \nmid D$, then there is only one equivalence class of maximal O_p-lattices in V_p, represented by the standard unimodular lattice $(O_p^n, f = \mathbb{I}_n)$. If $p|D$, then there are two equivalence classes of maximal O_p-lattices in V_p, represented by the principal lattice $(O_p^n, f = \mathbb{I}_n)$ and a non-principal lattice $((\Pi_p O_p)^{\oplus(n-c)} \oplus O_p^{\oplus c}, \mathbb{J}_n)$, respectively, where $c = \lfloor n/2 \rfloor$, and Π_p is a uniformising element in O_p with $\Pi_p\overline{\Pi}_p = p$, and $\mathbb{J}_n = \text{anti-diag}(1, \ldots, 1)$ is the anti-diagonal matrix of size n. Thus, there are 2^t genera of maximal O-lattices in V when $n \geq 2$.

For each positive integer n and a pair (D_1, D_2) of positive integers with $D = D_1D_2$, denote by $\mathscr{L}_n(D_1, D_2)$ the genus consisting of maximal O-lattices in (V, f) of rank n such that for all primes $p|D_1$ (resp. $p|D_2$) the O_p-lattice (L_p, f) belongs to the principal class (resp. the non-principal class). We denote by $[\mathscr{L}_n(D_1, D_2)]$ the set of equivalence classes of lattices in $\mathscr{L}_n(D_1, D_2)$ and by $H_n(D_1, D_2) := \#[\mathscr{L}_n(D_1, D_2)]$ the class number of the genus $\mathscr{L}_n(D_1, D_2)$. The mass $M_n(D_1, D_2)$ of $[\mathscr{L}_n(D_1, D_2)]$ is defined by

$$M_n(D_1, D_2) = \text{Mass}([\mathscr{L}_n(D_1, D_2)]) := \sum_{L \in [\mathscr{L}_n(D_1, D_2)]} \frac{1}{|\operatorname{Aut}(L)|}, \tag{3}$$

where $\operatorname{Aut}(L) := \{\alpha \in G : L\alpha = L\}$. Note that if $\alpha \in \operatorname{Aut}(L)$ then $n(\alpha) = 1$, because $n(\alpha) > 0$ and $n(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$.

Let $G^1 := \{\alpha \in G : n(\alpha) = 1\}$. The class number and mass for a G^1-genus of O-lattices are defined analogously to the case of G: two O-lattices L_1 and L_2 are said to be isomorphic, denoted $L_1 \simeq L_2$, if there exists an element $\alpha \in G^1$ such that $L_2 = L_1\alpha$; similarly, two O_p-lattices $L_{1,p}$ and $L_{2,p}$ are said to be isomorphic, denoted $L_{1,p} \simeq L_{2,p}$ if there exists an element $\alpha_p \in G_p^1$ such that $L_{2,p} = L_{1,p}\alpha_p$. Two O-lattices L_1 and L_2 are said to be in the same G^1-genus if $(L_1)_p \simeq (L_2)_p$ for all primes p. We denote by $\mathscr{L}_n^1(D_1, D_2)$ the G^1-genus which consists of maximal O-lattices in (V, f) of rank n satisfying

$$(V_p, f_p) \simeq \begin{cases} (O_p^n, \mathbb{I}_n) & \text{for } p \nmid D_2; \\ ((\Pi_p O_p)^{n-c} \oplus O_p^c, \mathbb{J}_n) & \text{for } p \mid D_2, \end{cases}$$

where $c := \lfloor n/2 \rfloor$. We denote by $[\mathscr{L}_n^1(D_1, D_2)]$ the set of isomorphism classes of O-lattices in $\mathscr{L}_n^1(D_1, D_2)$ and by $H_n^1(D_1, D_2) := \#[\mathscr{L}_n^1(D_1, D_2)]$ the class number of the G^1-genus $\mathscr{L}_n^1(D_1, D_2)$. Similarly, the mass $M_n^1(D_1, D_2)$ of $[\mathscr{L}_n^1(D_1, D_2)]$ is defined by

$$M_n^1(D_1, D_2) = \text{Mass}([\mathscr{L}_n^1(D_1, D_2)]) := \sum_{L \in [\mathscr{L}_n^1(D_1, D_2)]} \frac{1}{|\operatorname{Aut}_{G^1}(L)|}, \tag{4}$$

where $\operatorname{Aut}_{G^1}(L) := \{\alpha \in G^1 : L\alpha = L\}$, which is also equal to $\operatorname{Aut}(L)$.

Lemma 2.4. *The natural map $\iota : [\mathscr{L}_n^1(D_1, D_2)] \to [\mathscr{L}_n(D_1, D_2)]$ is a bijection. In particular, we have the equalities*

$$M_n^1(D_1, D_2) = M_n(D_1, D_2) \quad \textit{and} \quad H_n^1(D_1, D_2) = H_n(D_1, D_2). \tag{5}$$

Proof. Fix an O-lattice L_0 in $\mathscr{L}_n(D_1, D_2)$ and regard G and G^1 as algebraic groups over $\mathbb{Q}$. Denote by $\widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ the profinite completion of $\mathbb{Z}$ and by $\mathbb{A}_f = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ the finite adele ring of $\mathbb{Q}$. We have natural isomorphisms of pointed sets

$$[\mathscr{L}_n(D_1, D_2)] \simeq U \backslash G(\mathbb{A}_f)/G(\mathbb{Q}), \quad [\mathscr{L}_n^1(D_1, D_2)] \simeq U^1 \backslash G^1(\mathbb{A}_f)/G^1(\mathbb{Q}),$$

where U is the stabiliser of $L_0 \otimes \widehat{\mathbb{Z}}$ in $G(\mathbb{A}_f)$ and $U^1 := U \cap G^1(\mathbb{A}_f)$. Via these isomorphisms, the natural map $\iota : [\mathscr{L}_n^1(D_1, D_2)] \to [\mathscr{L}_n(D_1, D_2)]$ is nothing but the map induced by the identity map

$$\iota : U^1 \backslash G^1(\mathbb{A}_f)/G^1(\mathbb{Q}) \to U \backslash G(\mathbb{A}_f)/G(\mathbb{Q}).$$

The map n induces a surjective map $U \backslash G(\mathbb{A}_f)/G(\mathbb{Q}) \to n(U) \backslash \mathbb{A}_f^\times / \mathbb{Q}_+^\times$. One shows that $n(U) = \widehat{\mathbb{Z}}^\times$ so the latter term is trivial. Then every double coset in $U \backslash G(\mathbb{A}_f)/G(\mathbb{Q})$ is presented by an element of norm one. Therefore, ι is surjective. Let $g_1, g_2 \in G^1(\mathbb{A}_f)$ such that $\iota[g_1] = \iota[g_2]$ in the G-double coset space. Then $g_1 = u g_2 \gamma$ for some $u \in U$ and $\gamma \in G(\mathbb{Q})$. Applying n, one obtains $n(\gamma) = 1$ and hence $n(u) = 1$. This proves the injectivity of ι. □

For each $n \geq 1$, define

$$v_n := \prod_{i=1}^{n} \frac{|\zeta(1-2i)|}{2}, \tag{6}$$

where $\zeta(s)$ is the Riemann zeta function. For each prime p and $n \geq 1$, define

$$L_n(p, 1) := \prod_{i=1}^{n} (p^i + (-1)^i) \tag{7}$$

and

$$L_n(1, p) := \begin{cases} \prod_{i=1}^{c} (p^{4i-2} - 1) & \text{if } n = 2c \text{ is even;} \\ \frac{(p-1)(p^{4c+2}-1)}{p^2-1} \cdot \prod_{1=1}^{c} (p^{4i-2} - 1) & \text{if } n = 2c+1 \text{ is odd.} \end{cases} \tag{8}$$

Proposition 2.5. *We have*

$$M_n(D_1, D_2) = v_n \cdot \prod_{p | D_1} L_n(p, 1) \cdot \prod_{p | D_2} L_n(1, p). \tag{9}$$

Proof. When $(D_1, D_2) = (D, 1)$, the formula (9) is proved in [16, Proposition 9]. By Lemma (2.4), we may replace $M_n(D_1, D_2)$ by $M_n^1(D_1, D_2)$ in (9). We have

$$\frac{M_n^1(D_1, D_2)}{M_n^1(D, 1)} = \prod_{p | D_2} \frac{\mathrm{vol}(\mathrm{Aut}_{G_p^1}(O_p^n, \mathbb{I}_n))}{\mathrm{vol}(\mathrm{Aut}_{G_p^1}((\Pi_p O_p)^{n-c} \oplus O_p^c, \mathbb{J}_n))}, \tag{10}$$

where $c = \lfloor n/2 \rfloor$ and where $\mathrm{vol}(U_p)$ denotes the volume of an open compact subgroup $U_p \subseteq G_p^1$ for a Haar measure on G_p^1. The right hand side of (10) does not depend on the choice of the Haar measure. It is easy to see that the dual lattice $((\Pi_p O_p)^{n-c} \oplus O_p^c)^\vee$ of $(\Pi_p O_p)^{n-c} \oplus O_p^c$ with respect to $\mathbb{J}_n$ is equal to $O_p^c \oplus (\Pi_p^{-1} O_p)^{n-c}$. Therefore,

$$\mathrm{Aut}_{G_p^1}((\Pi_p O_p)^{n-c} \oplus O_p^c, \mathbb{J}_n) = \mathrm{Aut}_{G_p^1}((\Pi_p O_p)^c \oplus O_p^{n-c}, \mathbb{J}_n).$$

On the other hand, in the notation of Theorem 3.1, we have

$$\frac{\mathrm{vol}(\mathrm{Aut}_{G_p^1}(O_p^n, \mathbb{I}_n))}{\mathrm{vol}(\mathrm{Aut}_{G_p^1}((\Pi_p O_p)^c \oplus O_p^{n-c} c, \mathbb{J}_n))} = \frac{\mathrm{Mass}(\Lambda_{n,p^c})}{\mathrm{Mass}(\Lambda_{n,p^0})} = \frac{L_{n,p^c}}{L_{n,p^0}} = \frac{L_n(1,p)}{L_n(p,1)} \tag{11}$$

by (24). Then the formula (9) follows from (10), (11) and (9) for $(D_1, D_2) = (D, 1)$. □

2.3. **The Gauss problem for definite quaternion Hermitian maximal lattices.**

In this subsection we determine for which n and (D_1, D_2) the class number $H_n(D_1, D_2)$ is equal to one. The Bernoulli numbers B_n are defined by (cf. [43, p. 91])

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + \sum_{n=1}^{\infty} B_{2n} \frac{t^{2n}}{(2n)!}. \tag{12}$$

For each $n \geq 1$, we have

$$B_{2n} = (-1)^{(n+1)} \frac{2(2n)!}{(2\pi)^{2n}} \zeta(2n) \tag{13}$$

and

$$\frac{|\zeta(1-2n)|}{2} = \frac{|B_{2n}|}{4n} = \frac{(2n-1)!\zeta(2n)}{(2\pi)^{2n}}. \tag{14}$$

Below is a table of values of $|B_{2n}|$ and $|\zeta(1-2n)|/2$:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\lvert B_{2n}\rvert$	$\frac{1}{6}$	$\frac{1}{30}$	$\frac{1}{42}$	$\frac{1}{30}$	$\frac{5}{66}$	$\frac{691}{2730}$	$\frac{7}{6}$	$\frac{3617}{510}$	$\frac{43867}{798}$	$\frac{174611}{330}$	$\frac{864513}{138}$	$\frac{236364091}{2730}$
$\frac{\lvert\zeta(1-2n)\rvert}{2}$	$\frac{1}{24}$	$\frac{1}{240}$	$\frac{1}{504}$	$\frac{1}{480}$	$\frac{1}{264}$	$\frac{691}{2730\cdot 24}$	$\frac{1}{24}$	$\frac{3617}{510\cdot 32}$	$\frac{43867}{798\cdot 36}$	$\frac{174611}{330\cdot 40}$	$\frac{864513}{138\cdot 44}$	$\frac{236364091}{2730\cdot 48}$
$\frac{\lvert\zeta(1-2n)\rvert}{2}$	$\frac{1}{24}$	$\frac{1}{240}$	$\frac{1}{504}$	$\frac{1}{480}$	$\frac{1}{264}$	$\frac{691}{2730\cdot 24}$	$\frac{1}{24}$	0.222	1.527	13.228	142.38	1803.8

We have (cf. (6))

$$\begin{aligned} v_1 &= \frac{1}{2^3 \cdot 3}, \quad v_2 = \frac{1}{2^7 \cdot 3^2 \cdot 5}, \quad v_3 = \frac{1}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}, \\ v_4 &= \frac{1}{2^{15} \cdot 3^5 \cdot 5^2 \cdot 7}, \quad v_5 = \frac{1}{2^{18} \cdot 3^6 \cdot 5^2 \cdot 7 \cdot 11}. \end{aligned} \tag{15}$$

Lemma 2.6. *If $n \geq 6$, then either the numerator of v_n is not one or $v_n > 1$.*

Proof. Put $A_n = |\zeta(1-2n)|/2$. First, by

$$\zeta(2n) < 1 + \int_2^{\infty} \frac{1}{x^{2n}} dx = 1 + \frac{1}{2^{2n+1}},$$

we have

$$\frac{A_{n+1}}{A_n} > \frac{(2n+1)(2n)}{(2\pi)^2 \cdot \zeta(2n)} > \left(\frac{2n}{2\pi}\right)^2 \cdot \frac{1 + \frac{1}{2n}}{1 + \frac{1}{2^{2n+1}}} > 1 \quad \text{for } n \geq 3.$$

From the table and the fact that A_n is increasing for $n \geq 4$ which we have just proved, we have

$$v_n = \prod_{i=1}^{6} A_i \cdot \prod_{i=7}^{11} A_i \cdot \prod_{i=12}^{n} A_i > \frac{1}{504^6} \cdot 1 \cdot (1803)^{n-11} \quad \text{for } n \geq 12.$$

Thus, $v_n > 1$ for $n \geq 17$.

By a classical result of Clausen and von Staudt (see [3, Theorem 3.1, p. 41]), $B_{2n} \equiv -\sum_{p-1|2n} (1/p) \mod 1$ where p are primes. So if $n \leq 17$ (even for $n \leq 344$), then B_{2n} has denominators only for primes such that $p - 1 \leq 34$ (or $p - 1 \leq 344 \cdot 2$) and this does not include 691. Thus, for $6 \leq n \leq 344$, we have $691 | v_n$. This proves the lemma. □

Corollary 2.7. *For $n \geq 6$, we have $H_n(D_1, D_2) > 1$.*

Proof. By Lemma 2.6, either $v_n > 1$ or the numerator of v_n is not one. From the mass formula (3), either $M_n(D_1, D_2) > 1$ or the numerator of $M_n(D_1, D_2)$ is not one. Therefore, $H_n(D_1, D_2) > 1$. □

Proposition 2.8. *We have $H_3(2,1) = 1$, $H_3(1,2) = 1$, and $H_4(1,2) = 1$.*

Proof. It follows from Proposition 2.5 and Equations (8) and (15) that

$$M_3(1,2) = \frac{1}{2^{10} \cdot 3^2 \cdot 5} \qquad \text{and} \qquad M_4(1,2) = \frac{1}{2^{15} \cdot 3^2 \cdot 5^2}.$$

It follows from [21, Section 5] that the unique lattice (L, h) in the non-principal genus $H_2(1,2)$ has an automorphism group of cardinality $1920 = 2^7 \cdot 3 \cdot 5$.

Consider the lattice $(O, p\mathbb{I}_1) \oplus (L, h)$ contained in $\mathscr{L}_3(1,2)$. By Corollary 2.2 we see that

$$\mathrm{Aut}((O, p\mathbb{I}_1) \oplus (L, h)) \simeq \mathrm{Aut}((O, p\mathbb{I}_1)) \cdot \mathrm{Aut}((L, h)) = O^\times \cdot \mathrm{Aut}((L, h)).$$

Since $O^\times = E_{24} \simeq \mathrm{SL}_2(\mathbb{F}_3)$ has cardinality 24 (cf. [23, Equation (57)]), it follows that

$$|\mathrm{Aut}((O, p\mathbb{I}_1) \oplus (L, h))| = 24 \cdot 1920 = 2^{10} \cdot 3^2 \cdot 5 = \frac{1}{M_3(1,2)},$$

showing that the lattice $(O, p\mathbb{I}_1) \oplus (L, h)$ is unique and hence that $H_3(1,2) = 1$.

Next, consider the lattice $(L, h)^{\oplus 2}$ contained in $\mathscr{L}_4(1,2)$. Again by Corollary 2.2 we see that

$$\mathrm{Aut}((L, h)^{\oplus 2}) \simeq \mathrm{Aut}((L, h))^2 \cdot C_2$$

which has cardinality

$$1920^2 \cdot 2 = 2^{15} \cdot 3^2 \cdot 5^2 = \frac{1}{M_4(1,2)},$$

showing that also $(L, h)^{\oplus 2}$ is unique and therefore $H_4(1,2) = 1$. Finally, we compute that

$$M_3(2,1) = \frac{1}{2^{10} \cdot 3^4} = \frac{1}{24^3 \cdot 3!} = \frac{1}{|\mathrm{Aut}(O^3, \mathbb{I}_3)|}, \text{ and therefore } H_3(2,1) = 1.$$

□

Theorem 2.9. *The class number $H_n(D_1, D_2)$ is equal to one if and only if $D = p$ is a prime number and one of the following holds:*

(1) *$n = 1$, $(D_1, D_2) = (p, 1)$ and $p \in \{2, 3, 5, 7, 13\}$;*
(2) *$n = 2$, and either $(D_1, D_2) = (p, 1)$ with $p = 2, 3$ or $(D_1, D_2) = (1, p)$ with $p \in \{2, 3, 5, 7, 11\}$;*
(3) *$n = 3$, and either $(D_1, D_2) = (2, 1)$ or $(D_1, D_2) = (1, 2)$;*
(4) *$n = 4$ and $(D_1, D_2) = (1, 2)$.*

Proof. (1) When $n = 1$ we only have the principal genus class number and $H_1(D, 1)$ is the class number $h(B)$ of B. The corresponding Gauss problem is a classical result: $h(B) = 1$ if and only if $D \in \{2, 3, 5, 7, 13\}$; see the list in [44, p. 155]. We give an alternative proof of this fact for the reader's convenience. Suppose that $H_1(D, 1) = 1$. Then

$$M_1(D,1) = \frac{\prod_{p|D}(p-1)}{24} = \frac{1}{m}, \quad \text{where } m \in 2\mathbb{N}. \tag{16}$$

The discriminant D has an odd number of prime divisors, since B is a definite quaternion algebra. That the numerator of $M_1(D, 1)$ is 1 implies that every prime factor p of D must satisfy $(p-1)|24$ and hence $p \in \{2, 3, 5, 7, 13\}$. Suppose that D has more

than one prime divisor; using the condition (16), D must then be $2 \cdot 3 \cdot 7 = 42$. Using the class number formula (see [9, 44], cf. Pizer [40, Theorem 16, p. 68])

$$H_1(D,1) = \frac{\prod_{p|D}(p-1)}{12} + \frac{1}{4}\prod_{p|D}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\prod_{p|D}\left(1 - \left(\frac{-3}{p}\right)\right),$$

we calculate that $H_1(42,1) = 2$. Hence, D must be a prime p, which is in $\{2,3,5,7,13\}$. Conversely, we check that $H_1(p,1) = 1$ for these primes.

(2) See Hashimoto-Ibukiyama [16, p. 595], [17, p. 696]. One may still want to verify $H_2(D_1,D_2) > 1$ for pairs (D_1,D_2) not in the data there. Using the class number formula in [17] we compute that $M_2(1, 2\cdot 3\cdot 11) = 1/2$ and $H_2(1, 2\cdot 3\cdot 11) = 9$. For the remaining cases, one can show that either the numerator of $M_2(D_1,D_2)$ is not equal to 1 or $M_2(D_1,D_2) > 1$, by the same argument as that used below for $n \geq 3$.

(3)+(4) The principal genus part for $n = 3$ with $D = p$ a prime is due to Hashimoto [15], based on an explicit class number formula. We shall prove directly that for $n \geq 3$, (3) and (4) are the only cases for which $H_n(D_1,D_2) = 1$. In particular, our proof of the principal genus part of (3) is independent of Hashimoto's result. By Corollary 2.7, it is enough to treat the cases $n = 3,4,5$, so we assume this. We have $L_{n+1}(p,1) = L_n(p,1)(p^{n+1} + (-1)^{n+1})$, and

$$L_2(1,p) = (p^2-1), \quad L_3(1,p) = (p-1)(p^6-1),$$
$$L_4(1,p) = (p^2-1)(p^6-1), \quad L_5(1,p) = (p-1)(p^6-1)(p^{10}-1).$$

In particular, (p^3-1) divides both $L_n(p,1)$ and $L_n(1,p)$ for $n = 3,4,5$. Observe that if $L_n(p,1)$ or $L_n(1,p)$ has a prime factor greater than 11, then $H_n(D_1,D_2) > 1$ for all (D_1,D_2) with $p|D_1D_2$; this follows from Proposition 2.5 and (15). We list a prime factor d of p^3-1 which is greater than 11:

p	3	5	7	11	13
$d \mid p^3-1$	13	31	19	19	61

Thus, $H_n(D_1,D_2) > 1$ for $n = 3,4,5$ and $p|D$ for some prime p with $3 \leq p \leq 13$. It remains to treat the cases $p \geq 17$ and $p = 2$. We compute that $M_3(17,1) \doteq 7.85$ and $M_4(1,17) \doteq 4.99$. One sees that $M_3(1,17) > M_3(17,1)$, $M_5(17,1) > M_3(17,1)$ and $M_4(17,1) > M_4(1,17)$. Therefore $M_n(p,1) > 1$ and $M_n(1,p) > 1$ for $p \geq 17$. Thus, $H_n(D_1,D_2) = 1$ implies that $D = 2$. One checks that $31|L_5(2,1)$, $31|L_5(1,2)$ and $17|L_4(2,1)$. Thus

$$H_5(2,1) > 1, \quad H_5(1,2) > 1, \quad \text{and} \quad H_4(2,1) > 1.$$

It remains to show that $H_3(2,1) = 1$, $H_3(1,2) = 1$ and $H_4(1,2) = 1$, which is done in Proposition 2.8.

