Isogeny classes and endomorphism algebras of abelian varieties over finite fields

by

Yuri G. Zarhin
Isogeny classes and endomorphism algebras of abelian varieties over finite fields

by

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
Pennsylvania State University
University Park, PA 16802
USA

MPIM 22-35
ISOGENY CLASSES AND ENDMORPHISMS
ALGEBRAS OF ABELIAN VARIETIES OVER FINITE
FIELDS

YURI G. ZARHIN

Abstract. We construct non-isogenous simple ordinary abelian
varieties over an algebraic closure of a finite field with isomorphic
endomorphism algebras.

1. Introduction

1.1. If $K$ is a number field then we write $\text{Cl}(K)$ for the (finite commu-
tative) ideal class group of $K$, $\text{cl}(K)$ for the class number of $K$ (i.e., the
cardinality of $\text{Cl}(K)$) and $\text{exp}(K)$ for the exponent of $\text{Cl}(K)$. Clearly,
$\text{exp}(K)$ divides $\text{cl}(K)$. (The equality holds if and only if $\text{Cl}(K)$ is cyclic,
which is not always the case, see [1, Tables].) In addition, $\text{exp}(K)$ is
odd if and only if $\text{cl}(K)$ is odd. We write $\mathcal{O}_K$ for the ring of integers
in $K$ and $U_K$ for the group of units, i.e., the multiplicative group of
invertible elements in $\mathcal{O}_K$. As usual, an element of $U_K$ is called a unit
in $K$ or a $K$-unit. It is well known (and can be easily checked) that if
a unit $u$ in $K$ is a square in $K$ then it is also a square in $U_K$.

Let $p$ be a prime and $q$ a positive integer that is a power of $p$. We
write $\mathbb{F}_p$ for the $p$-element finite field and $\mathbb{F}_q$ for its $q$-element overfield.
As usual, $\overline{\mathbb{F}}_p$ stands for an algebraic closure of $\mathbb{F}_p$, which is also an
algebraic closure of $\mathbb{F}_q$. We have

$$\mathbb{F}_p \subset \mathbb{F}_q \subset \overline{\mathbb{F}}_p.$$  

If $X$ is an abelian variety over $\overline{\mathbb{F}}_p$ then we write $\text{End}^0(X)$ for its endo-
morphism algebra $\text{End}(X) \otimes \mathbb{Q}$, which is a finite-dimensional semisimple
algebra over the field $\mathbb{Q}$ of rational numbers. If $X$ is defined over $k = \mathbb{F}_q$ then we write $\text{End}_k(X)$ for its ring of $k$-endomorphisms and
$\text{End}_k^0(X)$ for the $\mathbb{Q}$-algebra $\text{End}_k(X) \otimes \mathbb{Q}$; one may view $\text{End}_k^0(X)$ as
the $\mathbb{Q}$-subalgebra of $\text{End}^0(X)$ with the same 1.

2010 Mathematics Subject Classification. 11G10, 11G25, 14G15.

The author was partially supported by Simons Foundation Collaboration grant
# 585711. Part of this work was done during his stay in January - May 2022 at
the Max-Planck Institut für Mathematik (Bonn, Germany), whose hospitality and
support are gratefully acknowledged.
It is well known that isogenous abelian varieties have isomorphic endomorphism algebras and the same dimension (and $p$-adic Newton polygon). In addition, an abelian variety is simple if and only if its endomorphism algebra is a division algebra over $\mathbb{Q}$. It is also known (Grothendieck-Tate) that $\text{End}^0(X)$ uniquely determines the dimension of $X$ [8]. Namely, $2\dim(X)$ is the maximal $\mathbb{Q}$-dimension of a semisimple commutative $\mathbb{Q}$-subalgebra of $\text{End}^0(X)$. However, it turns out that there are non-isogenous abelian varieties over $\overline{\mathbb{F}}_p$ with isomorphic endomorphism algebras.

The aim of this note is to provide explicit examples of such varieties. Let me start with a classical result of M. Deuring about elliptic curves [3], [14, Ch. 4].

**Proposition 1.2.** Let $K$ be an imaginary quadratic field.

(i) Let $p$ be a prime and $E$ an elliptic curve over $\overline{\mathbb{F}}_p$ such that $\text{End}^0(E)$ is isomorphic to $K$.

Then $p$ splits in $K$ and $E$ is ordinary.

(ii) Let $p$ be a prime that splits in $K$.

Then all the elliptic curves $E$ over $\overline{\mathbb{F}}_p$ with $\text{End}^0(E) \cong K$ are mutually isogenous.

I did not find in the literature the following assertion that complements Proposition 1.2.

**Proposition 1.3.** Let $K$ be an imaginary quadratic field and $p$ a prime that splits in $K$. Let us put $q = p^{\exp(K)}$.

