Journal of Pure and Applied Algebra 216 (2012) 1418–1427

Contents lists available at SciVerse ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

# Superspecial abelian varieties over finite prime fields

Chia-Fu Yu *

*Institute of Mathematics, Academia Sinica and NCTS (Taipei Office), 6th Floor, Astronomy Mathematics Building, No. 1, Roosevelt Rd. Sec. 4, Taipei, 10617, Taiwan*

ARTICLE INFO

*Article history:*
Received 13 June 2011
Received in revised form 13 November 2011
Available online 22 December 2011
Communicated by E.M. Friedlander

*MSC:* 14K10; 11G10; 14G15; 11E41

ABSTRACT

In this paper, we determine the number of isomorphism classes of superspecial abelian varieties $A$ over the prime field $\mathbb{F}_p$ within a rational isogeny class. This generalizes a result of Deuring on the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ that have a model defined over $\mathbb{F}_p$.



## 1. Introduction

In this paper, we study the counting problem of a class of certain abelian varieties over finite fields. More precisely, we consider superspecial abelian varieties over a finite prime field inside an isogeny class, and compute explicitly the number of them up to isomorphism.

Let $p$ be a rational prime number and $g \geq 1$ be a positive integer. An abelian variety over a field $k$ of characteristic $p$ is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over an algebraic closure $\bar{k}$ of $k$; it is called *superspecial* if it is isomorphic to a product of supersingular elliptic curves over $\bar{k}$. Fix a supersingular elliptic curve $E_0$ over $\mathbb{F}_p$ such that $\pi_{E_0}^2 = -p$, where $\pi_{E_0}$ is the relative Frobenius endomorphism of $E_0$. Such an elliptic curve exists (see Deuring [3] or use the Honda–Tate theory [20, Theorem 1, p. 96]). When $p > 3$ the condition $\pi_{E_0}^2 = -p$ for $E_0$ is superfluous; this follows from the Hasse–Weil bound for eigenvalues of the Frobenius morphism $\pi_{E_0}$. We consider the set $\mathbb{S}$ of isomorphism classes of $g$-dimensional superspecial abelian varieties $A$ over $\mathbb{F}_p$ such that there is an isogeny from $E_0^g$ to $A$ over $\mathbb{F}_p$. Using a theorem of Tate [21, Theorem 1 (c), p. 139], the condition for $A$ isogenous to $E_0^g$ over $\mathbb{F}_p$ is equivalent to that the relative Frobenius morphism $\pi_A$ of $A$ over $\mathbb{F}_p$ satisfies $\pi_A^2 = -p$ (also see Lemma 2.2). In this paper, we calculate the number of these superspecial abelian varieties.

**Theorem 1.1.** *Notation as above, we have*

$$|\mathbb{S}| = \begin{cases} h(\sqrt{-p}), & \text{if } p = 2 \text{ or } p \equiv 1 \pmod 4, \\ (g+1)h(\sqrt{-p}), & \text{if } p \equiv 7 \pmod 8 \text{ or } p = 3, \\ (g+3)h(\sqrt{-p}), & \text{if } p \equiv 3 \pmod 8 \text{ and } p \neq 3, \end{cases} \tag{1.1}$$

*where $h(\sqrt{-p})$ denotes the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.*

Theorem 1.1 generalizes a result of Deuring on the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ that have a model defined over $\mathbb{F}_p$; see (1.5).

* Tel.: +886 2 2368 5999x628; fax: +886 2 2368 9771.
*E-mail address:* chiafu@math.sinica.edu.tw.

0022-4049/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2011.12.007

We discuss some background on the topic. First of all, it is well-known (due to Deuring [3]) that every supersingular elliptic curve over an algebraically closed field of characteristic $p$ has a model defined over $\mathbb{F}_{p^2}$. Also, if we let $B_{p,\infty}$ denote the quaternion algebra over $\mathbb{Q}$ ramified exactly at $p$ and $\infty$, then the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is in one-to-one correspondence with the set of ideal classes of a maximal order of the quaternion algebra $B_{p,\infty}$. The same picture can be generalized to higher dimensions:

(a) There is only one isomorphism class of superspecial abelian varieties of dimension $>1$ over $\overline{\mathbb{F}}_p$ (this is due to Deligne, Ogus and Shioda).
(b) The set $\Lambda_g$ of isomorphism classes of superspecial *principally polarized* abelian varieties over $\overline{\mathbb{F}}_p$ has the similar description as a double coset space for an algebraic group $G$ associated to certain quaternion Hermitian form (see Ibukiyama–Katsura–Oort [11, Theorem 2.10]).

The class number $|\Lambda_g|$ is calculated by Deuring [3,4], Eichler [5] and Igusa [12] for $g = 1$ and by Hashimoto and Ibukiyama [9] for $g = 2$. The class number formula obtained in [9] is very complicated. It is believed after the work [9] that calculating the class number $|\Lambda_g|$ explicitly for higher genus $g$ is an extremely difficult task. However, exploring some structures and relationships among them arising from $\Lambda_g$ is still interesting.