□

3. The geometric theory: mass formulae and class numbers

3.1. **Set-up and definition of masses.**

For the remainder of this paper, let p be a prime number, let g be a positive integer, and let k be an algebraically closed field of characteristic p. Unless stated otherwise, k will be the field of definition of abelian varieties.

The cardinality of a finite set S will be denoted by $|S|$. Let α_p be the unique local-local finite group scheme of order p over $\mathbb{F}_p$; it is defined to be the kernel of the Frobenius morphism on the additive group $\mathbb{G}_a$ over $\mathbb{F}_p$. As before, denote by $\widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ the profinite completion of $\mathbb{Z}$ and by $\mathbb{A}_f = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ the finite adele ring of $\mathbb{Q}$. Let $B_{p,\infty}$ denote the definite quaternion $\mathbb{Q}$-algebra

of discriminant p. Fix a quaternion Hermitian $B_{p,\infty}$-space (V, f) of rank g, let $G = G(V, f)$ be the quaternion Hermitian group associated to (V, f) and $G^1 \subseteq G$ the subgroup consisting of elements $g \in G$ of norm $n(g) = 1$. We regard G^1 and G as algebraic groups over $\mathbb{Q}$.

For any integer $d \geq 1$, let $\mathscr{A}_{g,d}$ denote the (coarse) moduli space over $\overline{\mathbb{F}}_p$ of g-dimensional polarised abelian varieties (X, λ) with polarisation degree $\deg(\lambda) = d^2$. An abelian variety over k is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves; it is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves. For any $m \geq 1$, let $\mathscr{S}_{g,p^m}$ be the supersingular locus of $\mathscr{A}_{g,p^m}$, which consists of all polarised supersingular abelian varieties in $\mathscr{A}_{g,p^m}$. Then $\mathscr{S}_g := \mathscr{S}_{g,1}$ is the moduli space of g-dimensional principally polarised supersingular abelian varieties.

If S is a finite set of objects with finite automorphism groups in a specified category, the *mass* of S is defined to be the weighted sum

$$\mathrm{Mass}(S) := \sum_{s \in S} \frac{1}{|\operatorname{Aut}(s)|}.$$

For any $x = (X_0, \lambda_0) \in \mathscr{S}_{g,p^m}(k)$, we define

$$\Lambda_x = \{(X, \lambda) \in \mathscr{S}_{g,p^m}(k) : (X, \lambda)[p^\infty] \simeq (X_0, \lambda_0)[p^\infty]\}, \tag{17}$$

where $(X, \lambda)[p^\infty]$ denotes the polarised p-divisible group associated to (X, λ). We define a group scheme G_x over $\mathbb{Z}$ as follows. For any commutative ring R, the group of its R-valued points is defined by

$$G_x(R) = \{\alpha \in (\mathrm{End}(X_0) \otimes_{\mathbb{Z}} R)^\times : \alpha^t \lambda_0 \alpha = \lambda_0\}. \tag{18}$$

Since any two polarised supersingular abelian varieties are isogenous, i.e., there exists a quasi-isogeny $\varphi : X_1 \to X_2$ such that $\varphi^* \lambda_2 = \lambda_1$, the algebraic group $G_x \otimes \mathbb{Q}$ is independent of x (up to isomorphism) and it is known to be isomorphic to G^1. We shall fix an isomorphism $G_x \otimes \mathbb{Q} \simeq G^1$ over $\mathbb{Q}$ and regard $U_x := G_x(\widehat{\mathbb{Z}})$ as an open compact subgroup of $G^1(\mathbb{A}_f)$. By [47, Theorem 2.1], there is a natural bijection between the following pointed sets:

$$\Lambda_x \simeq G^1(\mathbb{Q}) \backslash G^1(\mathbb{A}_f) / U_x. \tag{19}$$

In particular, Λ_x is a finite set. The mass of Λ_x is then defined as

$$\mathrm{Mass}(\Lambda_x) = \sum_{(X,\lambda) \in \Lambda_x} \frac{1}{|\mathrm{Aut}(X, \lambda)|}. \tag{20}$$

If U is an open compact subgroup of $G^1(\mathbb{A}_f)$, the *arithmetic mass* for (G^1, U) is defined by

$$\mathrm{Mass}(G^1, U) := \sum_{i=1}^{h} \frac{1}{|\Gamma_i|}, \quad \Gamma_i := G^1(\mathbb{Q}) \cap c_i U c_i^{-1}, \tag{21}$$

where $\{c_i\}_{i=1,\ldots,h}$ is a complete set of representatives of the double coset space $G^1(\mathbb{Q}) \backslash G^1(\mathbb{A}_f) / U$. The definition of $\mathrm{Mass}(G^1, U)$ is independent of the choices of representatives $\{c_i\}_i$. Then we have the equality (cf. [47, Corollary 2.5])

$$\mathrm{Mass}(\Lambda_x) = \mathrm{Mass}(G^1, U). \tag{22}$$

3.2. **Superspecial mass formulae.**

For each integer c with $0 \leq c \leq \lfloor g/2 \rfloor$, let Λ_{g,p^c} denote the set of isomorphism classes of g-dimensional polarised superspecial abelian varieties (X, λ) whose polarisation λ satisfies $\ker(\lambda) \simeq \alpha_p^{2c}$. The mass of Λ_{g,p^c} is

$$\mathrm{Mass}(\Lambda_{g,p^c}) = \sum_{(X,\lambda) \in \Lambda_{g,p^c}} \frac{1}{|\mathrm{Aut}(X, \lambda)|}.$$

Note that the p-divisible group of a superspecial abelian variety of given dimension is unique up to isomorphism. Furthermore, the polarised p-divisible group associated to any member in Λ_{g,p^c} is unique up to isomorphism, cf. [31, Proposition 6.1]. Therefore, if $x = (X_0, \lambda_0)$ is any member in Λ_{g,p^c}, then we have $\Lambda_x = \Lambda_{g,p^c}$ (cf. (17)). In particular, the mass $\mathrm{Mass}(\Lambda_{g,p^c})$ of the superspecial locus Λ_{g,p^c} is a special case of $\mathrm{Mass}(\Lambda_x)$.

We fix a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ such that its Frobenius endomorphism π_E satisfies $\pi_E = -p$, and let $E_k = E \otimes_{\mathbb{F}_{p^2}} k$. It is known that every polarisation on E_k^g is defined over $\mathbb{F}_{p^2}$, that is, it descends uniquely to a polarisation on E^g over $\mathbb{F}_{p^2}$. For each integer c with $0 \le c \le \lfloor g/2 \rfloor$, we denote by $P_{p^c}(E^g)$ the set of isomorphism classes of polarisations μ on E^g such that $\ker(\mu) \simeq \alpha_p^{2c}$; we define $P_{p^c}(E_k^g)$ similarly, and have the identification $P_{p^c}(E_k^g) = P_{p^c}(E^g)$. As superspecial abelian abelian varieties of dimension $g > 1$ are unique up to isomorphism, there is a bijection $P_{p^c}(E^g) \simeq \Lambda_{g,p^c}$ when $g > 1$. For brevity, we shall also write $P(E^g)$ for $P_1(E^g)$.

Theorem 3.1. *For any $g \ge 1$ and $0 \le c \le \lfloor g/2 \rfloor$, we have*

$$\mathrm{Mass}(\Lambda_{g,p^c}) = v_g \cdot L_{g,p^c},$$

where v_g is defined in (6) *and where*

$$L_{g,p^c} = \prod_{i=1}^{g-2c} (p^i + (-1)^i) \cdot \prod_{i=1}^{c} (p^{4i-2} - 1) \cdot \frac{\prod_{i=1}^{g} (p^{2i} - 1)}{\prod_{i=1}^{2c} (p^{2i} - 1) \prod_{i=1}^{g-2c} (p^{2i} - 1)}. \tag{23}$$

Proof. This follows from [14, Proposition 3.5.2] by the functional equation for $\zeta(s)$. See [10, p. 159] and [16, Proposition 9] for the case where $c = 0$ (the principal genus case). See also [48] for a geometric proof in the case where $g = 2c$ (the non-principal genus case). □

Clearly, $L_{g,p^0} = L_g(p, 1)$. One can also see from (23) that for $c = \lfloor g/2 \rfloor$,

$$L_{g,p^c} = \begin{cases} \prod_{i=1}^{c} (p^{4i-2} - 1) & \text{if } g = 2c \text{ is even;} \\ \frac{(p-1)(p^{4c+2}-1)}{p^2-1} \cdot \prod_{1=1}^{c} (p^{4i-2} - 1) & \text{if } g = 2c+1 \text{ is odd,} \end{cases} \tag{24}$$

and therefore $L_{g,p^c} = L_g(1, p)$, cf. (8). For $g = 5$ and $c = 1$, one has

$$\mathrm{Mass}(\Lambda_{5,p}) = v_5 \cdot (p-1)(p^2+1)(p^3-1)(p^4+1)(p^{10}-1), \tag{25}$$

noting that this case is different from either the principal genus or the non-principal genus case.

Lemma 3.2. *For any $g \ge 1$ and $0 \le c \le \lfloor g/2 \rfloor$, the local component L_{g,p^c} in* (23) *is a polynomial in p over $\mathbb{Z}$ of degree $(g^2 + 4gc - 8c^2 + g - 2c)/2$. Furthermore, the minimal degree occurs precisely when $c = 0$ if g is odd and when $c = g/2$ if g is even.*

Proof. It suffices to show that the term

$$A := \frac{\prod_{i=1}^{g} (p^{2i} - 1)}{\prod_{i=1}^{2c} (p^{2i} - 1) \prod_{i=1}^{g-2c} (p^{2i} - 1)}$$

is a polynomial in p with coefficients in $\mathbb{Z}$. Notice that $A = [g; 2c]_{p^2}$, where

$$[n; k]_q := \frac{\prod_{i=1}^{n} (q^i - 1)}{\prod_{i=1}^{k} (q^i - 1) \cdot \prod_{i=1}^{n-k} (q^i - 1)}, \quad n \in \mathbb{N},\ k = 0, \ldots, n.$$

It is known that $[n; k]_q \in \mathbb{Z}[q]$; cf. [11]. Alternatively, one considers the recursive relation $[n+1\ ;\ k]_q = [n; k]_q + q^{n-k+1}[n; k-1]_q$ and concludes that $[n, k]_q \in \mathbb{Z}[q]$ by induction.

The degree of L_{g,p^c} is

$$\begin{aligned}
&\sum_{i=1}^{g-2c} i + \sum_{i=1}^{c}(4i-2) + \sum_{i=g-2c+1}^{g} 2i - \sum_{i=1}^{2c} 2i \\
&= \frac{1}{2}\left[(g-2c)(g-2c+1) + c\cdot 4c + 2c\cdot(4g-4c+2) - 2c(4c+2)\right] \\
&= \frac{1}{2}\left[g^2 + 4gc - 8c^2 + g - 2c\right].
\end{aligned} \tag{26}$$

The degree is a polynomial function of degree 2 in c with negative leading coefficient. So the minimum occurs either at $c = 0$ or at $c = \lfloor g/2 \rfloor$; the former happens if g is odd and the latter happens if g is even. □

If $g = 2m$ is even, then the polynomial $L_{g,1}$ has degree $g(g+1)/2 = 2m^2 + m$ and L_{g,p^m} has degree $2m^2$.

3.3. **Mass formulae and class number formulae for supersingular abelian surfaces and threefolds.**

3.3.1. *Non-superspecial supersingular abelian surfaces.*

Let $x = (X_0, \lambda_0)$ be a principally polarised supersingular abelian surface over k. If X_0 is superspecial, then $\Lambda_x = \Lambda_{2,p^0}$ and the class number formula for $|\Lambda_{2,p^0}|$ is obtained in [16]. We assume that X_0 is not superspecial, that is, $a(X_0) = 1$. In this case there is a unique (up to isomorphism) polarised superspecial abelian surface (Y_1, λ_1) such that $\ker(\lambda_1) \simeq \alpha_p^2$ and an isogeny $\phi : (Y_1, \lambda_1) \to (X_0, \lambda_0)$ of degree p which is compatible with polarisations. Furthermore, there is a unique polarisation μ_1 on E^2 such that $\ker(\mu_1) \simeq \alpha_p^2$ such that $(Y_1, \lambda_1) \simeq (E^2, \mu_1) \otimes_{\mathbb{F}_{p^2}} k$. Then x corresponds to a point t in $\mathbb{P}^1(k) = \mathbb{P}^1_{\mu_1}(k) := \{\phi_1 : (E^2, \mu_1)\otimes k \to (X, \lambda)$ an isogeny of degree $p\}$, called the Moret-Bailly parameter for (X_0, λ_0).

The condition $a(X_0) = 1$ implies that $t \in \mathbb{P}^1(k) \setminus \mathbb{P}^1(\mathbb{F}_{p^2}) = k \setminus \mathbb{F}_{p^2}$. We consider two different cases, corresponding to the structures of $\mathrm{End}(X_0)$: the case $t \in k \setminus \mathbb{F}_{p^4}$, which we call the first case (I), and the case $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$, called the second case (II). The following explicit formula for the class number of a non-superspecial supersingular "genus" Λ_x is due to the first-named author [21].

Theorem 3.3. *Let $x = (X_0, \lambda_0)$ be a principally polarised supersingular abelian surface over k with $a(X_0) = 1$ and let h be the cardinality of Λ_x.*

(1) *In case (I), i.e., when $t \in k \setminus \mathbb{F}_{p^4}$, we have*

$$h = \begin{cases} 1 & \text{if } p = 2; \\ \frac{p^2(p^4-1)(p^2-1)}{5760} & \text{if } p \geq 3. \end{cases}$$

(2) *In case (II), i.e., when $t \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$, we have*

$$h = \begin{cases} 1 & \text{if } p = 2; \\ \frac{p^2(p^2-1)^2}{2880} & \text{if } p \equiv \pm 1 \bmod 5 \text{ or } p = 5; \\ 1 + \frac{(p-3)(p+3)(p^2-3p+8)(p^2+3p+8)}{2880} & \text{if } p \equiv \pm 2 \bmod 5. \end{cases}$$

(3) *For each case, we have $h = 1$ if and only if $p = 2, 3$.*

Proof. Parts (1) and (2) follow from Theorems 1.1 and 3.6 of [21]. Part (3) follows from the table in Section 1 of [21]. □

Theorem 3.4. *Let $x = (X_0, \lambda_0)$ and $t \in \mathbb{P}^1(k)$ be as in Theorem 3.3. Then*

$$\mathrm{Mass}(\Lambda_{x'}) = \frac{L_p}{5760}, \tag{27}$$

with

$$L_p = \begin{cases} (p^2-1)(p^4-p^2), & \text{if } t \in \mathbb{P}^1(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2}); \\ 2^{-e(p)}(p^4-1)(p^4-p^2) & \text{if } t \in \mathbb{P}^1(k) \setminus \mathbb{P}^1(\mathbb{F}_{p^4}), \end{cases}$$

where $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$.

Proof. See [51, Theorem 1.1]; also cf. [21, Proposition 3.3]. □

Corollary 3.5. *Let $p = 2$, and let $x' = (X', \lambda')$ be a principally polarised supersingular abelian surface over k with $a(X') = 1$. Let $\varphi : (E_k^2, \mu_1) \to (X', \lambda')$ be the minimal isogeny with Moret-Bailly parameter $t \in \mathbb{P}^1(k) - \mathbb{P}^1(\mathbb{F}_{p^2})$, where μ_1 is a polarisation on E^2 such that $\ker(\mu_1) \simeq \alpha_p^2$. Then*

$$|\operatorname{Aut}(X', \lambda')| = \begin{cases} 160, & \text{if } t \in \mathbb{P}^1(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2}); \\ 32 & \text{if } t \in \mathbb{P}^1(k) \setminus \mathbb{P}^1(\mathbb{F}_{p^4}). \end{cases} \tag{28}$$

Proof. By Theorem 3.3, we have $|\Lambda_{x'}| = 1$ in both cases. The mass formula (cf. Theorem 3.4) for $p = 2$ yields

$$\mathrm{Mass}(\Lambda_{x'}) = \begin{cases} 1/160, & \text{if } t \in \mathbb{P}^1(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2}); \\ 1/32 & \text{if } t \in \mathbb{P}^1(k) \setminus \mathbb{P}^1(\mathbb{F}_{p^4}). \end{cases}$$

This proves (28). □

3.3.2. *Supersingular abelian threefolds.*

We briefly describe the framework of polarised flag type quotients as developed in [31]. Let $E/\mathbb{F}_{p^2}$ be the elliptic curve fixed in Section 3.2. An α-group of rank r over an $\mathbb{F}_p$-scheme S is a finite flat group scheme which is Zariski-locally isomorphic to α_p^r. For an abelian scheme X over S, put $X^{(p)} := X \times_{S,F_S} S$, where $F_S : S \to S$ denotes the absolute Frobenius morphism on S. Denote by $F_{X/S} : X \to X^{(p)}$ and $V_{X/S} : X^{(p)} \to X$ be the relative Frobenius and Verschiebung morphisms, respectively. If $f : X \to Y$ is a morphism of abelian varieties, we also write $X[f]$ for $\ker(f)$.

Definition 3.6. (cf. [31, Section 3]) Let g be a positive integer.

(1) For any polarisation μ on E^g such that $\ker(\mu) = E^g[F]$ if g is even and $\ker(\mu) = 0$ otherwise, a g-dimensional *polarised flag type quotient (PFTQ)* with respect to μ is a chain of polarised abelian varieties over a base $\mathbb{F}_{p^2}$-scheme S

$$(Y_\bullet, \rho_\bullet) : (Y_{g-1}, \lambda_{g-1}) \xrightarrow{\rho_{g-1}} (Y_{g-2}, \lambda_{g-2}) \cdots \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_0, \lambda_0),$$

such that:
   (i) $(Y_{g-1}, \lambda_{g-1}) = (E^g, p^{\lfloor (g-1)/2 \rfloor}\mu) \times_{\operatorname{Spec} \mathbb{F}_{p^2}} S$;
   (ii) $\ker(\rho_i)$ is an α-group of rank i for $1 \le i \le g-1$;
   (iii) $\ker(\lambda_i) \subseteq Y_i[\mathsf{V}^j \circ \mathsf{F}^{i-j}]$ for $0 \le i \le g-1$ and $0 \le j \le \lfloor i/2 \rfloor$, where $\mathsf{F} = F_{Y_i/S}$ and $\mathsf{V} = V_{Y_i/S}$.

An isomorphism of g-dimensional polarised flag type quotients is a chain of isomorphisms $(\alpha_i)_{0 \le i \le g-1}$ of polarised abelian varieties such that $\alpha_{g-1} = \mathrm{id}_{Y_{g-1}}$.

(2) A g-dimensional polarised flag type quotient $(Y_\bullet, \rho_\bullet)$ is said to be *rigid* if

$$\ker(Y_{g-1} \to Y_i) = \ker(Y_{g-1} \to Y_0) \cap Y_{g-1}[\mathsf{F}^{g-1-i}], \quad \text{for } 1 \le i \le g-1.$$

(3) Let $\mathscr{P}_\mu$ (resp. $\mathscr{P}'_\mu$) denote the moduli space over $\mathbb{F}_{p^2}$ of g-dimensional (resp. rigid) polarised flag type quotients with respect to μ.