Then there exists an elliptic curve $E$ that is defined with all its endomorphisms over $\mathbb{F}_q$ and such that $\text{End}^0(E) \cong K$.

**Remark 1.4.** One may deduce from ([4, Satz 3], [9, Sect. 6, Cor. 1 on p. 507]) that if we put $q_1 = p^{\ell(K)}$ then there exists an elliptic curve $E$ that is defined with all its endomorphisms over $\mathbb{F}_{q_1}$ and such that $\text{End}(E) \cong \mathcal{O}_K$ (and therefore $\text{End}^0(E) \cong K$).

The next result is an analogue of Proposition 1.2 for abelian surfaces and quartic fields.

**Proposition 1.5.** Let $K$ be a CM quartic field that is a cyclic extension of $\mathbb{Q}$.

(i) Let $p$ be a prime and $Y$ an abelian surface over $\overline{\mathbb{F}}_p$ such that $\text{End}^0(Y)$ is isomorphic to $K$.

Then $p$ splits completely in $K$ and $Y$ is simple ordinary.

(ii) Let $p$ be a prime that splits in $K$. 


Then all the abelian surfaces $Y$ over $\overline{\mathbb{F}}_p$ with $\text{End}^0(Y) \cong K$ are mutually isogenous. In addition, there exists such an $Y$ that is defined with all its endomorphisms over $\mathbb{F}_{p^c}$ where $c = \exp(K)$.

Our main result is the following assertion.

**Theorem 1.6.** Let $n$ be a positive integer and $K$ is a CM field that is a cyclic degree $2^n$ extension of $\mathbb{Q}$. Let $K_0$ be the only degree $2^{n-1}$ subfield of $K$, which is the maximal totally real subfield of $K$. Let us put $c = \exp(K)$.

(i) Let $p$ be a prime and $A$ an abelian variety over $\overline{\mathbb{F}}_p$ such that $\text{End}^0(A)$ is isomorphic to $K$. Then $p$ splits completely in $K$ and $A$ is an ordinary simple abelian variety of dimension $2^{n-1}$.

(ii) Let $p$ be a prime that splits completely in $K$. Let us put $q = p^c$.

1. There are precisely $2^{2^{n-1} - n}$ isogeny classes of abelian varieties $A$ over $\overline{\mathbb{F}}_p$, whose endomorphism algebra $\text{End}^0(A)$ is isomorphic to $K$.

2. Each of these isogeny classes contains an abelian variety that is defined with all its endomorphisms over $\mathbb{F}_q$.

3. Assume additionally that every totally positive unit in $K_0$ is a square in $K_0$.

Then each of these isogeny classes contains an abelian variety that is defined with all its endomorphisms over $\mathbb{F}_q$.

**Remark 1.7.** (a) If $n = 1$ then $K$ is an imaginary quadratic field and therefore $K_0 = \mathbb{Q}$ and $U_\mathbb{Q} = \{\pm 1\}$. The only (totally) positive unit in $\mathbb{Q}$ is 1, which is obviously a square in $\mathbb{Q}$. Hence, Propositions 1.2 and 1.3 are the special case of Theorem 1.6 with $n = 1$. On the other hand, Proposition 1.5 follows readily from the special case of Theorem 1.6 with $n = 2$.

(b) If $n \geq 3$ then the number $2^{2^{n-1} - n}$ of the corresponding isogeny classes is strictly greater than 1. This gives us examples of non-isogenous abelian varieties over $\overline{\mathbb{F}}_p$, whose endomorphism algebras are isomorphic to $K$ and therefore are mutually isomorphic.

(c) Now let $n$ be an arbitrary positive integer. By Chebotarev’s density theorem, the set of primes that split completely in $K$ is infinite (and even has a positive density $1/2^n$).
**Corollary 1.8.** Let \( r \) be a Fermat prime (e.g., \( r = 3, 5, 17, 257, 65537 \)). Let \( p \) be a prime that is congruent to 1 modulo \( r \). Let us put
\[
isg(r) = \frac{\varphi(r-1)}{2(r-1)}.
\]
Then there are precisely \( isg(r) \) isogeny classes of simple \((r-1)/2\)-dimensional ordinary abelian varieties \( A \) over \( \bar{\mathbb{F}}_p \), whose endomorphism algebra
\[
\text{End}^0(A) = \text{End}(A) \otimes \mathbb{Q}
\]
is isomorphic to the \( r \)th cyclotomic field \( \mathbb{Q}(\zeta_r) \). In addition, if \( c = \exp(\mathbb{Q}(\zeta_r)) \) and \( q = p^c \) then each of these isogeny classes contains an abelian variety that is defined with all its endomorphisms over \( \mathbb{F}_q \).