The well-known Deuring–Eichler mass formula suggests that instead of calculating the class number $|\Lambda_g|$ itself, the weighted version

$$\mathrm{Mass}(\Lambda_g) := \sum_{(A,\lambda)\in\Lambda_g} \#\,\mathrm{Aut}(A,\lambda)^{-1}$$

should be more accessible (also see [28, Introduction] for a discussion). This has been calculated, namely the case of Siegel modular varieties, by Ekedahl [6, p. 159] and some others (see Hashimoto–Ibukiyama [9, Proposition 9, p. 568], and Katsura–Oort [13, Section 2, Theorems 5.1 and 5.3]). The mass formula for $\Lambda_g$ is stated as follows:

$$\mathrm{Mass}(\Lambda_g) = \frac{(-1)^{g(g+1)/2}}{2^g}\left\{\prod_{k=1}^{g}\zeta(1-2k)\right\}\cdot\prod_{k=1}^{g}\left\{(p^k+(-1)^k\right\}, \tag{1.2}$$

where $\zeta(s)$ is the zeta function.

The analogous formula for the mass associated to the set of superspecial polarized abelian varieties with real multiplication is established in [24, Theorem 3.7 and Subsection 4.6]; namely one considers the Hilbert modular varieties instead of the Siegel modular varieties. This result is applied for determining the number of supersingular components (those are entirely contained in the supersingular locus) of the reduction mod $p$ of Hilbert modular varieties with Iwahori level structure at a prime $p$; see [26, Section 4] for more details. The geometric mass formula (1.2) is generalized to good reduction of quaternion Shimura varieties; see [25, Theorem 1.2] for the precise formula. The proof of this generalized mass formula is built on a very general result which reduces the computation of geometric masses to that of arithmetic masses (see [28, Theorem 2.2] for the precise statement). Then one applies the results of Prasad [18], Shimura [19] and others on exact arithmetic mass formulas to conclude the desired exact geometric mass formulas; see [28,25].

In the function field analogue where superspecial abelian varieties are replaced by supersingular Drinfeld modules, the mass formula is obtained by J. Yu and the author (see [23, Theorem 2.1, p. 906]) for any rank and any global function fields, based on some earlier works of Gekeler [7,8].

Another viewpoint to depart concerning counting superspecial points (still over $\overline{\mathbb{F}}_p$ and with a principal polarization) is that the superspecial locus itself is an $\ell$-adic Hecke orbit, where $\ell$ is a prime $\neq p$, in the fine moduli space We refer the reader to Chai [1] for the definition and results about $\ell$-adic Hecke orbits. It turns out that the similar formalism allows one to calculate the cardinality of each *supersingular* Hecke orbit (in a fine moduli space), rather the superspecial locus considered previously, provided one knows the underlying $p$-divisible group structure. The structure for the case of genus $g = 2$ is analyzed in J.-D. Yu and the author [27, Theorem 1.1] using the Moret-Bailly family [15].

Theorem 1.1 is not a weighted version, rather it is a class number problem. It sits between the trivial case (a) and the extremely difficult case (b) above. As will be seen later, the cardinality of $\mathbb{S}$ may not be *one* class number but a sum of several class numbers. Also, the set $\mathbb{S}$ may not consist of one $\ell$-adic Hecke orbit over $\mathbb{F}_p$ (here two abelian varieties over $\mathbb{F}_p$ lie in the same $\ell$-adic Hecke orbit over $\mathbb{F}_p$ if there is an $\ell$-quasi-isogeny from one to another over $\mathbb{F}_p$), rather it consists of $g+1$ Hecke orbits in some cases (see Proposition 4.5). However, the computation of each class number is not difficult in our case, as the strong approximation holds for the algebraic group concerned; see Lemma 4.1.

The proof of Theorem 1.1 uses the classification of modules over certain non-maximal order $R$ of a number field $E$. The classification is of interest on its own right; on the other hand, it is also useful to determine isomorphism classes in other isogeny classes over $\mathbb{F}_p$ (see Theorem 3.1).

Note that we impose a condition (by requiring objects $A$ isogenous to $E_0^g$ over $\mathbb{F}_p$) on $\mathbb{S}$ which makes the computation more accessible. As any superspecial abelian variety $A$ is isogenous (even isomorphic) to $E_0^g$ over $\overline{\mathbb{F}}_p$, this condition is unseen in the geometric setting, or can be thought of as an arithmetic constraint. Suppose that one does not impose this isogeny condition, and let $\mathbb{S}'$ be the set of isomorphism classes of $g$-dimensional superspecial abelian varieties over $\mathbb{F}_p$; one has $\mathbb{S}\subset\mathbb{S}'$. In the