Now let $g = 3$. According to [31, Section 9.4], $\mathscr{P}_\mu$ is a two-dimensional geometrically irreducible scheme over $\mathbb{F}_{p^2}$. The projection to the last member gives a proper $\overline{\mathbb{F}}_p$-morphism

$$\begin{aligned} \mathrm{pr}_0 : \mathscr{P}_\mu &\to \mathscr{S}_{3,1}, \\ (Y_\bullet, \rho_\bullet) &\mapsto (Y_0, \lambda_0). \end{aligned}$$

Moreover, for each principally polarised supersingular abelian threefold (X, λ) there exist a $\mu \in P(E^3)$ and a polarised flag type quotient $y \in \mathscr{P}_\mu$ such that $\mathrm{pr}_0(y) = [(X, \lambda)] \in \mathscr{S}_{3,1}$, cf. [25, Proposition 5.4]. Put differently, the morphism

$$\mathrm{pr}_0 : \coprod_{\mu \in P(E^3)} \mathscr{P}_\mu \to \mathscr{S}_{3,1} \tag{29}$$

is surjective and generically finite. We define the mass function on $\mathscr{P}_\mu(k)$ as follows:

$$\mathrm{Mass} : \mathscr{P}_\mu(k) \to \mathbb{Q}, \quad \mathrm{Mass}(y) := \mathrm{Mass}(\Lambda_x),\ x = \mathrm{pr}_0(y). \tag{30}$$

We now describe the structure of $\mathscr{P}_\mu$. First of all, this structure is independent of the choice of μ; see [31, Section 3.10]. The map

$$\pi : ((Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (Y_0, \lambda_0)) \mapsto ((Y_2, \lambda_2) \to (Y_1, \lambda_1))$$

induces a morphism $\pi : \mathscr{P}_\mu \to \mathbb{P}^2$ whose image is isomorphic to the Fermat curve C defined by the equation $X_1^{p+1} + X_2^{p+1} + X_3^{p+1} = 0$. Moreover, as a fibre space over C, $\mathscr{P}_\mu$ is isomorphic to $\mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1))$; see [31, Sections 9.3-9.4] and [23, Proposition 3.5]. According to [31, Section 9.4] (cf. [23, Definition 3.14]), there is a section $s : C \twoheadrightarrow T \subseteq \mathscr{P}_\mu$ of π. Furthermore, one has $\mathscr{P}'_\mu = \mathscr{P}_\mu - T$.

We pull back the a-numbers of the points of $\mathscr{S}_3$ to the a-numbers of the points of $\mathscr{P}_\mu$, by setting $a(y) := a(\mathrm{pr}_0(y))$ for $y \in \mathscr{P}_\mu(k)$. We shall write a point $y \in \mathscr{P}_\mu(k)$ as (t, u), where $t = \pi(y)$ and $u \in \pi^{-1}(t) =: \mathbb{P}^1_t(k)$.

Lemma 3.7. *Let $y = (t, u) \in \mathscr{P}_\mu(k)$ be a point corresponding to a PFTQ.*

(i) *If $y \in T$ then $a(y) = 3$.*
(ii) *If $t \in C(\mathbb{F}_{p^2})$, then $a(y) \geq 2$. Moreover, $a(y) = 3$ if and only if $u \in \mathbb{P}^1_t(\mathbb{F}_{p^2})$.*
(iii) *We have $a(y) = 1$ if and only if $y \notin T$ and $t \notin C(\mathbb{F}_{p^2})$.*

Proof. See [31, Sections 9.3-9.4]. □

Theorem 3.8. *Let $y = (t, u) \in \mathscr{P}_\mu(k)$ be a point such that $t \in C(\mathbb{F}_{p^2})$. Then*

$$\mathrm{Mass}(y) = \frac{L_p}{2^{10} \cdot 3^4 \cdot 5 \cdot 7},$$

where

$$L_p = \begin{cases} (p-1)(p^2+1)(p^3-1) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ (p-1)(p^3+1)(p^3-1)(p^4-p^2) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ 2^{-e(p)}(p-1)(p^3+1)(p^3-1)p^2(p^4-1) & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}), \end{cases}$$

where $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$.

Proof. See [23, Theorem A]. □

Theorem 3.8 gives the mass formula for points with a-number greater than or equal to 2. To describe the mass formula for points with a-number 1, we need the construction of an auxiliary divisor $\mathscr{D} \subseteq \mathscr{P}'_\mu$, cf. [23, Definition 5.16], and a function $d : C(k) \setminus C(\mathbb{F}_{p^2}) \to \{3,4,5,6\}$, cf. [23, Definition 5.12] that is proven in [23, Proposition 5.13] to be related to the field of definition of the parameter t. The function d is surjective when $p \neq 2$, and it only takes value 3 when $p = 2$.

Theorem 3.9. *Let $y = (t,u) \in \mathscr{P}'_\mu(k)$ be a point such that $t \notin C(\mathbb{F}_{p^2})$. Then*

$$\mathrm{Mass}(y) = \frac{p^3 L_p}{2^{10} \cdot 3^4 \cdot 5 \cdot 7},$$

where

$$L_p = \begin{cases} 2^{-e(p)} p^{2d(t)} (p^2-1)(p^4-1)(p^6-1) & \text{if } y \notin \mathscr{D}; \\ p^{2d(t)} (p-1)(p^4-1)(p^6-1) & \text{if } t \notin C(\mathbb{F}_{p^6}) \text{ and } y \in \mathscr{D}; \\ p^6 (p^2-1)(p^3-1)(p^4-1) & \text{if } t \in C(\mathbb{F}_{p^6}) \text{ and } y \in \mathscr{D}. \end{cases}$$

Proof. See [23, Theorem B]. □

Remark 3.10. In [23] the authors define a stratification on $\mathscr{P}_\mu$ and $\mathscr{S}_3$ which is the coarsest one so that the mass function is constant. Using Theorem 3.8, the locus of $\mathscr{S}_3$ with a-number ≥ 2 decomposes into three strata: one stratum with a-number 3 and two strata with a-number 2.

In the locus with a-number 1, the stratification depends on p. When $p = 2$, the d-value is always 3 and Theorem 3.9 gives three strata, which are of dimension 0, 1, 2, respectively. When $p \neq 2$, the d-value $d(t) = 3$ if and only if $t \in C(\mathbb{F}_{p^6})$, cf. [23, Proposition 5.13]. In this case, Theorem 3.9 says that the mass function depends only on the d-value of t and on whether or not $y \in \mathscr{D}$, and hence it gives eight strata. The largest stratum is the open subset whose preimage consists of points $y = (t,u)$ with $d(t) = 6$ and $y \notin \mathscr{D}$, and the smallest mass-value stratum is the zero-dimensional locus whose preimage consists of points $y = (t,u)$ with $d(t) = 3$ and $y \in \mathscr{D}$. Note that the mass-value strata for which the points $y = (t,u)$ have d-value less than 6 and are in the divisor $\mathscr{D}$ are also zero-dimensional. Besides the the superspecial locus, in which points have a-number three, the smaller mass-value stratum with a-number 2 also has dimension 0.

For every point x in the largest stratum, one has

$$\mathrm{Mass}(\Lambda_x) \sim \frac{p^{27}}{2^{11} \cdot 3^4 \cdot 5 \cdot 7} \quad \text{as } p \to \infty. \tag{31}$$

On the other hand, for every point x in the superspecial locus, one has

$$\mathrm{Mass}(\Lambda_x) \sim \frac{p^6}{2^{10} \cdot 3^4 \cdot 5 \cdot 7} \quad \text{as } p \to \infty. \tag{32}$$

From all known examples, we observe that the mass Λ_x is a polynomial function in p with $\mathbb{Q}$-coefficients. It is plausible to expect that this holds true as well for any x in $\mathscr{S}_g$ and for arbitrary g. Under this assumption, it is of interest to determine the largest degree of $\mathrm{Mass}(\Lambda_x)$, viewed as a polynomial in p. By all known examples, the smallest degree should occur exactly when x is superspecial and be $g(g+1)/2$. This is indeed the case for any g. We will give a proof of this elsewhere.

4. The geometric theory: Automorphism groups of polarised abelian varieties

4.1. **Powers of an elliptic curve.**

Let E be an elliptic curve over a field K with canonical polarisation λ_E and let $(X_0, \lambda_0) = (E^n, \lambda_{\mathrm{can}})$, where $\lambda_{\mathrm{can}} = \lambda_E^n$ equals the product polarisation on E^n. Denote by $R := \mathrm{End}(E)$ the endomorphism ring of E over K and by $B = \mathrm{End}^0(E)$ its endomorphism algebra; B carries the canonical involution $a \mapsto \bar{a}$. Then B is either $\mathbb{Q}$, an imaginary quadratic field, or the definite $\mathbb{Q}$-algebra $B_{p,\infty}$ of prime discriminant p. We identify the endomorphism ring $\mathrm{End}(E^t) = \{a^t : a \in \mathrm{End}(E)\}$ with $\mathrm{End}(E)^{\mathrm{opp}}$. Via the isomorphism λ_E, the (anti-)isomorphism $\mathrm{End}(E^t) = \mathrm{End}(E)^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}(E)$ maps a^t to $\lambda_E^{-1} a^t \lambda_E = \bar{a}$. In other words, using the polarisation λ_E we identify $\mathrm{End}(E)^{\mathrm{opp}} = \mathrm{End}(E^t)$ with $\{\bar{a} : a \in \mathrm{End}(E)\}$.

The set $\mathrm{Hom}(E, X_0) = R^n$ is a free right R-module whose elements we view as column vectors. It carries a left $\mathrm{End}(X_0)$-module structure and it follows that $\mathrm{End}(X_0) = \mathrm{Mat}_n(R) = \mathrm{End}_R(R^n)$ and $\mathrm{End}^0(X_0) = \mathrm{Mat}_n(B) = \mathrm{End}_B(B^n)$, where B^n naturally identifies with $\mathrm{Hom}(E, X_0) \otimes \mathbb{Q}$. The map $\mathrm{End}(X_0) \to \mathrm{End}(X_0^t)$, sending a to its dual a^t, induces an isomorphism of rings $\mathrm{End}(X_0)^{\mathrm{opp}} \simeq \mathrm{End}(X_0)$. The Rosati involution on $\mathrm{End}^0(X_0) = \mathrm{Mat}_n(B)$ induced by λ_0 is given by $A \mapsto A^* = \bar{A}^T$. Let $\mathscr{H}_n(B)$ be the set of positive-definite Hermitian[1] matrices H in $\mathrm{Mat}_n(B)$, satisfying $H = H^*$ and $v^* H v > 0$ for every non-zero vector $v \in B^n$. Let $\mathscr{P}(X_0)_{\mathbb{Q}}$ denote the set of fractional polarisations on X_0.

Lemma 4.1. *The map $\lambda \mapsto \lambda_0^{-1}\lambda$ gives a bijection $\mathscr{P}(X_0)_{\mathbb{Q}} \xrightarrow{\sim} \mathscr{H}_n(B)$, under which λ_0 corresponds to the identity $\mathbb{I}_n$.*

Proof. This is shown in [37, 7.12-7.14] for the case where X_0 is a superspecial abelian variety over an algebraically closed field of characteristic p and the same argument holds for the present situation. □

For each $H \in \mathscr{H}_n(B)$, we define a Hermitian form on B^n by

$$h : B^n \times B^n \to B, \quad h(v_1, v_2) := v_1^* \cdot H \cdot v_2, \quad v_1, v_2 \in B^n. \tag{33}$$

If $H = \lambda_0^{-1}\lambda$ is the corresponding Hermitian form for λ, then the Rosati involution induced by λ is the adjoint of h: $A \mapsto H^{-1} \cdot A^* \cdot H$. The correspondence mentioned above induces an identification of automorphism groups

$$\mathrm{Aut}(X_0, \lambda) = \mathrm{Aut}(R^n, h) := \{A \in \mathrm{GL}_n(B) \text{ s.t. } A(R^n) = R^n \text{ and } A^* \cdot H \cdot A = H\}. \tag{34}$$

In particular, the identification (34) induces an identification of automorphism groups

$$\mathrm{Aut}(X_0, \lambda_0) = \mathrm{Aut}(R^n, \mathbb{I}_n), \tag{35}$$

and we know that

$$\begin{aligned} \mathrm{Aut}(R^n, \mathbb{I}_n) &= \{A \in \mathrm{GL}_n(R) \text{ s.t. } A^* \cdot A = \mathbb{I}_n\} \\ &\simeq (R^\times)^n \cdot S_n, \end{aligned} \tag{36}$$

where the last equality follows from the analogous result in [23, Theorem 6.1].

If E is the unique supersingular elliptic curve over $\overline{\mathbb{F}}_2$ up to isomorphism, then $R^\times = E_{24} \simeq \mathrm{SL}_2(\mathbb{F}_3)$ (cf. [23, (57)]) and the automorphism group $\mathrm{Aut}(X_0, \lambda_0)$ has $(24)^n n!$ elements by (35) and (36). We expect that this is the maximal size of $\mathrm{Aut}(X, \lambda)$ for any n-dimensional principally polarised abelian variety (X, λ) over any field K. We show a partial result towards confirming this expectation.

[1] Strictly speaking, one should call such a matrix H symmetric, Hermitian or quaternion Hermitian according to whether B is $\mathbb{Q}$, an imaginary quadratic field, or $B_{p,\infty}$.

Proposition 4.2. *For $n \leq 3$, the number $(24)^n n!$ is the maximal order of the automorphism group of an n-dimensional principally polarised abelian variety (X, λ) over any field K.*

Proof. Since any principally polarised abelian variety(X, λ) is of finite type over the prime field of K, it admits a model (X_1, λ_1) over a finitely generated $\mathbb{Z}$-algebra S such that $\mathrm{Aut}_K(X, \lambda) = \mathrm{Aut}_S(X_1, \lambda_1)$. Taking any $\overline{\mathbb{F}}_p$-point s of S with residue field $k(s)$, one has $\mathrm{Aut}_S(X_1, \lambda_1) \subseteq \mathrm{Aut}_{\overline{\mathbb{F}}_p}((X_1, \lambda_1) \otimes_S k(s))$. Thus, without loss of generality we may assume that the ground field K is the algebraically closed field $\overline{\mathbb{F}}_p$ for some prime p. Further we can assume that (X, λ) is defined over a finite field $\mathbb{F}_q$ with $\mathrm{End}(X) = \mathrm{End}(X \otimes \overline{\mathbb{F}}_p)$. Note that $\mathrm{Aut}(X, \lambda)$ is a finite subgroup of $\mathrm{Aut}(X)$ and hence a finite subgroup of $\mathrm{End}^0(X)^\times$. We will bound the size of $\mathrm{Aut}(X, \lambda)$ by a maximal finite subgroup G of $\mathrm{End}^0(X)^\times$.

When $n = 1$, it is well known that 24 is the maximal cardinality of $\mathrm{Aut}(E)$ of an elliptic curve E over $\overline{\mathbb{F}}_p$ for some prime p and it is realised by the supersingular elliptic curve over $\overline{\mathbb{F}}_2$, cf. [44, V. Proposition 3.1, p. 145] .

Suppose $n = 2$. If X simple, then X is either ordinary or almost ordinary. By Tate's Theorem, the endomorphism algebra $\mathrm{End}^0(X)$ is a CM field and G consists of its roots of unity, so $|G| \leq 12$. If X is isogenous to $E_1 \times E_2$ where E_1 is not isogenous to E_2, then $\mathrm{End}^0(E_1 \times E_2) = \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2)$ and any maximal finite subgroup G of $\mathrm{End}^0(E_1)^\times \times \mathrm{End}^0(E_2)^\times$ is of the form $\mathrm{Aut}(E_1') \times \mathrm{Aut}(E_2')$ for elliptic curves E_i' isogenous to E_i. This reduces to the case $n = 1$ and hence $|G| \leq 24^2$. Suppose now that $X \sim E^2$. If $L = \mathrm{End}^0(E)$ is imaginary quadratic, then $\mathrm{End}^0(X) \simeq \mathrm{Mat}_2(L) \simeq \mathrm{End}^0(\widetilde{E}^2)$ for a complex elliptic curve $\widetilde{E}$ with CM by L. By [4], G has order ≤ 96. Thus, we may assume that E is supersingular so L is a quaternion algebra. If X is superspecial, then the classification of $\mathrm{Aut}(X, \lambda)$ has been studied by Katsura and Oort; we have $|\mathrm{Aut}(X, \lambda)| \leq 1152$ by [24, Table 1, p. 137]. If X is non-superspecial, then $\mathrm{Aut}(X, \lambda) < \mathrm{Aut}(\widetilde{X}, \widetilde{\lambda})$, where $(\widetilde{X}, \widetilde{\lambda})$ is the superspecial variety determined by the minimal isogeny of (X, λ). The classification of $\mathrm{Aut}(\widetilde{X}, \widetilde{\lambda})$ has been studied by the first author [20]. By [20, Lemma 2.1 p. 132 and Remark 1, p. 343] $\mathrm{Aut}(\widetilde{X}, \widetilde{\lambda})$ has order ≤ 720 if $p > 2$ and has order 1920 if $p = 2$. For the case $p = 2$ and $a(X) = 1$, the automorphism group $\mathrm{Aut}(X, \lambda)$ has order either 32 or 160 by Corollary 3.5. This proves the case $n = 2$.

Now let $n = 3$. Write $X \sim \prod_{i=1}^r X_i^{n_i}$ as the product of isotypic components up to isogeny, where the X_i's are mutually non-isogenous simple factors. By induction and by the same argument as for $n = 2$, we reduce to the case where $r = 1$, that is, X is elementary. Thus, we need to bound the size of maximal finite subgroups G in the simple $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$. Finite subgroups in a division ring or in a certain simple $\mathbb{Q}$-algebra have been studied by Amitsur [2] and Nebe [34]. A convenient list for our case is given by Hwang-Im-Kim [19, Section 5]. From this list we see that $|G| \leq 24^3 \cdot 6$ and that equality occurs exactly when $\mathrm{End}^0(X) \simeq \mathrm{Mat}_3(B_{2,\infty})$; see Theorem 5.13 of *loc. cit.* This proves the proposition. □

Remark 4.3. Similarly, if E is the unique elliptic curve with CM by $\mathbb{Z}[\zeta_3]$ over $\mathbb{C}$ up to isomorphism, then $R^\times = \mathbb{Z}[\zeta_3]^\times = \mu_6$ and the automorphism group $\mathrm{Aut}(X_0, \lambda_0)$ has $6^n n!$ elements by (35) and (36). We expect that this is the maximal size of $\mathrm{Aut}(X, \lambda)$ for any n-dimensional principally polarised abelian variety (X, λ) over any field K of characteristic *zero*.

4.2. **Varieties isogenous to a power of an elliptic curve.**

Let E/K and $R = \mathrm{End}(E)$ be as in the previous subsection. Let $\mathscr{A}$ denote the category of abelian varieties over K and $\mathscr{A}^{\mathrm{pol}}$ denote that of abelian varieties (X, λ) together with a fractional polarisation over K; we call (X, λ) a $\mathbb{Q}$-polarised abelian variety. Let $\mathscr{A}_E$ (resp. $\mathscr{A}_E^{\mathrm{pol}}$) be the full subcategory of $\mathscr{A}$ (resp. of $\mathscr{A}^{\mathrm{pol}}$) consisting of abelian varieties that are isogenous to a power of E over K. By an R-lattice we mean a finitely presented torsion-free R-module. Denote by Lat_R and ${}_R\mathrm{Lat}$ the categories of right R-lattices and left R-lattices, respectively. We

may write $R^{\mathrm{opp}} = \{a^T : a \in R\}$ with multiplication $a^T b^T := (ba)^T$. For a right R-module M, we write $M^{\mathrm{opp}} := \{m^T : m \in M\}$ for the left R^{opp}-module defined by $a^T m^T = (ma)^T$ for $a \in R$ and $m \in M$. The functor $I : M \mapsto M^{\mathrm{opp}}$ induces an equivalence of categories from Lat_R to ${}_{R^{\mathrm{opp}}}\mathrm{Lat}$. A Hermitian form on M here will mean a non-degenerate Hermitian form $h : M_{\mathbb{Q}} \times M_{\mathbb{Q}} \to B$ in the usual sense, where $M_{\mathbb{Q}} := M \otimes \mathbb{Q}$. If h takes R-values on M, we say h is integral. Let $\mathrm{Lat}_R^{\mathrm{H}}$ (resp. ${}_{R^{\mathrm{opp}}}\mathrm{Lat}^{\mathrm{H}}$) denote the category of positive-definite Hermitian right R-lattices (resp. left R^{opp}-lattices). The functor

$$I : \mathrm{Lat}_R^{\mathrm{H}} \to {}_{R^{\mathrm{opp}}}\mathrm{Lat}^{\mathrm{H}}$$

induces an equivalence of categories.

To each $\mathbb{Q}$-polarised abelian variety (X, λ) in $\mathscr{A}_E^{\mathrm{pol}}$, we associate a pair (M, h), where

$$M := \mathrm{Hom}(E, X) \tag{37}$$

is a right R-lattice, and where

$$h = h_\lambda : M_{\mathbb{Q}} \otimes M_{\mathbb{Q}} \to B, \quad h_\lambda(f_1, f_2) := \lambda_E^{-1} f_1^t \lambda f_2 \tag{38}$$

is a pairing on $M_{\mathbb{Q}}$.