**Remark 1.9.** The congruence condition on \( p \) means that \( p \) splits completely in \( \mathbb{Q}(\zeta_r) \). There are infinitely many such \( p \), thanks to Dirichlet’s theorem about primes in an arithmetic progression. More precisely, the set of such primes has density \( 1/(r-1) \).

**Remark 1.10.** It is well known that the property of being simple (resp. ordinary) is invariant under isogenies.

**Remark 1.11.** Let \( r \) be a Fermat prime. Clearly, \( isg(r) = 1 \) if and only if \( r \leq 5 \).

Let \( p \) be a prime \( p \) that is congruent to 1 mod \( r \). It follows from Theorem 1.6 that \( r \leq 5 \) if and only if there is a precisely one isogeny class of simple ordinary \((r-1)/2\)-dimensional abelian varieties over \( \bar{\mathbb{F}}_p \), whose endomorphism algebra is isomorphic to \( \mathbb{Q}(\zeta_r) \). In other words, all such abelian varieties are mutually isogenous over \( \bar{\mathbb{F}}_p \), if and only if \( r \in \{3, 5\} \).

**Example 1.12.** (i) Take \( r = 3 \). We have \( isg(3) = 1 \). It follows from Remark 1.11 that if \( p \equiv 1 \mod 3 \) then all ordinary elliptic curves over \( \bar{\mathbb{F}}_p \) with endomorphism algebra \( \mathbb{Q}(\zeta_3) \) are isogenous. (This assertion seems to be well known.) This implies that each such elliptic curve is isogenous over \( \bar{\mathbb{F}}_p \) to \( y^2 = x^3 - 1 \).

(ii) Take \( r = 5 \). We have \( isg(5) = 1 \). It follows from Remark 1.11 that if \( p \equiv 1 \mod 5 \) then all abelian varieties over \( \bar{\mathbb{F}}_p \) with endomorphism algebra \( \mathbb{Q}(\zeta_5) \) are two-dimensional simple ordinary and mutually isogenous. This implies that each such abelian variety is isogenous to the jacobian of the genus 2 curve \( y^2 = x^5 - 1 \).

**Example 1.13.** Let us take \( r = 17 \). Then \( cl(\mathbb{Q}(\zeta_{17})) = 1 \) [13]. Let us choose a prime \( p \) that is congruent to 1 modulo 17 (e.g., \( p = 103 \)). We
have
\[ \text{isg}(17) = \frac{2^8}{16} = 16. \]

By Theorem 1.6, there are precisely 16 isogeny classes of simple ordinary 8-dimensional abelian varieties over \( \overline{\mathbb{F}}_p \) with endomorphism algebras \( \mathbb{Q}(\zeta_{17}) \). In addition, each of these isogeny classes contains an abelian eightfold that is defined with all its endomorphisms over \( \mathbb{F}_p \).

This implies that there exist sixteen 8-dimensional ordinary simple abelian varieties \( A_1, \ldots, A_{16} \) over \( \overline{\mathbb{F}}_p \) that are mutually non-isogenous but each endomorphism algebra \( \text{End}^0(A_i) \) is isomorphic to \( \mathbb{Q}(\zeta_{17}) \) (for all \( i \) with \( 1 \leq i \leq 16 \)). In particular,
\[ \text{End}^0(A_i) \cong \text{End}^0(A_j) \quad \forall \, i, j \quad (1 \leq i < j \leq 16). \]

In addition, each \( A_i \) and all its endomorphisms are defined over \( \mathbb{F}_p \).

This gives an answer to a question of L. Watson [15].

The following assertion is a natural generalization of Corollary 1.8.

**Corollary 1.14.** Let \( r \) be an odd prime and \( (r - 1) = 2^n \cdot m \) where \( n \) is a positive integer and \( m \) is a positive odd integer. Let \( H \) be the only order \( m \) subgroup of the cyclic Galois group \( \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}) = (\mathbb{Z}/r\mathbb{Z})^* \) of order \( (r - 1) \). Let
\[ K = K^{(r)} := \mathbb{Q}(\zeta_r)^H \]
be the subfield of \( H \)-invariants in \( \mathbb{Q}(\zeta_r) \). Then:

(i) Let \( p \) be a prime and \( A \) an abelian variety over \( \overline{\mathbb{F}}_p \) such that \( \text{End}^0(A) \) is isomorphic to \( K^{(r)} \).

Then \( p \) splits completely in \( K^{(r)} \) and \( A \) is an ordinary simple abelian variety of dimension \( 2^{n-1} \).

(ii) Let \( p \) be a prime that splits completely in \( K^{(r)} \) and let \( q = p^c \) where \( c = \exp(K^{(r)}) \).