Lemma 4.4. (1) *The pair (M, h) constructed above is a positive-definite Hermitian R-lattice. The Hermitian form h is integral on M if and only if λ is a polarisation, and it is perfect if and only if λ is a principal polarisation.*

(2) *Let λ be a fractional polarisation on $X_0 = E^n$. Then the associated Hermitian form h_λ on $M := \mathrm{Hom}(E, X_0) = R^n$ defined in* (38) *is the Hermitian form defined in* (33)*.*

Proof. (1) One checks that

$$h(f_1 a, f_2) = \lambda_E^{-1} a^t f_1^t \lambda f_2 = (\lambda_E^{-1} a^t \lambda_E) \lambda_E^{-1} f_1^t \lambda f_2 = \bar{a} h(f_1, f_2) \tag{39}$$

and $h(f_1, f_2 a) = h(f_1, f_2) a$. Moreover,

$$\overline{h(f_1, f_2)} = \lambda_E^{-1} (\lambda_E^{-1} f_1^t \lambda f_2)^t \lambda_E = \lambda_E^{-1} f_2^t \lambda f_1 \lambda_E^{-1} \lambda_E = h(f_2, f_1), \tag{40}$$

so the R-lattice is indeed Hermitian. For $f \neq 0 \in M$, we have $h(f, f) = \lambda_E^{-1} f^* \lambda$. Since $f^* \lambda$ is a fractional polarisation on E, the composition $\lambda_E^{-1} f^* \lambda$ is a positive element in B, which is a positive rational number in our case. This shows that h is positive-definite. The last two statements are clear as the polarisation λ_E is principal.

(2) For $f_1, f_2 \in \mathrm{Hom}(E, X)_{\mathbb{Q}} = B^n$, we have $h(f_1, f_2) = \lambda_E^{-1} f_1^t \lambda_0 \lambda_0^{-1} \lambda f_2$. If we write $f_1 = (a_1, \ldots, a_n)^T \in B^n$ and $\lambda_0^{-1} \lambda f_2 = (b_1, \ldots, b_n)^T =: \underline{b}$, then $\lambda_E^{-1} f_1^t \lambda_0 = (\bar{a}_1, \ldots, \bar{a}_n)^T$ and $h(f_1, f_2) = \sum_{i=1}^n \bar{a}_i b_i = f_1^* \cdot \underline{b} = f_1^* \cdot H \cdot f_2$ for $H = \lambda_0^{-1} \lambda$.

□

The sheaf Hom functor $\mathscr{H}om_R(-, E) : {}_R\mathrm{Lat}^{\mathrm{opp}} \to \mathscr{A}_E$ produces a fully faithful functor whose essential image will be denoted by $\mathscr{A}_{E,\mathrm{ess}}$. We refer to [22] for the construction and properties of $\mathscr{H}om_R(-, E)$. The functor $\mathrm{Hom}(-, E) : \mathscr{A}_E \to {}_R\mathrm{Lat}^{\mathrm{opp}}$ provides the inverse on $\mathscr{A}_{E,\mathrm{ess}}$. The following result can be regarded as a polarised version of the construction in [22].

Proposition 4.5. *The functor $(X, \lambda) \mapsto (M, h)$ introduced in Equations* (37) *and* (38) *induces an equivalence of categories*

$$\mathscr{A}_{E,\mathrm{ess}}^{\mathrm{pol}} \longrightarrow \mathrm{Lat}_R^H.$$

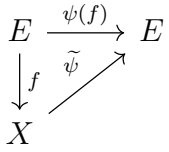
Moreover, λ is a polarisation if and only h is integral, and it is a principal polarisation if and only h is a perfect pairing on M.

Proof. Let $T : \mathscr{A}_E \to \mathscr{A}_{E^t}$ be the functor sending X to X^t; it induces an anti-equivalence of categories. The composition $\mathrm{Hom}(-, E^t) \circ T$ sends X to $\mathrm{Hom}(X^t, E^t)$ and $I \circ \mathrm{Hom}(E, -)$ sends X to $\mathrm{Hom}(E, X)^{\mathrm{opp}}$. The map that sends $f \in \mathrm{Hom}(E, X)$ to $f^t \in \mathrm{Hom}(X^t, E^t)$ gives a natural isomorphism $I \circ \mathrm{Hom}(E, -) \to \mathrm{Hom}(-, E^t) \circ T$. Restricted to $\mathscr{A}_{E,\mathrm{ess}}$, the functor $\mathrm{Hom}(-, E^t) \circ T$ is an equivalence of categories. Therefore, $\mathrm{Hom}(E, -)$ induces an equivalence of categories from $\mathscr{A}_{E,\mathrm{ess}}$ to Lat_R.

The dual $M^t := \mathrm{Hom}_R(M, R)$ of a right R-lattice M, which a priori is a left R-lattice, may be regarded as a right R-lattice via $f \cdot a := \bar{a} f$. This is simply the right R^{opp}-module $(M^t)^{\mathrm{opp}}$ with the identification $R^{\mathrm{opp}} = \{\bar{a} : a \in R\}$. Suppose that $M = \mathrm{Hom}(E, X)$ is in the essential image of the equivalence, coming from some $(X, \lambda) \in \mathscr{A}_{E,\mathrm{ess}}$. We claim that the map

$$\begin{aligned} \varphi : \mathrm{Hom}(E, X^t) &\to M^t \\ \alpha &\mapsto (\varphi_\alpha : m \mapsto \lambda_E^{-1} \alpha^t m) \end{aligned} \tag{41}$$

is an isomorphism of right R-lattices. Indeed, it is injective by construction. For surjectivity, pick any $\psi \in M^t$. Since $\psi \in \mathrm{Hom}(\mathrm{Hom}(E, X), \mathrm{Hom}(E, E))$ and the functor $\mathrm{Hom}(E, -)$ is fully faithful, there exists a unique map $\widetilde{\psi} \in \mathrm{Hom}(X, E)$ such that $\psi(f) = \widetilde{\psi} \circ f$ for all maps $f \in \mathrm{Hom}(E, X) = M$.



Then $\psi(m) = \widetilde{\psi} m$ and we have $\widetilde{\psi}^t \in \mathrm{Hom}(E^t, X^t)$. Considering $\alpha = \widetilde{\psi}^t \lambda_E \in \mathrm{Hom}(E, X^t)$, it follows from the construction that

$$\varphi_\alpha(m) = \lambda_E^{-1} \alpha^t m = \lambda_E^{-1} \lambda_E \widetilde{\psi} m = \psi(m)$$

for all $m \in M$, hence $\psi = \varphi_\alpha$, which proves the claim.

To prove the proposition, it remains to show that for any $X \in \mathscr{A}_{E,\mathrm{ess}}$ we have a bijection between fractional polarisations on X in $\mathrm{Hom}(X, X^t) \otimes \mathbb{Q}$ and positive-definite Hermitian forms on $M_{\mathbb{Q}}$ in $\mathrm{Hom}(M, M^t) \otimes \mathbb{Q}$. By the definition $\mathrm{Hom}(E, X) = M$, the isomorphism $\mathrm{Hom}(E, X^t) \simeq M^t$, and the fact that the functor $\mathrm{Hom}(E, -)$ is fully faithful, the natural map $\mathrm{Hom}(X, X^t) \to \mathrm{Hom}(M, M^t)$ is an isomorphism. Note that the induced isomorphism $\mathrm{Hom}(X, X^t) \otimes \mathbb{Q} \to \mathrm{Hom}(M, M^t) \otimes \mathbb{Q}$ is the same as the construction in Equation (38). Hence, for every positive-definite Hermitian form h on $M_{\mathbb{Q}}$, there exists a unique symmetric element $\lambda_1 \in \mathrm{Hom}(X, X^t)_{\mathbb{Q}}$ such that $h_{\lambda_1} = h$ and it suffices to show that λ_1 is a fractional polarisation on X.

Any quasi-isogeny $\beta : X \to E^n$ induces an isomorphism $\beta_* : M \otimes \mathbb{Q} \to \mathrm{Hom}(E, E^n) \otimes \mathbb{Q} = B^n$ of B-modules. Let $\lambda := \beta_* \lambda_1$ be the pushforward map in $\mathrm{Hom}(E^n, (E^n)^t) \otimes \mathbb{Q}$, and let $h_\lambda : B^n \times B^n \to B$ be the Hermitian form defined by (38). Then $\beta_* : (M_{\mathbb{Q}}, h) \to (B^n, h_\lambda)$ is an isomorphism of B-modules with pairings. Since h is a positive-definite Hermitian form by assumption, so is the pairing h_λ. Let $H \in \mathscr{H}_n(B)$ be the positive-definite Hermitian matrix corresponding to h_λ with respect to the standard basis. By Lemma 4.4(2), H is equal to $\lambda_{\mathrm{can}}^{-1} \lambda$. Since $H \in \mathscr{H}_n(B)$, by Lemma 4.1 the map λ is a fractional polarisation and therefore λ_1 is a fractional polarisation, as required. □

By [22, Theorem 1.1] we obtain the following consequence.

Corollary 4.6. *Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$ with Frobenius endomorphism π and endomorphism ring $R = \mathrm{End}(E)$. The functor $\mathrm{Hom}(E, -) : \mathscr{A}_E^{\mathrm{pol}} \to \mathrm{Lat}_R^H$ induces an equivalence of categories if and only if one the following holds:*

- *E is ordinary and $\mathbb{Z}[\pi] = R$;*
- *E is supersingular, $K = \mathbb{F}_p$ and $\mathbb{Z}[\pi] = R$; or*
- *E is supersingular, $K = \mathbb{F}_{p^2}$ and R has rank 4 over $\mathbb{Z}$.*

Remark 4.7. A few results similar to Proposition 4.5 exist in the literature. The first case of Corollary 4.6 is proven in [26]. More precisely, when E is ordinary and $R = \mathbb{Z}[\pi]$, in [26, Theorem 3.3] the constructions of [22] are used to derive an equivalence of categories between $\mathscr{A}_E^{\mathrm{pol}}$ and Lat_R^H.
When $R = \mathbb{Z}[\pi]$, Serre's tensor construction (cf. [29]) gives an analogue of Corollary 4.6 in some cases, when replacing $\mathscr{H}om$ with $\otimes_R E$. The tensor construction is used in [1, Theorem A] for a ring R with positive involution, a projective finitely presented right R-module M with an R-linear map $h : M \to M^t$, and an abelian scheme A over a base S with R-action via $\iota : R \hookrightarrow \mathrm{End}_S(A)$ and an R-linear polarisation $\lambda : A \to A^t$, to prove that $h \otimes \lambda : M \otimes_R A \to M^t \otimes_R A^t$ is a polarisation if and only if h is a positive-definite R-valued Hermitian form. Also, for a superspecial abelian variety X over an algebraically closed field k of characteristic p it is shown in [37, 7.12-7.14] that the functors $X \mapsto M = \mathrm{Hom}(E, X)$ and $M \mapsto M \otimes_R E = X$ yield bijections between principal polarisations on X and positive-definite perfect Hermitian forms on M.

For any elliptic curve E over a field K, we know that $B = \mathrm{End}^0(E)$ satisfies the conditions in Section 2 and in particular those of Corollary 2.2. This means that when E is defined over a finite field and is in one of the cases of Corollary 4.6, then we may apply the categorical constructions above to automorphism groups, in order to obtain the following result.

Corollary 4.8. (1) *For any $(X, \lambda) \in \mathscr{A}_{E,\mathrm{ess}}^{\mathrm{pol}}$, the lattice (M, h) associated to (X, λ) admits a unique orthogonal decomposition*

$$(M, h) = \perp_{i=1}^{r} \perp_{j=1}^{e_i} (M_{ij}, h_i).$$

Hence, we have that

$$\mathrm{Aut}(X, \lambda) \simeq \mathrm{Aut}(M, h) \simeq \prod_{i=1}^{r} \mathrm{Aut}(M_{i1})^{e_i} \cdot S_{e_i}. \tag{42}$$

(2) *Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$ such that Corollary 4.6 applies. Then for any $(X, \lambda) \in \mathscr{A}_E^{\mathrm{pol}}$, the automorphism group $\mathrm{Aut}(X, \lambda)$ can be computed as in Equation* (42).

Corollary 4.9. *Let R be a maximal order in the definite quaternion $\mathbb{Q}$-algebra $B_{p,\infty}$. Let $\mathrm{Sp}^{\mathrm{pol}}$ be the category of fractionally polarised superspecial abelian varieties over an algebraically closed field k of characteristic p. Then there is an equivalence of categories between $\mathrm{Sp}^{\mathrm{pol}}$ and $\mathrm{Lat}_R^{\mathrm{H}}$. Moreover, for any object (X, λ) in $\mathrm{Sp}^{\mathrm{pol}}$, the automorphism group $\mathrm{Aut}(X, \lambda)$ can be computed as in Equation* (42).

Proof. Choose an elliptic curve E over $\mathbb{F}_{p^2}$ with Frobenius endomorphism $\pi = -p$ and endomorphism ring $\mathrm{End}(E) \simeq R$. Then the category $\mathscr{A}_E$ is the same as that of superspecial abelian varieties over $\mathbb{F}_{p^2}$ with Frobenius endomorphism $-p$, because every supersingular abelian variety with Frobenius endomorphism $-p$ is superspecial. The functor sending each object X in $\mathscr{A}_E$ to $X \otimes_{\mathbb{F}_{p^2}} k$ induces an equivalence of categories between $\mathscr{A}_E$ and the category of superspecial abelian varieties over k (cf. [50, Proposition 5.1]). Thus, it induces an equivalence

of categories between $\mathscr{A}_E^{\mathrm{pol}}$ and $\mathrm{Sp}^{\mathrm{pol}}$. By Corollary 4.6, there is an equivalence of categories between $\mathrm{Sp}^{\mathrm{pol}}$ and $\mathrm{Lat}_R^{\mathrm{H}}$. The last statement of the corollary follows from Corollary 4.8. □

4.3. **Unique decomposition property.**

Definition 4.10. Let (X, λ) be a $\mathbb{Q}$-polarised abelian variety over K. We say (X, λ) *indecomposable* if whenever we have an isomorphism $(X_1, \lambda_1) \times (X_2, \lambda_2) = (X_1 \times X_2, \lambda_1 \times \lambda_2) \simeq (X, \lambda)$, either $\dim X_1 = 0$ of $\dim X_2 = 0$.

By induction on the dimension of X, every object (X, λ) in $\mathscr{A}^{\mathrm{pol}}$ decomposes into a product of indecomposable objects.

Definition 4.11. (1) An object (X, λ) in $\mathscr{A}^{\mathrm{pol}}$ is said to have *the Remak-Schmidt property* if for any two decompositions into indecomposable objects $(X, \lambda) \simeq \prod_{i=1}^r (X_i, \lambda_i)$ and $(X, \lambda) \simeq \prod_{j=1}^s (X'_j, \lambda'_j)$, we have $r = s$ and there exist a permutation $\sigma \in S_r$ and an isomorphism $(X_i, \lambda_i) \simeq (X'_{\sigma(i)}, \lambda'_{\sigma(i)})$ for every $1 \leq i \leq r$.

(2) An object (X, λ) in $\mathscr{A}^{\mathrm{pol}}$ is said to have *the strong Remak-Schmidt property* if for any two decompositions into indecomposable objects $\phi = (\phi_i)_i : \prod_{i=1}^r (X_i, \lambda_i) \xrightarrow{\sim} (X, \lambda)$ and $\phi' = (\phi'_j)_j : \prod_{j=1}^s (X'_j, \lambda'_j) \xrightarrow{\sim} (X, \lambda)$, we have $r = s$ and there exist a permutation $\sigma \in S_r$ and an isomorphism $\alpha_i : (X_i, \lambda_i) \xrightarrow{\sim} (X'_{\sigma(i)}, \lambda'_{\sigma(i)})$ such that $\phi_i = \phi'_{\sigma(i)} \circ \alpha_i$ for every $1 \leq i \leq r$.

Lemma 4.12. *Let X be an object in $\mathscr{A}_E$. Then there exist an object $\widetilde{X}$ in $\mathscr{A}_{E,\mathrm{ess}}$ and an isogeny $\gamma : X \to \widetilde{X}$ such that for any morphism $\phi : X \to Y$ with object Y in $\mathscr{A}_{E,\mathrm{ess}}$, there exists a unique morphism $\alpha : \widetilde{X} \to Y$ such that $\alpha \circ \gamma = \phi$. Dually, there exist an object $\widetilde{X}$ in $\mathscr{A}_{E,\mathrm{ess}}$ and an isogeny $\varphi : \widetilde{X} \to X$ that satisfies the similar universal property.*

Proof. We first construct a morphism $\gamma : X \to \widetilde{X}$, where $\widetilde{X}$ is an object in $\mathscr{A}_{E,\mathrm{ess}}$. It will be more convenient to adopt the contravariant functors. Let $M := \mathrm{Hom}(X, E)$ and let $\widetilde{X} := \mathscr{H}om_R(M, E)$. The abelian variety $\widetilde{X}$ represents the functor

$$S \mapsto \mathrm{Hom}_R(M, E(S)), \quad M = \mathrm{Hom}(X, E)$$

for any any K-scheme S. Define a morphism $\gamma : X \to \widetilde{X}$ by

$$\gamma : X(S) \to \widetilde{X}(S) = \mathrm{Hom}_R(M, E(S)) \quad \text{mapping} \quad x \mapsto (\gamma_x : f \mapsto f(x) \in E(S)), \tag{43}$$

for all $f \in M = \mathrm{Hom}(X, E)$.

Now let Y be an object in in $\mathscr{A}_{E,\mathrm{ess}}$ and $\phi : X \to Y$ be a morphism. Using (43), we also have a morphism $\gamma_Y : Y \to \widetilde{Y}$ which is an isomorphism as the functor $\mathrm{Hom}(-, E)$ induces an equivalence on $\mathscr{A}_{E,\mathrm{ess}}$. The morphism $\phi : X \to Y$ induces a map $M_Y := \mathrm{Hom}(Y, E) \to M = \mathrm{Hom}(X, E)$ by precomposition with ϕ. This map also induces, after applying the functor $\mathscr{H}om_R(-, E)$, a morphism $\beta : \widetilde{X} \to \widetilde{Y}$. We claim that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\gamma} & \widetilde{X} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \beta} \\ Y & \xrightarrow[\sim]{\gamma_Y} & \widetilde{Y} \end{array} \tag{44}$$

commutes; we will show this by proving it on S-points for any K-scheme S. Let $x \in X(S)$ and $g : Y \to E$. We have $\beta(\gamma_x)(g) = \gamma_x(g \circ \phi) = g(\phi(x))$. On the other hand $\gamma_Y(\phi(x))(g) = g(\phi(x))$. This shows the claim. Let $\alpha := \gamma_Y^{-1} \circ \beta : \widetilde{X} \to Y$, so we have $\alpha \circ \gamma = \phi$ by commutativity.

Finally, take $Y = E^n$ and any isogeny $\phi : X \to E^n$ and let $\alpha : \widetilde{X} \to E^n$ be the unique morphism satisfying $\alpha \circ \gamma = \phi$. Since $\dim X = \dim \widetilde{X} = \dim E^n = n$, it follows that γ is an isogeny. The dual construction is entirely analogous. □

Definition 4.13. Let X be an object in $\mathscr{A}_E$. We call the isogeny $\gamma : X \to \widetilde{X}$ (resp. $\varphi : \widetilde{X} \to X$) constructed in Lemma 4.12 the *minimal E-isogeny of X* and the abelian variety $\widetilde{X}$ the *E-hull* of X.

Remark 4.14. If E/K is a supersingular elliptic curve over an algebraically closed field $K = k$ of characteristic p, then $\mathscr{A}_E$ is the category of supersingular abelian varieties over k and $\mathscr{A}_{E,\mathrm{ess}}$ is the category of superspecial abelian varieties over k. In this case, a minimal E-isogeny $\gamma : X \to \widetilde{X}$ or $\varphi : \widetilde{X} \to X$ of a supersingular abelian variety X is precisely the minimal isogeny of X in the sense of Oort, cf. [23, Definition 2.11]. By Lemma 4.12, the minimal isogeny $(X, \gamma : X \to \widetilde{X})$ satisfies the stronger universal property where the test object $\phi : X \to Y$ does not have to be an isogeny.

Lemma 4.15. *Let X be an object in $\mathscr{A}_{E.\mathrm{ess}}$. Suppose there are abelian varieties $X_1, \ldots, X_r$ in $\mathscr{A}_E$ and there is an isomorphism $\phi : X_1 \times \cdots \times X_r \xrightarrow{\sim} X$. Then each abelian variety X_i lies in $\mathscr{A}_{E.\mathrm{ess}}$.*

Proof. According to the construction of minimal E-isogenies, let

$$M := \mathrm{Hom}(X, E) \simeq \prod_{i=1}^{r} M_i \quad \text{and} \quad \widetilde{X} := \mathscr{H}om_R(M, E) \simeq \prod_{i=1}^{r} \widetilde{X}_i,$$

where

$$M_i := \mathrm{Hom}(X_i, E) \quad \text{and} \quad \widetilde{X}_i := \mathscr{H}om_R(M_i, E).$$

By the definition of γ in Equation (43), we have

$$\gamma = (\gamma_i)_i : X \simeq X_1 \times \cdots \times X_r \longrightarrow \widetilde{X} \simeq \widetilde{X}_1 \times \cdots \times \widetilde{X}_r, \quad \text{where} \quad \gamma_i : X_i \to \widetilde{X}_i.$$

By applying the universal property of the minimal E-isogeny with $Y = X$ and $\phi = \mathrm{id}$, there is a unique isogeny $\alpha : \widetilde{X} \to X$ such that $\alpha \circ \gamma = \mathrm{id}$. This shows that γ is an isomorphism, which means that each $\gamma_i : X_i \to \widetilde{X}_i$ is an isomorphism. In particular, every abelian variety X_i lies in $\mathscr{A}_{E,\mathrm{ess}}$. □

Lemma 4.16. *Let $X_1, \ldots, X_r$ be objects in $\mathscr{A}_E$. Then $(\gamma_i)_i : X = \prod_{i=1}^r X_i \to \prod_{i=1}^r \widetilde{X}_i$ is the minimal E-isogeny of X.*

Proof. For any $Y \in \mathscr{A}_{E,\mathrm{ess}}$, as in Equation (44), we obtain the following commutative diagram:

$$\begin{array}{ccc} \prod_{i=1}^r X_i & \xrightarrow{(\gamma_i)_i} & \prod_{i=1}^r \widetilde{X}_i \\ \big\downarrow{\scriptstyle \sum_i \phi_i} & & \big\downarrow{\scriptstyle \beta = \sum_i \beta_i} \\ Y & \xrightarrow[\sim]{\gamma_Y} & \widetilde{Y}. \end{array} \tag{45}$$

Then the unique morphism $\alpha = \gamma_Y^{-1} \circ \beta$ satisfies the desired property $\alpha \circ (\gamma_i)_i = \sum_i \phi_i$. □

Theorem 4.17. *Every object (X, λ) in $\mathscr{A}_{E,\mathrm{ess}}^{\mathrm{pol}}$ has the strong Remak-Schmidt property.*

Proof. Let $\phi = (\phi_i)_i : \prod_{i=1}^r (X_i, \lambda_i) \xrightarrow{\sim} (X, \lambda)$ and $\phi' = (\phi'_j)_j : \prod_{i=1}^s (X'_j, \lambda'_j) \xrightarrow{\sim} (X, \lambda)$ be two decompositions of (X, λ) into indecomposable polarised abelian varieties. Let $(M, h) = (\mathrm{Hom}(E, X), h_\lambda)$ be the positive-definite Hermitian R-lattice associated to (X, λ). By Lemma 4.15, every (X_i, λ_i) and (X'_j, λ'_j) is an object in $\mathscr{A}_{E,\mathrm{ess}}^{\mathrm{pol}}$, and we let (M_i, h_i) and

(M'_j, h'_j) be the associated positive-definite Hermitian R-lattices, respectively. Applying the functor $\mathrm{Hom}(E, -)$, we obtain two decomposition of (M, h), namely $\phi_* : \prod_{i=1}^r (M_i, h_i) \xrightarrow{\sim} (M, h)$ and $\phi'_* : \prod_{j=1}^s (M'_j, h'_j) \xrightarrow{\sim} (M, h)$. Since the functor $(X, \lambda) \mapsto (M, h)$ from $\mathscr{A}_{E,\mathrm{ess}}^{\mathrm{pol}}$ to $\mathrm{Lat}_R^{\mathrm{H}}$ induces an equivalence of categories, every (M_i, h_i) and (M'_j, h'_j) is an indecomposable sublattice of (M, h). Therefore, there are two orthogonal decompostions of indecomposable sublattices of (M, h):

$$M = \perp_{i=1}^r \phi_*(M_i) \quad \text{and} \quad M = \perp_{j=1}^s \phi'_*(M'_j).$$

It follows from Theorem 2.1 that $r = s$ and that there is an permutation $\sigma \in S_r$ such that $\phi_*(M_i) = \phi'_*(M'_{\sigma(i)})$ for all i. For any i, let $\bar{\alpha}_i : (M_i, h_i) \xrightarrow{\sim} (M_{\sigma(i)}, h_{\sigma(i)})$ be the unique isomorphism such that $\phi'_{i,*} \circ \bar{\alpha}_i = \phi'_{\sigma(i),*}$. The unique lifted isomorphism of $\bar{\alpha}_i$, say $\alpha_i : (X_i, \lambda_i) \xrightarrow{\sim} (X'_{\sigma(i)}, \lambda'_{\sigma(i)})$, then satisfies $\phi_i = \phi'_{\sigma(i)} \circ \alpha_i$. □

Corollary 4.18. *Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$ such that Corollary 4.6 applies. Then every object $(X, \lambda) \in \mathscr{A}_E^{\mathrm{pol}}$ has the strong Remak-Schmidt property.*

Proof. This follows from Corollary 4.6 and Theorem 4.17. □

Remark 4.19. For the application of computing the automorphism groups of polarised abelian varieties, Theorem 4.17 and Corollary 4.18 actually do not provide any new useful information compared to Corollary 4.6. However, the significance of Theorem 4.17 lies in providing the possibility that there may be more polarised abelian varieties having the strong Remak-Schmidt property than those abelian varieties which can be described directly in terms of (skew-)Hermitian lattices. We have not yet seen this phenomenon explored in the literature.

Lemma 4.20. *Let $(X, \lambda) \in \mathscr{A}_E^{\mathrm{pol}}$ and let $\varphi : (\widetilde{X}, \widetilde{\lambda}) \to (X, \lambda)$ be the minimal E-isogeny of (X, λ), where $\widetilde{\lambda}$ is chosen to be $\varphi^*\lambda$. Then*

$$\mathrm{Aut}(X, \lambda) = \{\alpha \in \mathrm{Aut}(\widetilde{X}, \widetilde{\lambda}) : \alpha(H) = H\}, \tag{46}$$

where $H := \ker(\varphi)$ is the kernel of the morphism φ.

Proof. By the universal property of minimal E-isogenies, every $\sigma_0 \in \mathrm{Aut}(X, \lambda)$ uniquely lifts to an automorphism $\sigma \in \mathrm{Aut}(\widetilde{X}, \widetilde{\lambda})$. Since $X = \widetilde{X}/H$, an element $\sigma \in \mathrm{Aut}(\widetilde{X}, \widetilde{\lambda})$ descends to an element $\sigma_0 \in \mathrm{Aut}(X, \lambda)$ if and only if $\sigma(H) = H$. □

4.4. **Abelian varieties that are quotients of a power of an abelian variety over $\mathbb{F}_p$.**

In this subsection, we let E denote an abelian variety over $K = \mathbb{F}_p$ such that its endomorphism algebra $B = \mathrm{End}^0(E)$ is commutative. This means that E does not have a repeated simple factor (i.e., it is squarefree) nor a factor that is a supersingular abelian surface with Frobenius endomorphism $\sqrt{p}$. Since every abelian variety over a finite field is of CM type, the algebra B is a product of CM fields. Denote again by $a \mapsto \bar{a}$ the canonical involution of B. Let $R = \mathrm{End}(E)$ and fix a polarisation λ_E on E. We will use the same notation and terminology as in previous subsections, except that we let $\mathscr{A}_E$ (resp. $\mathscr{A}_E^{\mathrm{pol}}$) be the full subcategory of $\mathscr{A}$ (resp. $\mathscr{A}^{\mathrm{pol}}$) consisting of abelian varieties which are quotients of a power of E over $\mathbb{F}_p$.

Recall that an R-module M is called *reflexive* if the canonical map $M \to (M^t)^t$ is an isomorphism, where $M^t := \mathrm{Hom}_R(M, R)$. If $\mathbb{Z}[\pi_E, \bar{\pi}_E] = R$, where π_E denotes the Frobenius endomorphism of E, then R is Gorenstein and every R-lattice is automatically reflexive [6, Theorem 11 and Lemma 13].

Theorem 4.21. ([22, Theorem 8.1], [6, Theorem 25]) *Let E be an abelian variety over $\mathbb{F}_p$ as above and assume that $\mathbb{Z}[\pi_E, \bar{\pi}_E] = R$. Then the functor $\mathscr{H}om_R(-, E)$ induces an anti-equivalence of categories*

$$ {}_R\mathrm{Lat} \longrightarrow \mathscr{A}_E \tag{47}$$

and $\mathrm{Hom}(-, E)$ is its inverse functor. Moreover, the functor $\mathscr{H}om_R(-, E)$ is exact, and it is isomorphic to the Serre tensor functor $M \mapsto M^t \otimes B$.

Also see [49, Theorem 3.1] for a construction of a bijection from the set of isomorphism classes in ${}_R\mathrm{Lat}$ to that in $\mathscr{A}_E$. The category $\mathscr{A}_E$ contains more objects than those which are isogenous to a power of E in the case where E is not simple. Note that an abelian variety $X/\mathbb{F}_p$ lies in $\mathscr{A}_E$ if and only if there is a $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}[\pi_E] \to \mathbb{Q}[\pi_X]$ mapping π_E to the Frobenius endomorphism π_X of X. Let ${}_R\mathrm{Lat}^{\mathrm{f}}$ (resp. $\mathrm{Lat}^{\mathrm{f}}_R$) denote the full subcategary consisting of left (resp. right) R-lattices M such that $M \otimes \mathbb{Q}$ is a free B-module of finite rank. Similarly, let ${}_R\mathrm{Lat}^{\mathrm{f},H} \subseteq {}_R\mathrm{Lat}^{H}$ (resp. $\mathrm{Lat}^{\mathrm{f},H}_R \subseteq \mathrm{Lat}^{H}_R$) be the full subcategory of positive-definite Hermitian left (resp. right) R-lattices (M, h) with free B-module $M \otimes \mathbb{Q}$. The functor $\mathscr{H}om_R(-, E)$ induces an anti-equivalence from ${}_R\mathrm{Lat}^{\mathrm{f}}$ to the subcategory $\mathscr{A}^{\mathrm{f}}_E$ consisting of abelian varieties isogenous to a power of E. Moreover, we prove the following result about polarised varieties.

Theorem 4.22. *Let (E, λ_E) be a principally polarised abelian variety over $\mathbb{F}_p$ with the assumptions as in Theorem 4.21. Then the following hold.*

1. *The functor $(X, \lambda) \mapsto (M, h)$ introduced in Equations* (37) *and* (38) *induces an equivalence of categories*
$$\mathscr{A}^{\mathrm{pol}}_E \longrightarrow \mathrm{Lat}^H_R.$$
2. *For any $\mathbb{Q}$-polarised abelian variety (X, λ) over $\mathbb{F}_p$ in $\mathscr{A}^{\mathrm{pol}}_E$, the automorphism group $\mathrm{Aut}(X, \lambda)$ can be computed as in Equation* (42).
3. *Every $\mathbb{Q}$-polarised abelian variety (X, λ) over $\mathbb{F}_p$ in $\mathscr{A}^{\mathrm{pol}}_E$ has the strong Remak-Schmidt property.*

Proof. (1) We first show that (M, h) is a positive-definite Hermitian R-lattice. By Equations (39) and (40) in Lemma 4.4, h is Hermitian and it remains to show that h is positive-definite. Let E_i $(1 \leq i \leq r)$ be the simple abelian subvarieties of E and let $\varphi = \sum_i \iota_i : \prod_{i=1}^r E_i \to E$ be the canonical isogeny with inclusions $\iota_i : E_i \subseteq E$. Then we have an inclusion $M \subseteq \bigoplus_{i=1}^r M_i$, where $M_i = \mathrm{Hom}(E_i, X)$. Let λ_{E_i} be the restriction of the polarisation λ_E to E_i. The isogeny φ induces an isomorphism from $B \simeq \prod_i B_i$ onto a product of CM fields $B_i = \mathrm{End}^0(E_i)$, and the decomposition $M_{\mathbb{Q}} = \bigoplus_{i=1}^r M_{i,\mathbb{Q}}$ respects the decomposition $B \simeq \prod_i B_i$. Moreover, we have $(M_{\mathbb{Q}}, h) = \perp_{i=1}^r (M_{i,\mathbb{Q}}, h_i)$, where h_i is the restriction of h, which is also induced from the polarisation λ_{E_i}. Let $f = (f_i) \in M_{\mathbb{Q}}$ be a non-zero vector. Then $h(f, f) = (h_i(f_i, f_i))_i = (\lambda_{E_i}^{-1} f_i^* \lambda)_i$ and $\lambda_{E_i}^{-1} f_i^* \lambda$ is a totally positive element whenever $f_i \neq 0$. This shows that h is positive-definite. Then the same argument as in Proposition 4.5 proves the equivalence. Note that the principal polarisation λ_E ensures there is a natural isomorphism $\mathrm{Hom}(E, X^t) \simeq M^t$.

(2)+(3) These follow from Theorem 2.1 and Corollary 2.2 in the extended setting where B is a product of CM fields; see Remark 2.3.

□

Question 4.23. Is it true that any $\mathbb{Q}$-polarised abelian variety admits the strong Remak-Schmidt property?

5. The geometric theory: the Gauss problem for central leaves

5.1. First results and reductions.

Let $x = [(X_0, \lambda_0)] \in \mathscr{A}_g(k)$ be a point and let $\mathscr{C}(x)$ the central leaf passing through x.

Proposition 5.1 (Chai)**.** *The central leaf $\mathscr{C}(x)$ is finite if and only if X_0 is supersingular. In particular, a necessary condition for $|\mathscr{C}(x)| = 1$ is that $x \in \mathscr{S}_g(k)$.*

Proof. It is proved in [7, Proposition 1] that the prime-to-p Hecke orbit $\mathscr{H}^{(p)}(X_0, \lambda_0)$ (i.e., the points obtained from (X_0, λ_0) by polarised prime-to-p isogenies) is finite if and only if X_0 is supersingular. Since $\mathscr{H}^{(p)}(X_0, \lambda_0) \subseteq \mathscr{C}(x)$, the central leaf $\mathscr{C}(x)$ is finite only if X_0 supersingular. When X_0 is supersingular, we have $\mathscr{C}(x) = \Lambda_x$ by definition and hence $\mathscr{C}(x)$ is finite, cf. (19) . □

From now on we assume that $x \in \mathscr{S}_g(k)$. In this case

$$\mathscr{C}(x) = \Lambda_x \simeq G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_x,$$

where $U_x = G_x(\widehat{\mathbb{Z}})$ is an open compact subgroup. Similarly, for $0 \leq c \leq [g/2]$ we have

$$\Lambda_{g,p^c} \simeq G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{g,p^c},$$

where $U_{g,p^c} = G_{x_c}(\widehat{\mathbb{Z}})$ for a base point $x_c \in \Lambda_{g,p^c}$.

Lemma 5.2. *For every point $x \in \mathscr{S}_g(k)$, there exists a (non-canonical) surjective morphism $\pi : \Lambda_x \twoheadrightarrow \Lambda_{g,p^c}$ for some integer c with $0 \leq c \leq \lfloor g/2 \rfloor$. Moreover, one can select a base point x'_c in Λ_{g,p^c} so that $G_x(\mathbb{Z}_p)$ is contained in $G_{x'_c}(\mathbb{Z}_p)$ and π is induced from the the identity map*

$$G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_x \longrightarrow G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{x'_c}. \tag{48}$$

Proof. We have

$$G_{x_c}(\mathbb{Z}_p) \simeq \mathrm{Aut}_{G^1(\mathbb{Q}_p)}(\Pi_p O_p)^{n-c} \oplus O_p^c, \mathbb{J}_g) =: P_c.$$

By [41, Theorem 3.13, p. 150], the subgroups P_c for $c = 1, \ldots, [g/2]$ form a complete set of representatives of maximal parahoric subgroups of $G^1(\mathbb{Q}_p)$ up to conjugacy. So $G_x(\mathbb{Z}_p)$ is contained in $g_p^{-1} G_{x_c}(\mathbb{Z}_p) g_p$ for some integer c with $0 \leq c \leq \lfloor g/2 \rfloor$ and some element $g_p \in G^1(\mathbb{Q}_p)$. Thus, we we have a surjective map

$$G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_x \twoheadrightarrow G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/g_p^{-1} U_{g,p^c} g_p \xrightarrow{\cdot g_p} G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{g,p^c}. \tag{49}$$

This gives a surjective map $\Lambda_x \twoheadrightarrow \Lambda_{g,p^c}$. □

Let $\varphi : \widetilde{x} = (\widetilde{X}_0, \widetilde{\lambda}_0) \to x = (X_0, \lambda_0)$ the be minimal isogeny for x, cf. [23, Definition 2.11] and [31, Lemma 1.8]. Then $U_x \subseteq U_{\widetilde{x}}$ and we have a surjective map $\Lambda_x \twoheadrightarrow \Lambda_{\widetilde{x}}$ which is induced from the natural map

$$G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_x \longrightarrow G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{\widetilde{x}}. \tag{50}$$

If the open compact subgroup $U_{\widetilde{x}}$ is maximal, then $U_{\widetilde{x}}$ is conjugate to U_{g,p^c} for some $0 \leq c \leq \lfloor g/2 \rfloor$ and the map $\pi : \Lambda_x \twoheadrightarrow \Lambda_{g,p^c}$ in Lemma 5.2 is realised by the minimal isogeny φ.

Lemma 5.3. *Let x be a point in $\mathscr{S}_g(k)$. If $g = 1$, then $|\Lambda_x| = 1$ if and only if $p \in \{2, 3, 5, 7, 13\}$.*

Proof. In this case, the orbit Λ_x is the supersingular locus $\Lambda_{1,1}$. The assertion is well-known and also follows from Theorem 2.9.(1). □

Lemma 5.4. *Let x be a point in $\mathscr{S}_g(k)$. If $g = 2$, then $|\Lambda_x| = 1$ if and only if $p \in \{2, 3\}$.*

Proof. For the superspecial case, by the first part of Theorem 2.9.(2) we have $H_2(p,1) = 1$ if and only if $p = 2, 3$. For the non-superspecial case, it follows from Theorem 3.3.(3) that $|\Lambda_x| = 1$ for every non-superspecial point $x \in \mathscr{S}_2(k)$ if and only if $p = 2, 3$. □

Lemma 5.5. *Let x be a point in $\mathscr{S}_g(k)$. If $g \geq 5$, then $|\Lambda_x| > 1$.*

Proof. We first show that $|\Lambda_{g,p^c}| > 1$ for all primes p and all integers c with $0 \leq c \leq \lfloor g/2 \rfloor$. From Theorem 3.1 we have $\mathrm{Mass}(\Lambda_{g,p^c}) = v_g \cdot L_{p,p^c}$. Using Lemma 2.6 and the proof of Corollary 2.7, we show that $|\Lambda_{g,p^c}| > 1$ for all $g \geq 6$, all primes p and all c. By Theorem 2.9, we have $|\Lambda_{5,p^0}| = H_5(p,1) > 1$ and $|\Lambda_{5,p^2}| = H_5(1,p) > 1$ for all primes p. Using Theorem 3.1 and (25), we have $\mathrm{Mass}(\Lambda_{5,p}) = v_5 \cdot L_{5,p^1} = \mathrm{Mass}(\Lambda_{5,p^0})(p^5+1)$ and (p^3-1) divides $L_{5,p}$. From this the same proof of Theorem 2.9 shows that $|\Lambda_{5,p}| > 1$ for all primes p. By Lemma 5.2, for every point $x \in \mathscr{S}_g(k)$ we have $|\Lambda_x| \geq |\Lambda_{g,p^c}|$ for some $0 \leq c \leq \lfloor g/2 \rfloor$. Therefore, $|\Lambda_x| > 1$. □

For any matrix $A = (a_{ij}) \in \mathrm{Mat}_g(\mathbb{F}_{p^2})$, write $A^* = \overline{A}^T = (a_{ji}^p)$, where $\overline{A} = (a_{ij}^p)$ and T denotes the transpose. Let

$$U_g(\mathbb{F}_p) := \{A \in \mathrm{Mat}_g(\mathbb{F}_{p^2}) : A \cdot A^* = \mathbb{I}_g\}$$

denote the unitary group of rank g associated to the quadratic extension $\mathbb{F}_{p^2}/\mathbb{F}_p$. Let $\mathrm{Sym}_g(\mathbb{F}_{p^2}) \subseteq \mathrm{Mat}_g(\mathbb{F}_{p^2})$ be the subspace consisting of all symmetric matrices and $\mathrm{Sym}_g(\mathbb{F}_{p^2})^0 \subseteq \mathrm{Sym}_g(\mathbb{F}_{p^2})$ be the subspace consisting of matrices $B = (b_{ij})$ with $b_{ii} = 0$ for all i.

Definition 5.6. Let $\mathscr{E} \subseteq \mathrm{Mat}_g(\mathbb{F}_{p^2})$ be a maximal subfield of degree g over $\mathbb{F}_{p^2}$ stable under the involution $*$. Let

$$G := \left\{ \begin{pmatrix} \mathbb{I}_g & 0 \\ B & \mathbb{I}_g \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} \in \mathrm{GL}_{2g}(\mathbb{F}_{p^2}) : A \in U_g(\mathbb{F}_p), B \in \mathrm{Sym}_g(\mathbb{F}_{p^2}) \right\}; \tag{51}$$

$$\mathscr{E}^1 := \{A \in \mathscr{E}^\times : A^*A = \mathbb{I}_g\} = \mathscr{E}^\times \cap U_g(\mathbb{F}_p); \tag{52}$$

$$H := \left\{ \begin{pmatrix} \mathbb{I}_g & 0 \\ B & \mathbb{I}_g \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} : A \in \mathscr{E}^1, \quad B \in \mathrm{Sym}_g(\mathbb{F}_{p^2})^0 \right\}; \tag{53}$$

$$\Gamma := \left\{ \begin{pmatrix} \mathbb{I}_g & 0 \\ B & \mathbb{I}_g \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} : A \in \mathrm{diag}(\mathbb{F}_{p^2}^1, \ldots, \mathbb{F}_{p^2}^1) \cdot S_g,\ B \in \mathrm{diag}(\mathbb{F}_{p^2}, \ldots, \mathbb{F}_{p^2}) \right\}, \tag{54}$$

where $\mathbb{F}_{p^2}^1 \subseteq \mathbb{F}_{p^2}^\times$ denotes the subgroup of norm one elements and S_g denotes the symmetric group of $\{1, \ldots, g\}$.