Then there are precisely \( 2^{2n-1-n} \) isogeny classes of abelian varieties \( A \) over \( \overline{\mathbb{F}}_p \), whose endomorphism algebra \( \text{End}^0(A) \) is isomorphic to \( K^{(r)} \). In addition, each of these isogeny classes contains an abelian variety that is defined with all its endomorphisms over \( \mathbb{F}_q \).
Remark 1.15. Let $K = K^{(r)}$. It is well known that $r$ is totally ramified in $\mathbb{Q}(\zeta_r)$ and therefore in its subfield $K$ as well. This implies that if $K_0$ is the only degree $2^{n-1}$ subfield of $K$, which is the maximal totally real subfield of $K$, then the quadratic extension $K/K_0$ is ramified. On the other hand, it is known that ([5, Sect. 38], [2, p. 77-78]) that $c(K^{(r)})$ is odd (and therefore $c = \exp(K^{(r)})$ is also odd). It follows from [5, Sect. 37, Satz 42] (see also [2, Cor. 13.10 on p. 76]) that $K_0$ has units with independent signs (there are units of $K_0$ of every possible signature), which implies (thanks to [2, Lemma 12.2 on p. 55]) that every totally positive unit in $K_0$ is a square in $K_0$ and therefore is a square in $U_{K_0}$.

Example 1.16. Let us fix an integer $n \geq 2$. Here is a construction of infinitely many mutually non-isomorphic CM fields that are cyclic degree $2^n$ extensions of $\mathbb{Q}$. Let us consider the infinite (thanks to Dirichlet’s theorem) set of primes $r$ that are congruent to $1+2^n$ modulo $2^n+1$. Then $r - 1 = 2^n \cdot m$ where $m$ is an odd positive integer. In light of Corollary 1.14, the corresponding subfield $K^{(r)}$ of $\mathbb{Q}(\zeta_r)$ defined by (2) enjoys the desired properties. Since $K^{(r)}$ is a subfield of $\mathbb{Q}(\zeta_r)$, the field extension $K^{(r)}/\mathbb{Q}$ is ramified precisely at $r$. This implies that the fields $K^{(r)}$ are mutually non-isomorphic (and even linearly disjoint) for distinct $r$.

The paper is organized as follows. In Section 2 we review basic results about maximal ideals of $\mathcal{O}_K$. In Section 3 we concentrate on so called ordinary Weil’s $q$-numbers in $K$. In Section 4 we discuss simple abelian varieties over $\mathbb{F}_q$, whose Weil’s numbers lie in $K$. In Section 5 we discussed some basic facts of Honda-Tate theory [11, 6, 12]. Section 6 contains proofs of main results.

In what follows we will freely use the following elementary well known observation. Any $\mathbb{Q}$-subalgebra with 1 of a number field $K$ is actually a subfield of $K$; in particular, it is also a number field. E.g., if $u$ is an element of $L$ then the subfield $\mathbb{Q}(u)$ generated by $u$ coincides with the $\mathbb{Q}$-subalgebra $\mathbb{Q}[u]$ generated by $u$.

Acknowledgements. I am grateful to Ley Watson for an interesting stimulating question [15].

2. Preliminaries

2.1. We keep the notation and assumptions of Subsection 1.1 and Theorem 1.6. As usual, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ stand for the fields of rational, real and complex numbers and $\overline{\mathbb{Q}}$ for the (algebraically closed) subfield of all algebraic numbers in $\mathbb{C}$. We write $\mathbb{Z}$ (resp. $\mathbb{Z}_+$) for the ring of integers (resp. for the additive semigroup of nonnegative integers). If $T$ is a finite set then we write $\#(T)$ for the number of its elements.
Recall [6, 12] that an algebraic integer \( \pi \in \overline{\mathbb{Q}} \) is called a Weil’s \( q \)-number if all its Galois-conjugates have the archimedean absolute value \( \sqrt{q} \).

Throughout this paper, \( n \) is a positive integer and \( K \) is a CM field that is a degree \( 2^n \) cyclic extension of \( \mathbb{Q} \). We view \( K \) as a subfield of \( \mathbb{C} \); in particular, \( K \) is a subfield of \( \overline{\mathbb{Q}} \) that is stable under the complex conjugation. We denote by

\[ \rho : K \to K \]

the restriction of the complex conjugation to \( K \); one may view \( \rho \) as an element of order 2 in the Galois group

\[ G := \text{Gal}(K/\mathbb{Q}) \]

where \( G \) is a cyclic group of order \( 2^n \).