Lemma 5.7. *Using the notation introduced in Definition 5.6, the following statements hold.*

1. *Up to isomorphism, the double coset space $(\mathrm{diag}(\mathbb{F}_{p^2}^1, \ldots, \mathbb{F}_{p^2}^1) \cdot S_g)\backslash U_g(\mathbb{F}_p)/\mathscr{E}^1$ is independent of the choice of $\mathscr{E}$.*
2. *For $p = 2$, up to isomorphism, the double coset space $\Gamma\backslash G/H$ is independent of the choice of $\mathscr{E}$.*

Proof. (1) We know that $\mathscr{E}^1$ is a cyclic group of order $p^g + 1$ and choose a generator η of $\mathscr{E}^1$. One has $\eta^*\eta = 1$ and $\mathscr{E} = \mathbb{F}_{p^2}[\eta]$. Suppose that $\mathscr{E}_1$ is another maximal subfield stable under $*$. We will first show that $\mathscr{E}_1$ is conjugate to $\mathscr{E}$ under $U_g(\mathbb{F}_p)$. By the Noether-Skolem theorem, there is an element $\gamma \in \mathrm{GL}_g(\mathbb{F}_{p^2})$ such that $\mathscr{E}_1 = \gamma\mathscr{E}\gamma^{-1}$. Clearly, $\mathscr{E}_1 = \mathbb{F}_{p^2}[\eta_1]$ is generated by $\eta_1 := \gamma\eta\gamma^{-1}$ and η_1 has order $p^g + 1$. We also have $\eta_1^*\eta_1 = 1$; this follows from the fact that the norm-one subgroup $\mathscr{E}_1^1 \subseteq \mathscr{E}_1^\times$ is the unique subgroup of order $p^g + 1$ and that η_1 has order $p^g + 1$. It follows from $\eta^*\eta = 1$ that $\gamma^*\eta^*\gamma^*\gamma\eta\gamma^{-1} = 1$. Putting $\alpha = \gamma^*\gamma$, we find that

$$\eta^*\alpha\eta = \alpha \quad \text{and} \quad \alpha\eta\alpha^{-1} = \eta.$$

That is, α commutes with $\mathscr{E}$, and $\alpha \in \mathscr{E}^\times$ because $\mathscr{E}$ is a maximal subfield. As $\alpha = \gamma^*\gamma$, α lies in the subfield $F \subseteq \mathscr{E}$ fixed by the automorphism $*$ of order 2. Since the norm map $N : \mathscr{E}^\times \to F^\times, x \mapsto x^*x$ is surjective, we have $\alpha = \beta^*\beta$ for some $\beta \in \mathscr{E}^\times$. Let $\gamma_1 := \gamma\beta^{-1}$. Then

$$\gamma_1^*\gamma_1 = (\gamma\beta^{-1})^*(\gamma\beta^{-1}) = (\beta^{-1})^*\gamma^*\gamma\beta^{-1} = (\beta^{-1})^*\alpha\beta^{-1} = (\beta^{-1})^*\beta^*\beta\beta^{-1} = 1.$$

Therefore, $\mathscr{E}_1 = \gamma_1\mathscr{E}\gamma_1^{-1}$ and $\gamma_1 \in U_g(\mathbb{F}_p)$. The right translation by γ_1^{-1} gives an isomorphism $(\mathrm{diag}(\mathbb{F}^1_{p^2}, \dots, \mathbb{F}^1_{p^2})\cdot S_g)\backslash U_g(\mathbb{F}_p)/\mathscr{E}^1 \simeq (\mathrm{diag}(\mathbb{F}^1_{p^2}, \dots, \mathbb{F}^1_{p^2})\cdot S_g)\backslash U_g(\mathbb{F}_p)/\mathscr{E}_1^1$. This proves (1).

(2) We may regard $U_g(\mathbb{F}_p)$ as a subgroup of G via the map $A \mapsto \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix}$. Conjugation by G gives an action of $U_g(\mathbb{F}_p)$ on $\mathrm{Sym}_g(\mathbb{F}_{p^2})$ by $A \cdot B = \overline{A}B\overline{A}^T$, where $A \in U(\mathbb{F}_p)$ and $B \in \mathrm{Sym}_g(\mathbb{F}_{p^2})$. Suppose that $\mathscr{E}_1$ is another maximal subfield stable under $*$ and $H_1 \subseteq G$ is the extension of $\mathrm{Sym}_g(\mathbb{F}_{p^2})^0$ by $\mathscr{E}_1^1$. To show H_1 is conjugate to H under G, it suffices to show they are conjugate under $U_g(\mathbb{F}_p)$, since this is a subgroup of G. By (1), it then suffices to show that $\mathrm{Sym}_g(\mathbb{F}_{p^2})^0$ is stable under the action of $U_g(\mathbb{F}_p)$. When $p = 2$, one checks directly that the diagonal entries of the matrix $A(I_{ij} + I_{ji})\overline{A}^T$ are all zero, where I_{ij} is the matrix whose entries are 1 at (i, j) and zero elsewhere. Since the $I_{ij} + I_{ji}$ generate $\mathrm{Sym}_g(\mathbb{F}_{p^2})^0$, we find that it is indeed stable under the action of $U_g(\mathbb{F}_p)$. This proves (2).

□

Let $\mathbb{F}_q$ be a finite field of characteristic p. Let (V_0, ψ_0) be a non-degenerate symplectic space over $\mathbb{F}_q$ of dimension $2c$ and denote by $A \mapsto A^\dagger$ the symplectic involution on $\mathrm{End}(V_0)$ with respect to ψ_0. For any k-subspace W of $V_0 \otimes_{\mathbb{F}_q} k$, the endomorphism algebra of W over $\mathbb{F}_q$ is defined as

$$\mathrm{End}(V_0, W) := \{A \in \mathrm{End}(V_0) : A(W) \subseteq W\}, \tag{55}$$

and the automorphism group of W in the symplectic group $\mathrm{Sp}(V_0)$ is defined as

$$\mathrm{Sp}(V_0, W) := \mathrm{Sp}(V_0) \cap \mathrm{End}(V_0, W). \tag{56}$$

Proposition 5.8. *If W is a non-zero isotropic k-subspace of $V_0 \otimes_{\mathbb{F}_q} k$ such that $\mathrm{Sp}(V_0, W) \supseteq C_{q^c+1}$, then $\mathrm{End}(V_0, W) \simeq \mathrm{Mat}_{2c/d}(\mathbb{F}_{q^d})$ for some positive integer $d|2c$ such that $\mathrm{ord}_2(d) = \mathrm{ord}_2(2c)$. Moreover, if $2c$ is a power of 2, then $\mathrm{End}(V_0, W) \simeq \mathbb{F}_{q^{2c}}$ and $\mathrm{Sp}(V_0, W) = C_{q^c+1}$.*

Proof. Let η be a generator of C_{q^c+1} and let $\mathscr{E} = \mathbb{F}_q[\eta]$ be the $\mathbb{F}_q$-subalgebra of $\mathrm{End}(V_0)$ generated by η. Since $|C_{q^c+1}|$ is prime to q, the group algebra $\mathbb{F}_q[C_{q^c+1}]$ is semi-simple and it maps onto $\mathscr{E}$. On the other hand, the finite field $\mathbb{F}_{q^{2c}}$ is the smallest field extension of $\mathbb{F}_q$ which contains an element of order $q^c + 1$, so $\mathscr{E}$ contains a copy F of $\mathbb{F}_{q^{2c}}$ in $\mathrm{End}(V_0)$. Since $\dim V_0 = 2c = [\mathbb{F}_{q^{2c}} : \mathbb{F}_q]$, we see that F is a maximal subfield of $\mathrm{End}(V_0)$ and hence $\mathscr{E} = F$.

Since $C_{q^c+1} \subseteq \mathrm{Sp}(V_0)$ and $\mathrm{ord}(\eta) = q^c + 1$, we have that $\eta^\dagger = \eta^{-1} \in C_{q^c+1}$ and $\eta^\dagger \neq \eta$. So $\mathscr{E}$ is stable under $\dagger$, and $\dagger$ is an automorphism of $\mathscr{E}$ of order 2. Moreover, C_{q^c+1} is equal to the subgroup $\mathscr{E}^1 = \{a \in \mathscr{E}^\times : N_{\mathscr{E}/\mathscr{E}_0}(a) = 1\}$ of norm one elements in $\mathscr{E}^\times$, where $\mathscr{E}_0$ is the subfield of $\mathscr{E}$ fixed by $\dagger$.

Let $\Sigma_{\mathscr{E}} := \mathrm{Hom}_{\mathbb{F}_q}(\mathscr{E}, \overline{\mathbb{F}}_p)$ denote the set of embeddings of $\mathscr{E}$ into $\overline{\mathbb{F}}_p$; it is equipped with a left action by $\mathrm{Gal}(\overline{\mathbb{F}}_{q^{2c}}/\mathbb{F}_q) = \mathrm{Gal}(\mathscr{E}/\mathbb{F}_q) = \langle\sigma\rangle \simeq \mathbb{Z}/2c\mathbb{Z}$, which acts simply transitively. Arrange $\Sigma_{\mathscr{E}} = \{\sigma_i : i \in \mathbb{Z}/2c\mathbb{Z}\}$ in such a way that $\sigma \cdot \sigma_i = \sigma_{i+1}$ for all $i \in \mathbb{Z}/2c\mathbb{Z}$ and denote by V^i the σ_i-isotypic eigenspace of $V_0 \otimes k$. Then $V_0 \otimes_{\mathbb{F}_q} k = \oplus_{i\in\mathbb{Z}/2c\mathbb{Z}} V^i$ is a decomposition into simple $(\mathscr{E} \otimes_{\mathbb{F}_q} k)$-submodules. Since $W \subseteq V_0 \otimes_{\mathbb{F}_q} k$ is an $(\mathscr{E} \otimes_{\mathbb{F}_q} k)$-submodule, there is

a unique and non-empty subset $J \subseteq \mathbb{Z}/2c\mathbb{Z}$ such that $W = \oplus_{i\in J} V^i$. Note that the involution $\dagger$ acts on $\Sigma_{\mathscr{E}}$ from the right and one has $\sigma_i^\dagger = \sigma_{i+c}$.

We claim that $J \cap J^\dagger = \emptyset$. For $i, j \in \mathbb{Z}/2c\mathbb{Z}$, one computes that

$$\sigma_i(a)\psi(v_1, v_2) = \psi(a \cdot v_1, v_2) = \psi(v_1, a^\dagger \cdot v_2) = \sigma_{j+c}(a)\psi(v_1, v_2)$$

for any $a \in \mathscr{E}$, $v_1 \in V^i$ and $v_2 \in V^j$. It follows that $\psi(V^i, V^j) = 0$ if $i - j \neq c$ in $\mathbb{Z}/2c\mathbb{Z}$. Since ψ is non-degenerate, the latter is also a necessary condition. Since W is isotropic, J does not contain $\{i, i + c\}$ for any i and therefore $J \cap J^\dagger = \emptyset$, as claimed.

We represent the matrix algebra $\mathrm{End}(V_0)$ over $\mathbb{F}_q$ as a cyclic algebra, cf. [42, Theorem 30.4]:

$$\mathrm{End}(V_0) = \mathscr{E}[z], \qquad z^{2c} = 1, zaz^{-1} = \sigma(a) \text{ for all } a \in \mathscr{E}.$$

Multiplication by z maps V^i onto V^{i-1}:

$$a \cdot zv = z(\sigma^{-1}(a) \cdot v) = z\sigma_{i-1}(a)v = \sigma_{i-1}(a)zv, \quad \forall\, a \in \mathscr{E}, v \in V^i.$$

Consider an element $x = \sum_{i\in\mathbb{Z}/2c\mathbb{Z}} a_i z^i \in \mathrm{End}(V_0, W)$; if $a_i \neq 0$, then J is stable under the shift by $-i$. Let $d \geq 1$ be the smallest integer with $d|2c$ such that J is stable under the shift by $-d$. Then $\mathrm{End}(V_0, W) = \mathscr{E}[z^d] \simeq \mathrm{Mat}_{2c/d}(\mathbb{F}_{q^d})$. Since $J \cap J^\dagger = \emptyset$, we have $d \nmid c$, Therefore, d is a positive divisor of $2c$ such that $\mathrm{ord}_2(d) = \mathrm{ord}_2(2c)$. This proves the first statement. When $2c$ is a power of 2, the condition on d implies $d = 2c$ and therefore $\mathrm{End}(V_0, W) = \mathscr{E}$. This implies that $\mathrm{Sp}(V_0, W) = \mathscr{E}^1 = C_{q^c+1}$ and hence proves the second statement. □

5.2. The case $g = 3$.

Lemma 5.9. *We use the notation for G, Γ, H defined in Definition 5.6. For $g = 3$ and $p = 2$, we have $|\Gamma\backslash G/H| = 2$.*

Proof. Put $U := \mathrm{Sym}_g(\mathbb{F}_{p^2})$, embedded into $\mathrm{GL}_{2g}(\mathbb{F}_{p^2})$ via $B \mapsto \left(\begin{smallmatrix} \mathbb{I}_g & 0 \\ B & \mathbb{I}_g \end{smallmatrix}\right)$. Then $U_\Gamma := U \cap \Gamma \simeq \mathrm{diag}(\mathbb{F}_{p^2}, \ldots, \mathbb{F}_{p^2})$ and $U_H := U \cap H \simeq \mathrm{Sym}_g(\mathbb{F}_{p^2})^0$. Consider the surjective map induced by the natural projection

$$\mathrm{pr} : \Gamma\backslash G/H \to (\mathrm{diag}(\mathbb{F}_{p^2}^1, \ldots, \mathbb{F}_{p^2}^1) \cdot S_g)\backslash U_g(\mathbb{F}_p)/\mathscr{E}^1.$$

One shows directly that the fibre of the double coset $(\mathrm{diag}(\mathbb{F}_{p^2}^1, \ldots, \mathbb{F}_{p^2}^1) \cdot S_g) \cdot A \cdot \mathscr{E}^1$ for an element $A \in U_g(\mathbb{F}_p)$ is isomorphic to $U_\Gamma + \overline{A}U_H\overline{A}^T$. Since $\overline{A}U_H\overline{A}^T = U_H$ for $p = 2$ by Lemma 5.7.(2), we have $U_\Gamma + \overline{A}U_H\overline{A}^T = U_\Gamma + U_H = U$ and hence pr is an isomorphism.

Now let $g = 3$ and $p = 2$; we need to show that the target of pr has two double cosets. Put $\mathbb{F}_4 = \mathbb{F}_2[\zeta]$ with $\zeta^2 + \zeta + 1 = 0$ and

$$\eta := \begin{pmatrix} 0 & 0 & \zeta \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A := \begin{pmatrix} 1 & \zeta & \zeta \\ \zeta & 1 & \zeta \\ \zeta & \zeta & 1 \end{pmatrix}. \tag{57}$$

We choose $\mathscr{E}^1 = \langle\eta\rangle$ and verify directly that

$$U_3(\mathbb{F}_2) = \Big(\mathrm{diag}(\mathbb{F}_4^\times, \mathbb{F}_4^\times, \mathbb{F}_4^\times)S_3 \cdot 1 \cdot \mathscr{E}^1\Big) \coprod \Big(\mathrm{diag}(\mathbb{F}_4^\times, \mathbb{F}_4^\times, \mathbb{F}_4^\times)S_3 \cdot A \cdot \mathscr{E}^1\Big).$$

This shows that $|\Gamma\backslash G/H| = 2$; recall from Lemma 5.7.(2) that the double coset space is independent of the choices made. □

Proposition 5.10. *Let $p = 2$, let $x = (X, \lambda) \in \mathscr{S}_3(k)$ with $a(x) = 1$ and let $y = (t, u) \in \mathscr{P}'_\mu(k)$ be a point over x for the unique element $\mu = \mu_{\mathrm{can}}$ in $P(E^3)$. Assume that $y \in \mathscr{D}$ and $t \in C(\mathbb{F}_{p^6})$. Then $|\Lambda_x| = 2$. Moreover, the two members (X', λ') and (X'', λ'') of Λ_x have automorphism groups*

$$\mathrm{Aut}(X', \lambda') \simeq C_2^3 \rtimes C_9, \quad \mathrm{Aut}(X'', \lambda'') \simeq C_2^3 \times C_3,$$

where C_9 acts on C_2^3 by a cyclic shift.

Proof. Let $x_2 = (X_2, \lambda_2) \to x = (X, \lambda)$ be the minimal isogeny for (X, λ). As $a(X) = 1$ and the class number $H_3(2, 1) = 1$, we have $(X_2, \lambda_2) \simeq (E^3, p\mu_{\mathrm{can}})$. Again using $H_3(2, 1) = 1$, one has $|G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{x_2}| = 1$ so $G^1(\mathbb{A}_f) = G^1(\mathbb{Q})U_{x_2}$; recall that $U_x = G_x(\widehat{\mathbb{Z}})$ for any x. Hence,

$$\Lambda_x \simeq G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_x = G^1(\mathbb{Q})\backslash G^1(\mathbb{Q})U_{x_2}/U_x = G^1(\mathbb{Z})\backslash G_{x_2}(\mathbb{Z}_p)/G_x(\mathbb{Z}_p),$$

where $G^1(\mathbb{Z}) = G^1(\mathbb{Q}) \cap U_{x_2} = \mathrm{Aut}(X_2, \lambda_2)$, as $G_{x_2}(\mathbb{Z}_\ell) = G_x(\mathbb{Z}_\ell)$ for all primes $\ell \neq p$.

Let $\underline{M}_2 = (M_2, \langle\,,\rangle_2)$ and $\underline{M} = (M, \langle\,,\rangle)$ be the polarised Dieudonné modules associated to (X_2, λ_2) and (X, λ), respectively. Regarding $G_{x_2}(\mathbb{Z}_p) = \mathrm{Aut}_{\mathrm{DM}}(\underline{M}_2)$, we have a reduction-modulo-p map:

$$m_p : G_{x_2}(\mathbb{Z}_p) = \mathrm{Aut}_{\mathrm{DM}}(\underline{M}_2) \to \mathrm{Aut}(M_2/pM_2);$$

we write $G_{\underline{M}_2}$ for its image. For $G_x(\mathbb{Z}_p) = \mathrm{Aut}_{\mathrm{DM}}(\underline{M})$ it then follows from the construction that

$$G_x(\mathbb{Z}_p) = \{h \in G_{x_2}(\mathbb{Z}_p) : m_p(h)(M/pM_2) = M/pM_2\}.$$

Therefore, $G_x(\mathbb{Z}_p)$ contains the kernel $\ker(m_p) \subseteq G_{x_2}(\mathbb{Z}_p)$ and we obtain

$$\Lambda_x \simeq \Gamma\backslash G_{\underline{M}_2}/G_{\underline{M}}, \tag{58}$$

where $G_{\underline{M}}$ is the image $m_p(G_x(\mathbb{Z}_p))$ and $\Gamma := m_p(G^1(\mathbb{Z}))$. It follows from [23, Lemma 6.1] that reduction modulo p gives an exact sequence

$$1 \longrightarrow C_2^3 \longrightarrow \mathrm{Aut}(X_2, \lambda_2) \xrightarrow{m_p} \Gamma \longrightarrow 1.$$

Let $O = \mathrm{End}(E)$ be a maximal order of $\mathrm{End}^0(E) \simeq B_{p,\infty}$ and let $\Pi \in O$ be the Frobenius endomorphism. Clearly, $G_{\underline{M}_2} = m_p(\mathrm{Aut}_{\mathrm{DM}}(\underline{M}_2))$ is a subgroup of $\mathrm{GL}_3(O/pO) = \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi])$. In fact, the group $G_{\underline{M}_2}$ is isomorphic to the group G of Definition 5.6; cf. [23, Definition 5.3]. By further reduction modulo Π, we obtain an exact sequence

$$1 \longrightarrow U := \mathrm{Sym}_3(\mathbb{F}_4) \longrightarrow G_{\underline{M}_2} \xrightarrow{m_\Pi} U_3(\mathbb{F}_2) \longrightarrow 1.$$

Let $\mathscr{E}$ be the image of $\mathrm{End}_{\mathrm{DM}}(\underline{M})$ in $m_\Pi(\mathrm{End}_{\mathrm{DM}}(\underline{M}_2))$. Since $p = 2$ and $t \in C(\mathbb{F}_{2^6})$, $\mathscr{E} \simeq \mathbb{F}_{4^3}$ is a subalgebra of $\mathrm{Mat}_3(\mathbb{F}_4)$ of degree 3 which is stable under the induced involution $*$, and $U \cap G_{\underline{M}} = \mathrm{Sym}_3(\mathbb{F}_4)^0$. Therefore, $G_{\underline{M}}$ is isomorphic to the group H in Definition 5.6. As

$$G^1(\mathbb{Z}) = \mathrm{Aut}(X_2, \lambda_2) \simeq \mathrm{Aut}(E^3, \mu_{\mathrm{can}}) \simeq (O^\times)^3 \cdot S_3,$$

we further see that Γ is the same as in Definition 5.6. So by Lemma 5.9, for $x = (X, \lambda)$, the set

$$\Lambda_x \simeq \Gamma\backslash G/H \text{ has two elements,}$$

represented by

$$(X', \lambda') \leftrightarrow G^1(\mathbb{Z}) \cdot 1 \cdot G_x(\mathbb{Z}_p) \text{ and } (X'', \lambda'') \leftrightarrow G^1(\mathbb{Z}) \cdot \widetilde{A} \cdot G_x(\mathbb{Z}_p), \tag{59}$$

where $\widetilde{A}$ is a lift of A as in Equation (57). That is, we may take

$$\widetilde{A} := \frac{1}{a}\begin{pmatrix} 1 & \zeta & \zeta \\ \zeta & 1 & \zeta \\ \zeta & \zeta & 1 \end{pmatrix}, \text{ for } 1 \neq \zeta \in O^\times \text{ such that } \zeta^3 = 1 \text{ and } a = 2 + \zeta \in O.$$

The coset representation in (59) also immediately implies that

$$\mathrm{Aut}(X', \lambda') \simeq G^1(\mathbb{Z}) \cap G_x(\mathbb{Z}_p) \text{ and } \mathrm{Aut}(X'', \lambda'') \simeq G^1(\mathbb{Z}) \cap \widetilde{A}G_x(\mathbb{Z}_p)\widetilde{A}^{-1}.$$

The group $G^1(\mathbb{Z}) \cap G_x(\mathbb{Z}_p)$ sits in the short exact sequence

$$1 \longrightarrow C_2^3 \longrightarrow G^1(\mathbb{Z}) \cap G_x(\mathbb{Z}_p) \xrightarrow{m_\Pi} \mathscr{E}^1 \longrightarrow 1$$

and one has $|\operatorname{Aut}(X',\lambda')| = 8\cdot 9$. From the mass $\operatorname{Mass}(\Lambda_x) = 1/(2\cdot 3^2)$ and the fact that $|\Lambda_x| = 2$, we immediately see that $|\operatorname{Aut}(X'',\lambda'')| = 8\cdot 3$.

To determine the automorphism groups precisely, we argue as follows. We have that $x = (X,\lambda)$ either equals (X',λ') or equals (X'',λ''). In either case, the group $\operatorname{Aut}(X,\lambda)$ is the subgroup of $\operatorname{Aut}(X_2,\lambda_2)$ consisting of elements h such that $m_p(h) \in H$. Since $U_\Gamma \cap U_H = 0$, its image $m_p(\operatorname{Aut}(X,\lambda))$ is the same as its image $m_\Pi(\operatorname{Aut}(X,\lambda)) \subseteq \mathscr{E}^1 \simeq C_9$. Moreover, we know that $G^1(\mathbb{Z}) = (O^\times)^3\cdot S_3$ and that

$$G_x(\mathbb{Z}_p) = m_p^{-1}(H) = m_p^{-1}(\operatorname{Sym}_3(\mathbb{F}_4)^0\mathscr{E}^1) = m_\Pi^{-1}(\mathscr{E}^1),$$

where

$$C_2^3 \simeq \operatorname{diag}(\pm 1,\pm 1,\pm 1) = \ker(m_p)\cap (O^\times)^3\cdot S_3 \subseteq \ker(m_\Pi)\cap (O^\times)^3\cdot S_3$$

and $C_9 \simeq \mathscr{E}^1 = \langle \eta\rangle \subseteq (O^\times)^3\cdot S_3$ by construction. For (X',λ') we therefore must have

$$\operatorname{Aut}(X',\lambda') \simeq G^1(\mathbb{Z})\cap G_x(\mathbb{Z}_p) = C_2^3 \rtimes C_9$$

of cardinality $8\cdot 9$, since the conjugation action by η on $\operatorname{diag}(\pm 1,\pm 1,\pm 1)$ is non-trivial.

For (X'',λ''), we note that $\widetilde{A} \in G_{x_2}(\mathbb{Z}_p)$ normalises $\ker(m_\Pi) = m_p^{-1}(\operatorname{Sym}_3(\mathbb{F}_4)^0)$ by construction and compute that

$$\widetilde{A}\eta\widetilde{A}^{-1} = \frac{1}{2+\overline{\zeta}}\begin{pmatrix} 1 & 1 & 1\\ 1 & \zeta & \overline{\zeta}\\ \zeta & 1 & \overline{\zeta}\end{pmatrix} =: B,$$

where $\overline{\zeta} = \zeta^{-1}$. Hence, we get

$$\operatorname{Aut}(X'',\lambda'') \simeq G^1(\mathbb{Z})\cap \widetilde{A}G_x(\mathbb{Z}_p)\widetilde{A}^{-1} = \operatorname{diag}(\pm 1,\pm 1,\pm 1)\cdot\{B^3, B^6, B^9 = 1\} \simeq C_2^3\times C_3$$

of cardinality $8\cdot 3$, since the conjugation action by $\{1, B^3, B^6\}$ is trivial. □

Proposition 5.11. *Let $p = 2$, choose $x = (X,\lambda) \in \mathscr{S}_3(k)$ and let $y = (t,u) \in \mathscr{P}'_\mu(k)$ be a point over x for the unique element $\mu = \mu_{\mathrm{can}}$ in $P(E^3)$.*

(1) *Suppose that $t \in C(\mathbb{F}_{p^2})$, that is, $a(x) \geq 2$. Then $|\Lambda_x| = 1$ and we have that*

$$|\operatorname{Aut}(X,\lambda)| = \begin{cases} 24^3\cdot 6 = 2^{10}\cdot 3^4 & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^2});\\ 24\cdot 160 = 2^8\cdot 3\cdot 5 & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4})\setminus \mathbb{P}^1_t(\mathbb{F}_{p^2});\\ 24\cdot 32 = 2^8\cdot 3 & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}).\end{cases} \tag{60}$$

(2) *Suppose that $t \notin C(\mathbb{F}_{p^2})$, that is, $a(x) = 1$. Then*

$$|\Lambda_x| = \begin{cases} 4 & \text{if } y \notin \mathscr{D};\\ 4 & \text{if } t \notin C(\mathbb{F}_{p^6}) \text{ and } y \in \mathscr{D};\\ 2 & \text{if } t \in C(\mathbb{F}_{p^6}) \text{ and } y \in \mathscr{D}.\end{cases} \tag{61}$$

Proof. (1) If $u \in \mathbb{P}^1_t(\mathbb{F}_{p^2})$, then $a(x) = 3$ and $|\Lambda_x| = H_3(2,1) = 1$, and one computes that $\operatorname{Mass}(\Lambda_x) = 1/(2^{10}\cdot 3^4)$. Therefore, $|\operatorname{Aut}(X,\lambda)| = 24^3\cdot 6$. Alternatively, this also follows from [23, Lemma 7.1]. Now we assume that $a(x) = 2$. Using the mass formula (cf. Theorem 3.8), we compute that

$$\operatorname{Mass}(\Lambda_x) = \begin{cases} 1/(2^8\cdot 3\cdot 5) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4})\setminus \mathbb{P}^1_t(\mathbb{F}_{p^2});\\ 1/(2^8\cdot 3) & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}).\end{cases} \tag{62}$$

Let $(E_k^3, p\mu) \xrightarrow{\rho_2} (Y_1,\lambda_1) \xrightarrow{\rho_1} (Y_0,\lambda_0) \simeq (X,\lambda)$ be the PFTQ corresponding to the point $y = (t,u)$. Since $t \in C(\mathbb{F}_{p^2})$, Y_1 is superspecial and $(Y_1,\lambda_1) \simeq (E_k,\lambda_E)\times(E_k^2,\mu_1)$, where λ_E is the canonical principal polarisation of E and $\mu_1 \in P_1(E^2)$. Since $p = 2$,

we have $|\operatorname{Aut}(E,\lambda_E)| = |\operatorname{Aut}(E)| = 24$ and $|\operatorname{Aut}(E^2,\mu_1)| = 1920$, cf. [20]. By Corollary 4.9 and Equation (42), we have $|\operatorname{Aut}((E,\lambda_E)\times(E^2,\mu_1)| = |\operatorname{Aut}(E,\lambda_E)| \times |\operatorname{Aut}(E^2,\mu_1)| = 24\cdot 1920$. Notice that $\ker(\rho_1)$ is contained in $\ker(\mu_1)$ since $\ker(\lambda_E)$ is trivial. Therefore, (X,λ) is isomorphic to $(E,\lambda_E)\times(X',\lambda')$, where $X' = E_k^2/\ker(\rho_1)$. The computation of $\operatorname{Aut}(X,\lambda)$ is now reduced to computing $\operatorname{Aut}(X',\lambda')$. By Corollary 3.5, we have

$$|\operatorname{Aut}(X',\lambda')| = \begin{cases} 160, & \text{if } u \in \mathbb{P}^1(\mathbb{F}_{p^4}) - \mathbb{P}^1(\mathbb{F}_{p^2}); \\ 32 & \text{if } u \in \mathbb{P}^1(k) - \mathbb{P}^1(\mathbb{F}_{p^4}). \end{cases}$$

Therefore,

$$|\operatorname{Aut}(X,\lambda)| = \begin{cases} 24\cdot 160 = 2^8\cdot 3\cdot 5 & \text{if } u \in \mathbb{P}^1(\mathbb{F}_{p^4}) - \mathbb{P}^1(\mathbb{F}_{p^2}); \\ 24\cdot 32 = 2^8\cdot 3 & \text{if } u \in \mathbb{P}^1(k) - \mathbb{P}^1(\mathbb{F}_{p^4}). \end{cases}$$

Comparing this result with the values of $\operatorname{Mass}(\Lambda_x)$ in (62), we conclude that $|\Lambda_x| = 1$ in both cases.

(2) If $y \notin \mathscr{D}$, by [23, Corollary 7.5.(1)] we have that $|\Lambda_x| = 4$. Suppose then that $y \in \mathscr{D}$ and $t \notin C(\mathbb{F}_{p^6})$. For every point x' in Λ_x, consider the corresponding polarised abelian variety (X',λ') satisfying $(X',\lambda')[p^\infty] \simeq (X,\lambda)[p^\infty]$. If $y' \in \mathscr{P}'_\mu(k)$ is a point over x', then again $y' \in \mathscr{D}$ and $t' \notin C(\mathbb{F}_{p^6})$. Thus, by [23, Theorem 7.9.(1)], we have that $\operatorname{Aut}(X',\lambda') \simeq C_2^3 \times C_3$. Using the mass formula (cf. Theorem 3.9), noting that $d(t) = 3$ when $p = 2$, we compute that

$$\operatorname{Mass}(\Lambda_x) = \frac{1}{6}.$$

Therefore, $|\Lambda_x| = |C_2^3 \times C_3| \cdot \operatorname{Mass}(\Lambda_x) = 4$.

For the last case, where $y \in \mathscr{D}$ and $t \in C(\mathbb{F}_{p^6})$, the assertion $|\Lambda_x| = 2$ follows directly from Proposition 5.10.

□

5.3. **The case $g = 4$.**

Definition 5.12. (1) An *elementary sequence* is a map $\varphi : \{1,\dots,g\} \to \mathbb{Z}_{\geq 0}$ such that $\varphi(0) = 0$ and $\varphi(i) \leq \varphi(i+1) \leq \varphi(i)+1$ for all $0 \leq i < g$, cf. [37, Definition 5.6]. With each elementary sequence we associate an *Ekedahl-Oort stratum* $\mathscr{S}_\varphi$, which is a locally closed subset of the moduli space $\mathscr{A}_{g,1,n} \otimes \overline{\mathbb{F}}_p$ of principally polarised abelian varieties with level-n structure. Roughly speaking, it consists of those varieties whose p-torsion has a canonical filtration described by φ. On $\mathscr{S}_g$ we consider the stratification induced by $\mathscr{S}_\varphi \cap \mathscr{S}_g$.

(2) The p-divisible group of an abelian variety of dimension g is determined up to isogeny by its Newton polygon, which can be described as a set of slopes $(\lambda_1,\dots,\lambda_{2g})$ with $0 \leq \lambda_i \leq 1$ for all $1 \leq i \leq 2g$ and $\sum_i \lambda_i = g$, cf. [32]. These slopes moreover satisfy that $\lambda_i + \lambda_{2g+1-i} = 1$ for all $1 \leq i \leq 2g$ and that the denominator of each λ_i divides its multiplicity. All abelian varieties with the same Newton polygon form a *Newton stratum* of $\mathscr{A}_g$.

(3) For $1 \leq a \leq g$, we will denote the *a-number locus* of $\mathscr{S}_g$ by $\mathscr{S}_g(a) := \{x \in \mathscr{S}_g(k) : a(x) = a\}$.

Proposition 5.13. (1) *The Ekedahl-Oort strata in dimension $g = 4$ of p-rank zero are precisely the $\mathscr{S}_\varphi$ for those φ appearing in Figure 1.*

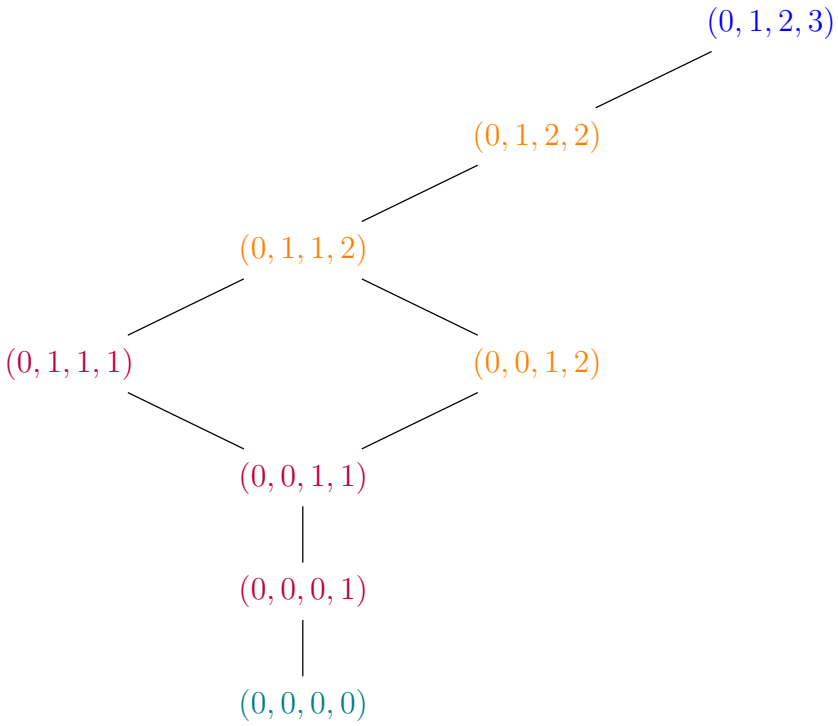


FIGURE 1. Ekedahl-Oort strata of p-rank zero in dimension $g = 4$. The blue stratum has a-number 1, the orange strata have a-number 2, the red strata have a-number 3 and the green stratum has a-number 4. Strata are connected by a line if the lower one is contained in the Zariski closer of the upper one.

(2) *The stratum* $\mathscr{S}_\varphi$ *for* $\varphi = (0,1,2,3)$ *has* a*-number* 1*, those for* $\varphi = (0,1,2,2)$*,* $(0,1,1,2)$*, and* $(0,0,1,2)$ *have* a*-number* 2*, those for* $\varphi = (0,1,1,1)$*,* $(0,0,1,1)$*, and* $(0,0,0,1)$ *have* a*-number* 3 *and that for* $\varphi = (0,0,0,0)$ *has* a*-number* 4*.*

(3) *The strata fully contained in the supersingular locus* $\mathscr{S}_4$ *are precisely the* $\mathscr{S}_\varphi$ *for* $\varphi = (0,0,0,0), (0,0,0,1), (0,0,1,1)$*, and* $(0,0,1,2)$*.*

(4) *The Newton strata of* p*-rank zero are those corresponding to the slope sequences*

$$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right), \left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2},\frac{2}{3},\frac{2}{3},\frac{2}{3}\right), \text{ and } \left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4}\right),$$

which we denote respectively by $\mathscr{N}_{\frac{1}{2}}$*,* $\mathscr{N}_{\frac{1}{3}}$*, and* $\mathscr{N}_{\frac{1}{4}}$*.*

(5) *We have*

$$\begin{aligned}\mathscr{S}_4 = \mathscr{N}_{\frac{1}{2}} = \left(\mathscr{S}_{(0,1,2,3)} \cap \mathscr{S}_4\right) \sqcup \mathscr{S}_{(0,0,0,0)} \sqcup \mathscr{S}_{(0,0,0,1)} \\ \sqcup \mathscr{S}_{(0,0,1,1)} \sqcup \mathscr{S}_{(0,0,1,2)} \sqcup \left(\mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4\right),\end{aligned}$$

and $\mathscr{S}_{(0,1,2,3)} \cap \mathscr{S}_4$ *is dense. In particular, we have*

$$\begin{aligned}\mathscr{S}_4(4) &= \mathscr{S}_{(0,0,0,0)}, \\ \mathscr{S}_4(3) &= \mathscr{S}_{(0,0,0,1)} \sqcup \mathscr{S}_{(0,0,1,1)}, \\ \mathscr{S}_4(2) &= \mathscr{S}_{(0,0,1,2)} \sqcup \left(\mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4\right).\end{aligned}$$

(6) *We have*

$$\mathscr{N}_{\frac{1}{3}} = \left(\mathscr{S}_{(0,1,2,3)} \cap \mathscr{N}_{\frac{1}{3}}\right) \sqcup \mathscr{S}_{(0,1,1,1)} \sqcup \left(\mathscr{S}_{(0,1,1,2)} \cap \mathscr{N}_{\frac{1}{3}}\right),$$

and $\mathscr{S}_{(0,1,2,3)} \cap \mathscr{N}_{\frac{1}{3}}$ *is dense.*

(7) *We have*

$$\mathscr{N}_{\frac{1}{4}} = \left(\mathscr{S}_{(0,1,2,3)} \cap \mathscr{N}_{\frac{1}{4}}\right) \sqcup \mathscr{S}_{(0,1,2,2)},$$

and $\mathscr{S}_{(0,1,2,3)} \cap \mathscr{N}_{\frac{1}{4}}$ *is dense.*

All intersections appearing in (5)–(7) are non-empty.

Proof. The p-rank of an Ekedahl-Oort stratum $\mathscr{S}_\varphi$ is $\max\{i : \varphi(i) = i\}$ and its a-number is $g - \varphi(g)$, proving (1) and (2). By [8, Step 2, p. 1379] we have $\mathscr{S}_\varphi \subseteq \mathscr{S}_4$ if and only if $\varphi(2) = 0$, proving (3). The p-rank of a Newton stratum is the number of non-zero slopes, which implies (4).

We read off from Figure 1 that $\mathscr{S}_{(0,1,2,3)} \cap \mathscr{S}_4$, $\mathscr{S}_{(0,1,2,3)} \cap \mathscr{N}_{\frac{1}{3}}$, and $\mathscr{S}_{(0,1,2,3)} \cap \mathscr{N}_{\frac{1}{3}}$ are the respective a-number 1 loci of $\mathscr{S}_4$, $\mathscr{N}_{\frac{1}{3}}$, and $\mathscr{N}_{\frac{1}{3}}$. Hence, density of these intersections follows from [31, Theorem 4.9(iii)] for $\mathscr{S}_4$, and from combining [36, Remark 5.4] with [8, Theorem 3.1] for $\mathscr{N}_{\frac{1}{3}}$, and $\mathscr{N}_{\frac{1}{3}}$.

By [13, Corollary 4.2 and Lemma 5.12] we see that $\mathscr{S}_{(0,1,2,2)} \subseteq \mathscr{N}_{\frac{1}{4}}$ by minimality of the associated p-divisble group, concluding the proof of (7). Similarly, from [13, Corollary 4.2 and Proposition 7.1], we obtain that $\mathscr{S}_{(0,1,1,1)} \subseteq \mathscr{N}_{\frac{1}{3}}$, again by minimality. Finally, we read off from Figure 1 that

$$\mathscr{S}_{(0,1,1,2)} = \left(\mathscr{S}_{(0,1,1,2)} \cap \mathscr{N}_{\frac{1}{3}}\right) \sqcup \left(\mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4\right).$$

Now [12, Theorem 4.17] implies that $\mathscr{S}_4(2)$ has $H_4(1,p) + H_4(p,1)$ many irreducible components of two types, of which those of the type corresponding to $\mathscr{S}_{(0,0,1,2)}$ yield $H_4(1,p)$ many; see also [31, §9.9]. Hence, the intersection $\mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4$ must yield the other $H_4(p,1)$ components and thus be non-empty. On the other hand, since $\mathscr{S}_{(0,1,1,2)} \not\subseteq \mathscr{S}_4$ by (2), the intersection $\mathscr{S}_{(0,1,1,2)} \cap \mathscr{N}_{\frac{1}{3}}$ is also non-empty. This finishes the proof of (5) and (6) and hence of the proposition. □

By Lemma 5.2, for every point $x \in \mathscr{S}_4(k)$, there exists an integer $0 \leq c \leq 2$ such that there exists a surjective morphism $\pi : \Lambda_x \twoheadrightarrow \Lambda_{g,p^c}$. For Ekedahl-Oort strata with $g = 4$ we have the following result:

Lemma 5.14. *We have* $c = 0$ *for* $x \in \mathscr{S}_{(0,0,0,0)}$*, and* $c = 1$ *for* $x \in \mathscr{S}_{(0,0,0,1)}$*, and* $c = 2$ *for* $x \in \mathscr{S}_{(0,0,1,1)} \cup \mathscr{S}_{(0,0,1,2)}$.