**Remark 2.2.** Let \( \pi \in K \subseteq \mathbb{C} \).

- Suppose that \( \pi \) is a Weil’s \( q \)-number. Then \( \pi \) is a algebraic integer, i.e., \( \pi \in \mathcal{O}_K \). Since the absolute value of \( \pi \) is the square root of \( q \), we have \( \pi \cdot \rho(\pi) = q \).
- Conversely, suppose that \( \pi \in \mathcal{O}_K \) (i.e., \( \pi \) is an algebraic integer) and

\[ \pi \cdot \rho(\pi) = q \quad \text{(3)} \]

Since \( K/\mathbb{Q} \) is Galois, all the Galois-conjugates of \( \pi \) also lie in \( \mathcal{O}_K \) and constitute the orbit

\[ G\pi = \{ \sigma(\pi) \mid \sigma \in G \} \]

of \( G \). Since \( G \) is commutative and contains \( \rho \), it follows from (3) that for all \( \sigma \in G \)

\[ \sigma(\pi) \cdot \rho(\sigma(\pi)) = \sigma(\pi) \cdot \sigma(\rho(\pi)) = \sigma(\pi \cdot \rho(\pi)) = \sigma(q) = q. \]

It follows readily that \( \pi \in K \) is a Weil’s \( q \)-number if and only if \( \pi \in \mathcal{O}_K \) and (3) holds.

We write \( W(q, K) \) for the set of Weil’s \( q \)-numbers in \( K \) and \( \mu_K \) for the (finite cyclic) multiplicative group of roots of unity in \( K \). Clearly, \( W(q, K) \) is a finite \( G \)-stable subset of \( \mathcal{O}_K \), which is also stable under multiplication by elements of \( \mu_K \). The latter gives rise to the free action of \( \mu_K \) on \( W(q, K) \) defined by

\[ \mu_K \times W(q, K) \to W(q, K), \quad \zeta, \pi \mapsto \zeta \pi, \quad \forall \zeta \in \mu_K, \pi \in W(q, K). \]

**Remark 2.3.** It is well known (and follows easily from a theorem of Kronecker [16, Ch. IV, Sect. 4, Th.8]) that \( \pi_1, \pi_2 \in W(q, K) \) lie in the same \( \mu_K \)-orbit (i.e., \( \pi_2/\pi_1 \) is a root of unity) if and only if the ideals \( \pi_1 \mathcal{O}_K \) and \( \pi_2 \mathcal{O}_K \) of \( \mathcal{O}_K \) do coincide.
Recall (Subsection 2.1) that $K$ is a subfield of the field $\mathbb{C}$ of complex numbers that is stable under the complex conjugation. Then

$$K_0 := K \cap \mathbb{R}$$

is a (maximal) totally real number (sub)field, whose degree $[K_0 : \mathbb{Q}]$ is

$$\frac{[K : \mathbb{Q}]}{2} = \frac{2^n}{2} = 2^{n-1}.$$

2.4. Recall that the Galois group $G = \text{Gal}(K/\mathbb{Q})$ is a cyclic group of order $2^n$. Hence, it has precisely one element of order 2 and therefore this element must coincide with the complex conjugation

$$\rho : K \to K.$$

The properties of $G$ imply that every nontrivial subgroup $H$ of $G$ contains $\rho$. It follows that every proper subfield of $K$ is totally real. Indeed, each such subfield is the subfield $K^H$ of $H$-invariants for a certain nontrivial subgroup $H$ of $G$. Since $H$ contains $\rho$, the subfield $K^H$ consists of $\rho$-invariants and therefore is totally real; in particular,

$$K^H \subset \mathbb{R}.$$

2.5. Let $\ell$ be a prime and $S(\ell)$ be the set of maximal ideals $\mathfrak{P}$ of $\mathcal{O}_K$ that divide $\ell$. Since $K/\mathbb{Q}$ is a Galois extension, $G$ acts transitively on $S(\ell)$. In particular, $\#(S(\ell))$ divides $\#(G) = 2^n$. This implies that if $\ell$ splits completely in $K$, i.e.,

$$\#(S(\ell)) = 2^n = \#(G)$$

then the action of $G$ on $S(\ell)$ is free.

On the other hand, if a prime $\ell$ does not split completely in $K$, i.e.,

$$\#(S(\ell)) < 2^n = \#(G),$$

then the action of $G$ on $S(\ell)$ is not free. Let $H(\ell)$ be the stabilizer of any $\mathfrak{P} \in S(\ell)$, which does not depend on a choice of $\mathfrak{P}$, because $G$ is commutative. Then $H(\ell)$ is a nontrivial subgroup of $G$ and therefore contains $\rho$, i.e.,

$$\rho(\mathfrak{P}) = \mathfrak{P} \quad \forall \mathfrak{P} \in S(\ell)$$

if $\ell$ does not split completely in $K$.