Proof. This follows from [14, Proposition 3.3.2]; the Deligne-Lusztig varieties $X(w')$ in *loc. cit.* are given by $w' = \mathrm{id}$ when $c = 0$, by $w' = (12)$ when $c = 1$ and by $w' = (1342)$ or $(13)(24)$ when $c = 2$. □

Remark 5.15. For any $x \in \mathscr{S}_4(k)$, the surjection $\Lambda_x \twoheadrightarrow \Lambda_{4,p^c}$ is realised through the minimal isogeny $\widetilde{x} \twoheadrightarrow x$ for x, i.e., $\Lambda_{\widetilde{x}} = \Lambda_{4,p^c}$ for the appropriate value of c. This is not necessarily true in $\mathscr{S}_g(k)$ with $g \neq 4$. If x is contained in a supersingular Ekedahl-Oort stratum (i.e., one of the strata in Proposition 5.13.(3)) this follows directly, cf. [14]. Otherwise, we have either $x \in \mathscr{S}_{(0,1,2,3)} \cap \mathscr{S}_4$ or $x \in \mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4$. In the former case, we have $a(x) = 1$, so $\Lambda_{\widetilde{x}} \simeq \Lambda_{4,p^2}$, as will see in the proof of Theorem 5.19. In the latter case, it follows from [12, Proposition 7.1] that $\Lambda_{\widetilde{x}} \simeq \Lambda_{4,1}$.

Lemma 5.16. *Let* $x \in \mathscr{S}_4(k)$*. When* $a(x) = 4$*, we have* $|\mathscr{C}(x)| > 1$.

Proof. By Proposition 5.13.(5), we have $x \in \mathscr{S}_{(0,0,0,0)}$, so by Lemma 5.14, there exists a surjection $\Lambda_x \twoheadrightarrow \Lambda_{4,p^0}$. As observed in Subsection 3.2, it holds that $|\Lambda_{4,p^0}| = H_4(p,1)$, so it follows from Theorem 2.9.(4) that $H_4(p,1) > 1$. This implies the result. □

Lemma 5.17. *Let $x \in \mathscr{S}_4(k)$. When $a(x) = 3$ and $x \in \mathscr{S}_{(0,0,0,1)}$, we have $|\mathscr{C}(x)| > 1$.*

Proof. By Lemma 5.14, there exists a surjection $\Lambda_x \twoheadrightarrow \Lambda_{4,p}$. By Theorem 3.1 we get that

$$\mathrm{Mass}(\Lambda_{4,p}) = \frac{(p-1)(p^2+1)(p^4+1)(p^6-1)^2}{2^{15}\cdot 3^5 \cdot 5^2 \cdot 7}.$$

Since (p^3-1) divides the numerator of $\mathrm{Mass}(\Lambda_{4,p})$, we may argue as in the proof of Theorem 2.9.(3)+(4) to conclude that this numerator is always larger than 1. This implies that $|\Lambda_{4,p}| > 1$, so the result follows. □

Lemma 5.18. *Let $x \in \mathscr{S}_4(k)$. When $a(x) = 2$ and $x \notin \mathscr{S}_{(0,0,1,2)}$, we have $|\mathscr{C}(x)| > 1$.*

Proof. By Proposition 5.13.(5), we know that $x \in \mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4$. By [12, Main results, p. 164] every generic point of $\mathscr{S}_{(0,1,1,2)} \cap \mathscr{S}_4$ has a minimal isogeny from $(E^g, p\mu)$ with a principal polarisation μ. It follows that the minimal isogeny $\widetilde{x} = (\widetilde{X}, \widetilde{\lambda})$ for $x = (X, \lambda)$ is either isomorphic to $(E^4, p\mu)$ or there exists an isogeny $(E^4, p\mu) \to (\widetilde{X}, \widetilde{\lambda})$ for some principal polarisation μ on E^4. Therefore, $|\Lambda_{\widetilde{x}}| = |\Lambda_{4,1}|$ or $|\Lambda_{\widetilde{x}}| = |\Lambda_{4,p}|$. These two numbers are both greater than one as shown in Theorem 2.9.(4) and in Lemma 5.17. Thus, $|\mathscr{C}(x)| \geq |\Lambda_{\widetilde{x}}| > 1$. □

Theorem 5.19. *For every $x \in \mathscr{S}_4(k)$, we have $|\mathscr{C}(x)| > 1$.*

Proof. It follows from Proposition 5.13.(5) and Lemmas 5.16–5.18 that it suffices to consider $x \in \mathscr{S}_4(k)$ such that one of the following holds:

(i) $x \in \mathscr{S}_{(0,0,1,2)} \sqcup \mathscr{S}_{(0,0,1,1)}$, or
(ii) $a(x) = 1$.

In Case (i), by Lemma 5.14, there exists a surjection $\Lambda_x \twoheadrightarrow \Lambda_{4,p^2}$, i.e., $c = 2$. In Case (ii), by [35, Theorem 2.2] (also see [25, Lemma 4.4]), there exists of unique four-dimensional rigid PFTQ

$$(Y_\bullet, \rho_\bullet) : (Y_3, \lambda_3) \to (Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (X_0, \lambda_0) = x$$

extending (X_0, λ_0). The construction in *loc. cit.* also shows that the composition

$$y_3 = (Y_3, \lambda_3) \to (X_0, \lambda_0) = x$$

is the minimal isogeny for x, and hence so is $y_3 = (Y_3, \lambda_3) \to y_2 = (Y_2, \lambda_2)$ for y_2. By Definition 3.6, the polarisation λ_3 is p times a polarisation μ on E^4. Dividing the polarisation by p therefore gives an isomorphism $\Lambda_{y_3} \simeq \Lambda_{4,p^2}$. Thus, the minimal isogeny gives rise to surjective maps $\Lambda_x \twoheadrightarrow \Lambda_{y_2} \twoheadrightarrow \Lambda_{4,p^2}$. Hence, to show that $|\mathscr{C}(x)| > 1$, it suffices to show that $|\Lambda_{y_2}| > 1$. Replacing x with y_2, we now also have a surjection $\Lambda_x \twoheadrightarrow \Lambda_{4,p^2}$ in Case (ii).

Since we have $L_{4,p^c} = L_4(1,p)$ from Equation (24), it follows immediately from Theorem 2.9.(4) that $|\mathscr{C}(x)| > 1$ when $p > 2$. So from now on, we assume that $p = 2$.

We use the same notation as in Subsection 5.1. Since $\Lambda_{4,4} \simeq G^1(\mathbb{Q})\backslash G^1(\mathbb{A}_f)/U_{x_2}$ where the base point $x_2 \in \Lambda_{4,4}$ is taken from the minimal isogeny for x, and $|\Lambda_{4,4}| = 1$, we get that $G^1(\mathbb{A}_f) = G^1(\mathbb{Q})U_{x_2}$. Hence,

$$\Lambda_x \simeq G^1(\mathbb{Q})\backslash G^1(\mathbb{Q})U_{x_2}/U_x \simeq G^1(\mathbb{Z})\backslash G_{x_2}(\mathbb{Z}_p)/G_x(\mathbb{Z}_p),$$

where $G_x(\mathbb{Z}_p)$ is the automorphism group of the polarised Dieudonné module associated to x. Applying the reduction-modulo-Π map m_Π , we obtain $m_\Pi(G_{x_2}(\mathbb{Z}_p)) = \mathrm{Sp}_4(\mathbb{F}_4)$.

Further, let (X_2, λ_2) be the superspecial abelian variety corresponding to the unique element $x_2 \in \Lambda_{4,4}$. Then by Proposition 2.8, and using the same notation, we know that

$G^1(\mathbb{Z}) = \mathrm{Aut}(X_2, \lambda_2) \simeq \mathrm{Aut}((L,h)^{\oplus 2}) \simeq \mathrm{Aut}(L,h)^2 \cdot C_2$ and $\mathrm{Aut}(L,h)$ is the group of cardinality 1920 described in [21, Section 5]. By [21, Section 5, p. 1178] the reduction modulo Π induces a surjective homomorphism $\phi_0 : \mathrm{Aut}(L,h) \twoheadrightarrow \mathrm{SL}_2(\mathbb{F}_4)$ whose kernel $\ker(\phi_0)$ has order 32 (also see *loc. cit.* for the description of $\ker(\phi_0)$). Then it follows that $m_\Pi(G^1(\mathbb{Z})) = m_\Pi(\mathrm{Aut}(X_2, \lambda_2)) \simeq \mathrm{SL}_2(\mathbb{F}_4)^2 \cdot C_2$.

Writing $\overline{G} := m_\Pi(G_x(\mathbb{Z}_p))$, we obtain

$$\Lambda_x \simeq (\mathrm{SL}_2(\mathbb{F}_4)^2 \cdot C_2) \backslash \mathrm{Sp}_4(\mathbb{F}_4) / \overline{G}, \tag{63}$$

since $\ker(m_\Pi) \subseteq G_x(\mathbb{Z}_p)$ (cf. the proof of Proposition 5.10). Thus,

$$\mathrm{Mass}(\Lambda_x) = \mathrm{Mass}(\Lambda_{4,4}) \cdot [\mathrm{Sp}_4(\mathbb{F}_4) : \overline{G}]. \tag{64}$$

We compute that

$$\mathrm{Mass}(\Lambda_{4,4}) = \frac{1}{2^{15} \cdot 3^2 \cdot 5^2} \tag{65}$$

from Theorem 3.1, using Equation (15). Standard computations also show that

$$|\mathrm{Sp}_4(\mathbb{F}_4)| = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17 \tag{66}$$

and that

$$|\mathrm{SL}_2(\mathbb{F}_4)^2 \cdot C_2| = 2^5 \cdot 3^2 \cdot 5^2. \tag{67}$$

By (65) and (66), Equation (64) reduces to

$$\mathrm{Mass}(\Lambda_x) = \frac{17}{2^7 \cdot |\overline{G}|}. \tag{68}$$

We deduce that $|\Lambda_x| > 1$ whenever $17 \nmid |\overline{G}|$. Suppose therefore that $17 \mid |\overline{G}|$, so that $\overline{G}$ contains a cyclic group C_{17} of order 17. We claim that then $\overline{G} = C_{17}$. This finishes the proof, since if $|\Lambda_x| = 1$, Equation (63) would imply that $\mathrm{Sp}_4(\mathbb{F}_4) = (\mathrm{SL}_2(\mathbb{F}_4)^2 \cdot C_2)\, \overline{G} = (\mathrm{SL}_2(\mathbb{F}_4)^2 \cdot C_2)\, C_{17}$. Comparing the cardinalities from (66) and (67) would then yield a contradiction.

Finally, we prove the claim. Let $(M_2, \langle\, ,\, \rangle_2)$ be the polarised Dieudonné module attached to x_2, and fix $V = M_2/\mathsf{V}M_2$ together with a non-degenerate symplectic form ψ induced by $p\langle\, ,\, \rangle_2$. The four-dimensional symplectic space (V, ψ) over k admits an $\mathbb{F}_4$-structure V_0 induced by the skeleton of M_2. Inside V we have an isotropic k-subspace $W = M/\mathsf{V}M_2$, where $M \subseteq M_2$ is the Dieudonné module associated to x and the inclusion is induced from the minimal isogeny. Note that $\dim W = 2$ in Case (i) and $\dim W = 1$ in Case (ii), respectively. According to our definition,

$$\overline{G} := \{A \in \mathrm{Sp}_4(\mathbb{F}_4) : A(W) = W\} = \mathrm{Sp}(V_0, W).$$

Thus, it follows from Proposition 5.8 for $g = 4$ that $\overline{G} = C_{17}$. This completes the proof of the claim and hence of the theorem. □

5.4. **Proof of the main result.**

Theorem 5.20. *Let $x = [X_0, \lambda_0] \in \mathscr{S}_g(k)$ and $\mathscr{C}(x)$ be the central leaf of $\mathscr{A}_g$ passing through the point x. Then $\mathscr{C}(x)$ has one element if and only if one of the following three cases holds:*

(i) $g = 1$ *and* $p \in \{2, 3, 5, 7, 13\}$.
(ii) $g = 2$ *and* $p = 2, 3$.
(iii) $g = 3$, $p = 2$, *and* $a(x) \geq 2$.

Proof. The cases where $g = 1, 2, 4$ or $g \geq 5$ follow from Lemma 5.3, Lemma 5.4, Theorem 5.19 and Lemma 5.5, respectively.

Suppose then that $g = 3$. By Lemma 5.2, either $|\Lambda_x| \geq |\Lambda_{3,1}| = H_3(p, 1)$ or $|\Lambda_x| \geq |\Lambda_{3,p}| = H_3(1, p)$. Thus, by Theorem 2.9, $|\Lambda_x| = 1$ occurs only when $p = 2$. Further assuming $p = 2$, by Proposition 5.11, $\mathscr{C}(x)$ has one element if and only if $a(x) \geq 2$. □

REFERENCES

[1] Zavosh Amir-Khosravi, *Serre's tensor construction and moduli of abelian schemes*, Manuscripta Math. **156** (2018), no. 3-4, pp. 409–456.

[2] S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), pp. 361–386.

[3] Tsuneo Arakawa, Tomoyoshi Ibukiyama, and Masanobu Kaneko, *Bernoulli numbers and zeta functions*, Springer Monographs in Mathematics, Springer, Tokyo, 2014, with an appendix by Don Zagier.

[4] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[5] Juliusz Brzezinski, *Definite quaternion orders of class number one*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, pp. 93–96, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[6] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over* $\mathbb{F}_p$, Algebra Number Theory **9** (2015), no. 1, pp. 225–265.

[7] Ching-Li Chai, *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Invent. Math. **121** (1995), no. 3, pp. 439–479.

[8] Ching-Li Chai and Frans Oort, *Monodromy and irreducibility of leaves*, Ann. of Math. (2) **173** (2011), no. 3, pp. 1359–1396.

[9] Martin Eichler, *Über die Idealklassenzahl total definiter Quaternionenalgebren*, Math. Z. **43** (1938), no. 1, pp. 102–109.

[10] Torsten Ekedahl, *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), no. 2, pp. 151–178.

[11] Harold Exton, *q-hypergeometric functions and applications*, Ellis Horwood Series: Mathematics and its Applications, Ellis Horwood Ltd., Chichester; Halsted Press [John Wiley & Sons, Inc.], New York, 1983, With a foreword by L. J. Slater.

[12] Shushi Harashita, *The a-number stratification on the moduli space of supersingular abelian varieties*, J. Pure Appl. Algebra **193** (2004), no. 1-3, pp. 163–191.

[13] ———, *Ekedahl-Oort strata and the first Newton slope strata*, J. Algebraic Geom. **16** (2007), no. 1, pp. 171–199.

[14] ———, *Ekedahl-Oort strata contained in the supersingular locus and Deligne-Lusztig varieties*, J. Algebraic Geom. **19** (2010), no. 3, pp. 419–438.

[15] Ki-ichiro Hashimoto, *Class numbers of positive definite ternary quaternion Hermitian forms*, Proc. Japan Acad. Ser. A Math. Sci. **59** (1983), no. 10, pp. 490–493.

[16] Ki-ichiro Hashimoto and Tomoyoshi Ibukiyama, *On class numbers of positive definite binary quaternion Hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), no. 3, pp. 549–601.

[17] ———, *On class numbers of positive definite binary quaternion Hermitian forms. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, pp. 695–699.

[18] Tommy Hofmann and Carlo Sircana, *Normal CM-fields with class number one*, arXiv e-prints (2020), arXiv:2011.12089.

[19] WonTae Hwang, Bo-Hae Im, and Hansol Kim, *A classification of the automorphism groups of polarized abelian threefolds over finite fields*, arXiv e-prints (2020), arXiv:2011.11419.

[20] Tomoyoshi Ibukiyama, *On automorphism groups of positive definite binary quaternion Hermitian lattices and new mass formula*, Automorphic forms and geometry of arithmetic varieties, Adv. Stud. Pure Math., vol. 15, Academic Press, Boston, MA, 1989, pp. 301–349.

[21] ———, *Principal polarizations of supersingular abelian surfaces*, J. Math. Soc. Japan **72** (2020), no. 4, pp. 1161–1180.

[22] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, Compos. Math. **154** (2018), no. 5, pp. 934–959.

[23] Valentijn Karemaker, Fuetaro Yobuko, and Chia-Fu Yu, *Mass formula and Oort's conjecture for supersingular abelian threefolds*, Adv. Math. **386** (2021), Paper No. 107812, 52.

[24] Toshiyuki Katsura and Frans Oort, *Families of supersingular abelian surfaces*, Compositio Math. **62** (1987), no. 2, pp. 107–167.
[25] ———, *Supersingular abelian varieties of dimension two or three and class numbers*, Algebraic geometry, Sendai, 1985, Adv. Stud. Pure Math., vol. 10, North-Holland, Amsterdam, 1987, pp. 253–281.
[26] Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, and Damien Robert, *Spanning the isogeny class of a power of an elliptic curve*, Math. Comp. **91** (2021), no. 333, pp. 401–449.
[27] Yoshiyuki Kitaoka, *Arithmetic of quadratic forms*, Cambridge tracts in Mathematics 106, Cambridge University Press, 1993.
[28] Martin Kneser, *Quadratische formen*, Springer, Berlin Heidelberg, 2002.
[29] Kristin Lauter, *The maximum or minimum number of rational points on genus three curves over finite fields*, Compositio Math. **134** (2002), no. 1, pp. 87–111, With an appendix by Jean-Pierre Serre.
[30] Geon-No Lee and Soun-Hi Kwon, *CM-fields with relative class number one*, Math. Comp. **75** (2006), no. 254, pp. 997–1013.
[31] Ke-Zheng Li and Frans Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998.
[32] Ju. I. Manin, *Theory of commutative formal groups over fields of finite characteristic*, Uspehi Mat. Nauk **18** (1963), no. 6 (114), pp. 3–90.
[33] J. Myron Masley and Hugh L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286(287)** (1976), pp. 248–256.
[34] Gabriele Nebe, *Finite quaternionic matrix groups*, Represent. Theory **2** (1998), pp. 106–223.
[35] Tadao Oda and Frans Oort, *Supersingular abelian varieties*, Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), Kinokuniya Book Store, Tokyo, 1978, pp. pp. 595–621.
[36] Frans Oort, *Newton polygons and formal groups: conjectures by Manin and Grothendieck*, Ann. of Math. (2) **152** (2000), no. 1, pp. 183–206.
[37] ———, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 345–416.
[38] Sun-Mi Park and Soun-Hi Kwon, *Class number one problem for normal CM-fields*, J. Number Theory **125** (2007), no. 1, pp. 59–84.
[39] Sun-Mi Park, Hee-Sun Yang, and Soun-Hi Kwon, *The class number one problem for the normal CM-fields of degree 32*, Trans. Amer. Math. Soc. **359** (2007), no. 10, pp. 5057–5089.
[40] Arnold Pizer, *On the arithmetic of quaternion algebras*, Acta Arith. **31** (1976), no. 1, pp. 61–89.
[41] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.
[42] Irving Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press Oxford University Press, Oxford, 2003, Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.
[43] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.
[44] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.
[45] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.
[46] Ken Yamamura, *The determination of the imaginary abelian number fields with class number one*, Math. Comp. **62** (1994), no. 206, pp. 899–921.
[47] Chia-Fu Yu, *On the mass formula of supersingular abelian varieties with real multiplications*, J. Aust. Math. Soc. **78** (2005), no. 3, pp. 373–392.
[48] ———, *The supersingular loci and mass formulas on Siegel modular varieties*, Doc. Math. **11** (2006), pp. 449–468.
[49] ———, *Superspecial abelian varieties over finite prime fields*, J. Pure Appl. Algebra **216** (2012), no. 6, pp. 1418–1427.
[50] ———, *On arithmetic of the superspecial locus*, Indiana Univ. Math. J. **67** (2018), no. 4, pp. 1341–1382.
[51] Chia-Fu Yu and Jeng-Daw Yu, *Mass formula for supersingular abelian surfaces*, J. Algebra **322** (2009), no. 10, pp. 3733–3743.

DEPARTMENT OF MATHEMATICS, GRADUATE SCHOOL OF SCIENCE, OSAKA UNIVERSITY, TOYONAKA, JAPAN
Email address: ibukiyam@math.sci.osaka-u.ac.jp

MATHEMATICAL INSTITUTE, UTRECHT UNIVERSITY, UTRECHT, THE NETHERLANDS
Email address: V.Z.Karemaker@uu.nl

INSTITUTE OF MATHEMATICS, ACADEMIA SINICA AND NATIONAL CENTER FOR THEORETIC SCIENCES, TAIPEI, TAIWAN
Email address: chiafu@math.sinica.edu.tw