Let $e(\ell)$ be the ramification index in $K/\mathbb{Q}$ of $\mathfrak{P} \in S(\ell)$, which does not depend on $\mathfrak{P}$, because $K/\mathbb{Q}$ is Galois. We have the equality of ideals

$$\ell \mathcal{O}_K = \prod_{\mathfrak{P} \in S(\ell)} \mathfrak{P}^{e(\ell)}.$$  (4)
It follows that $K/\mathbb{Q}$ is unramified at $\ell$ if and only if $e(\ell) = 1$. We write
\[ \text{ord}_\mathfrak{P} : K^* \to \mathbb{Z} \]
for the discrete valuation map attached to $\mathfrak{P}$. We have
\[ \text{ord}_\mathfrak{P}(\ell) = e(\ell) \ \forall \mathfrak{P} \in S(\ell); \] (6)
\[ \text{ord}_\mathfrak{P}(u) \geq 0 \ \forall u \in \mathcal{O}_K \setminus \{0\}, \mathfrak{P} \in S(\ell); \] (7)
\[ \text{ord}_\mathfrak{P}(\rho(u)) = \text{ord}_{\rho(\mathfrak{P})}(u) \ \forall u \in K^*, \mathfrak{P} \in S(\ell). \] (8)

2.6. Let $p$ be a prime, $j$ a positive integer, and $q = p^j$. Let $\pi \in O_K$ be a Weil’s $q = p^j$-number. Let us consider the ideal $\pi \mathcal{O}_K$ in $\mathcal{O}_K$. Then there is a nonnegative integer-valued function
\[ d_{\pi} : S(p) \to \mathbb{Z}^+, \mathfrak{P} \mapsto d_{\pi}(\mathfrak{P}) := \text{ord}_\mathfrak{P}(\pi) \] (9)
such that
\[ \pi \mathcal{O}_K = \prod_{\mathfrak{P} \in S(p)} \mathfrak{P}^{d_{\pi}(\mathfrak{P})}. \] (10)
It follows from (3) that
\[ d_{\pi}(\mathfrak{P}) + d_{\pi}(\rho(\mathfrak{P})) = \text{ord}_\mathfrak{P}(q) = j \cdot e(\ell) \ \forall \mathfrak{P} \in S(p). \] (11)

Lemma 2.7. Let $\pi \in O_K$ be a Weil’s $q = p^j$-number. If $p$ does not split completely in $K$ then $\pi^2/q$ is a root of unity.

Proof. Since $p$ does not split completely in $K$, it follows from arguments of Subsection 2.4 that
\[ \rho(\mathfrak{P}) = \mathfrak{P} \ \forall \mathfrak{P} \in S(p). \]
It follows from (11) that
\[ d_{\pi}(\mathfrak{P}) = \frac{j \cdot e(p)}{2} \ \forall \mathfrak{P} \in S(p); \]
in particular, $j$ is even if $e(p) = 1$ (i.e., if $K/\mathbb{Q}$ is unramified at $p$). This implies that $\pi^2/q$ is a $\mathfrak{P}$-adic unit for all $\mathfrak{P} \in S(p)$. On the other hand, it follows from (3) that $\pi^2/q$ is an $\ell$-adic unit for all primes $\ell \neq p$. It follows from the very definition of Weil’s numbers that
\[ |\sigma(\pi^2/q)|_\infty = 1 \ \forall \sigma \in G. \]
(Here $| \cdot |_\infty : \mathbb{C} \to \mathbb{R}_+$ is the standard archimedean value on $\mathbb{C}$.) Now it follows from a classical theorem of Kronecker [16, Ch. IV, Sect. 4, Th. 8] that $\pi^2/q$ is a root of unity. $\square$

Lemma 2.8. Suppose that a prime $p$ completely splits in $K$. (In particular, $K/\mathbb{Q}$ is unramified at $p$.) Let $\pi \in O_K$ be a Weil’s $q = p^j$-number. Then either $\mathbb{Q}(\pi) = K$ or $j$ is even and $\pi = \pm p^{j/2}$.}

ISOGENY CLASSES OF ABELIAN VARIETIES 9
Proof. So, $K/\mathbb{Q}$ is unramified at $p$, i.e., $e(p) = 1$ and

$$p\mathcal{O}_K = \prod_{\mathfrak{p} \in S(p)} \mathfrak{p}.$$  \hfill (12)

This implies that

$$q\mathcal{O}_K = \prod_{\mathfrak{p} \in S(p)} \mathfrak{p}^j.$$  \hfill (13)

Since $p$ splits completely in $K$, the group $G$ acts freely on $S(p)$, in light of Subsection 2.5. In particular,

$$\mathfrak{p} \neq \rho(\mathfrak{p}) \forall \mathfrak{p} \in S(p).$$  \hfill (14)

If the subfield $\mathbb{Q}(\pi)$ of $K$ does not coincide with $K$ then it is totally real, thanks to arguments of Subsection 2.4. This implies that $\rho(\pi) = \pi$. It follows from (3) that $\pi^2 = q$, i.e., $\pi = \pm p^{j/2}$. This implies that the ideal $q\mathcal{O}_K$ is a square. It follows from (13) that $j$ is even. \hfill \square

2.9. Suppose that a prime $p$ completely splits in $K$.

**Definition 2.10.** Let $\pi \in \mathcal{O}_K$ be a Weil’s $q = p^j$-number. We say that $\pi$ is an ordinary Weil’s $q$-number if the “slope” $\text{ord}_\mathfrak{p}(\alpha)/\text{ord}_\mathfrak{p}(q)$ is an integer for all $\mathfrak{p} \in S(p)$.

It (is well known and) follows from (3), (7) and (8) that if $\pi$ is an ordinary Weil’s $q$-number then

$$\frac{\text{ord}_\mathfrak{p}(\pi)}{\text{ord}_\mathfrak{p}(q)} = 0 \text{ or } 1.$$  \hfill (15)

3. Equivalence classes of ordinary Weil’s $q$-numbers

Let $p$ be a prime that splits completely in $K$. Throughout this section, by Weil’s numbers we mean Weil’s $q$-numbers where $q$ is a power of $p$. We write $W(q, K)$ for the set of Weil’s $q$-numbers in $K$. We write $\mu_K$ for the (finite cyclic) multiplicative group of roots of unity in $K$.

**Definition 3.1.** Let $q$ and $q'$ be integers $> 1$ that are integral powers of $p$. Let $\pi \in K$ (resp. $\pi' \in K$) be a Weil’s $q$-number (resp. Weil’s $q'$-number). Following Honda [6], we say that $\pi$ and $\pi'$ are equivalent, if there are positive integers $a$ and $b$ such that $\pi^a$ is Galois-conjugate to $\pi'^b$.

Clearly, if $\pi$ and $\pi'$ are equivalent then $\pi$ is ordinary if and only if $\pi'$ is ordinary. In order to classify ordinary Weil’s numbers in $K$ up to equivalence, we introduce the following notion that is inspired by the
notion of CM type for complex abelian varieties [10] (see also [6, Sect. 1, Th. 2] and [12, Sect. 5]).

**Definition 3.2.** We call a subset $\Phi \subset S(p)$ a $p$-type if $S$ is a disjoint union of $\Phi$ and $\rho(\Phi)$.

Clearly, $\Phi \subset S(p)$ is a $p$-type if and only if the following two conditions hold (recall that $[K : \mathbb{Q}] = 2^n$).

(i) $\#(\Phi) = 2^{n-1}$.  
(ii) If $\mathfrak{P} \in \Phi$ then $\rho(\mathfrak{P}) \not\in \Phi$.

It is also clear that $\Phi \subset S(p)$ is a $p$-type if and only if $\rho(\Phi)$ is a $p$-type.

Let $H(p)$ be the set of nonzero ideals $\mathfrak{B}$ of $\mathcal{O}_K$ such that

$$\mathfrak{B} \cdot \rho(\mathfrak{B}) = p \cdot \mathcal{O}_K.$$  

In light of (12) and (14), an ideal $\mathfrak{B}$ of $\mathcal{O}_K$ lies in $H(p)$ if and only if there exists a $2^{n-1}$-element subset $\Phi = \Phi(\mathfrak{B})$ of $H(p)$ that meets every $\rho$-orbit of $S(p)$ at exactly one place and

$$\mathfrak{B} = \prod_{\mathfrak{P} \in \Phi(\mathfrak{B})} \mathfrak{P}. \quad (16)$$

Such a $\Phi(\mathfrak{B})$ is uniquely determined by $\mathfrak{B} \in H(p)$: namely, it coincides with the set of maximal ideals in $\mathcal{O}_K$ that contain $\mathfrak{B}$. This implies that

$$\#(H(p)) = 2^{2n-1}. \quad (17)$$

Clearly,

$$\Phi(\sigma(\mathfrak{B})) = \sigma(\Phi(\mathfrak{B})) \quad \forall \sigma \in G. \quad (18)$$

**Lemma 3.3.** Let $m$ be a positive integer and $\pi$ be a Weil’s $q = p^m$-number in $K$. Then the following conditions are equivalent.

(i) $\pi$ is ordinary.

(ii) There exists an ideal $\mathfrak{B} \in H(p)$ such that

$$\pi \mathcal{O}_K = \mathfrak{B}^m. \quad (19)$$

(iii) The subset

$$\Psi(\pi) := \{ \mathfrak{P} \in S(p) \mid \frac{\text{ord}_\mathfrak{P}(\pi)}{\text{ord}_\mathfrak{P}(q)} = 1 \} \quad (20)$$

is a $p$-type.

If these equivalent conditions hold then such an ideal $\mathfrak{B}$ is unique and

$$\Phi(\mathfrak{B}) = \Psi(\pi).$$
Proof. We have
\[ \pi \mathcal{O}_K = \prod_{\mathfrak{p} \in S(p)} \mathfrak{p}^{d(\mathfrak{p})}, \] (21)
for some \( d(\mathfrak{p}) \in \mathbb{Z}_+ \) such that
\[ d(\mathfrak{p}) + d(\rho(\mathfrak{p})) = m, \] (22)
\[ \frac{\operatorname{ord}_\mathfrak{p}(\pi)}{\operatorname{ord}_\mathfrak{q}(q)} = \frac{d(\mathfrak{p})}{m} \quad \forall \mathfrak{p} \in S(p). \] (23)
This implies that
\[ \Psi(\pi) := \{ \mathfrak{p} \in S(p) \mid d(\mathfrak{p}) = m \} \subset S(p). \] (24)
Combining (24) with (22), we obtain that
\[ \rho(\Psi(\pi)) := \{ \mathfrak{p} \in S(p) \mid d(\mathfrak{p}) = 0 \} = \{ \mathfrak{p} \in S(p) \mid \frac{\operatorname{ord}_\mathfrak{p}(\pi)}{\operatorname{ord}_\mathfrak{q}(q)} = 0 \} \subset S(p); \] (25)
in particular, the subsets \( \Psi(\pi) \) and \( \rho(\Psi(\pi)) \) do not meet each other.

In light of (20) and (25) combined with (15), \( \pi \) is ordinary if and only if \( S(p) \) is a disjoint union of \( \Psi(\pi) \) and \( \rho(\Psi(\pi)) \), i.e., \( \Psi(\pi) \) is a \( p \)-type. This proves the equivalence of (i) and (iii). If (i) and (iii) hold then it follows from (21) that
\[ \pi \mathcal{O}_K = \prod_{\mathfrak{p} \in \Psi(\pi)} \mathfrak{p}^m = \mathfrak{B}^m \] where \( \mathfrak{B} := \prod_{\mathfrak{p} \in \Psi(\pi)} \mathfrak{p}. \)
Since \( \Psi(\pi) \) is a \( p \)-type, \( \mathfrak{B} \in H(p) \) and obviously \( \Phi(\mathfrak{B}) = \Psi(\pi) \). This proves that equivalent (i) and (iii) imply (ii).

Let us assume that (ii) holds. This means that there is \( \mathfrak{B} \in H(p) \) that satisfies (19). This implies that
\[ \mathfrak{B} = \prod_{\mathfrak{p} \in \Phi(\mathfrak{B})} \mathfrak{p}, \quad \pi \mathcal{O}_K = \mathfrak{B}^m = \prod_{\mathfrak{p} \in \Phi(\mathfrak{B})} \mathfrak{p}^m. \]
It follows that
\[ \frac{\operatorname{ord}_\mathfrak{p}(\pi)}{\operatorname{ord}_\mathfrak{q}(q)} = 1 \quad \forall \mathfrak{p} \in \Phi(\mathfrak{B}), \]
\[ \frac{\operatorname{ord}_\mathfrak{p}(\pi)}{\operatorname{ord}_\mathfrak{q}(q)} = 0 \quad \forall \mathfrak{p} \not\in \Phi(\mathfrak{B}). \]
This implies that \( \pi \) is ordinary and therefore (ii) implies (i). So, we have proven the equivalence of (i),(ii), (iii). The uniqueness of such \( \mathfrak{B} \) is obvious. \( \Box \)

Lemma 3.4. The natural action of \( G \) on \( H(p) \) is free. In particular, \( H(p) \) partitions into a disjoint union of \( 2^{2^n-1-n} \) orbits of \( G \), each of which consists of \( 2^n \) elements.
Proof. Suppose that there exists \( B \in H(p) \) such that its stabilizer
\[
G_B = \{ \sigma \in G \mid \sigma(B) = B \}
\]
is a nontrivial subgroup. Then \( G_B \) must contain \( \rho \), thanks to the arguments of Subsection 2.4. This means that \( \rho(B) = B \) and therefore
\[
p \cdot \mathcal{O}_K = B \cdot \rho(B) = B^2,
\]
which is not true, since \( p \) is unramified in \( K \). The obtained contradiction proves that the action of \( G \) on \( H(p) \) is free. Hence, every \( G \)-orbit in \( H(p) \) consists of \( \#(G) = 2^n \) elements and the number of such orbits is
\[
\frac{\#(H(p))}{\#(G)} = \frac{2^{2n-1}}{2^n} = 2^{2n-1-n}.
\]
□

In what follows we define (non-canonically) certain \( G \)-equivariant injective maps \( \mathcal{Z}, \Pi \) and \( \Pi_1 \) from \( H(p) \) to \( K \); they will play a crucial role in the classification of ordinary Weil's numbers in \( K \) up to equivalence.

Corollary 3.5. Let \( c = \exp(K) \). Then there exists a \( G \)-equivariant map
\[
\mathcal{Z} : H(p) \to \mathcal{O}_K \setminus \{0\} \subset \mathcal{O}_K \subset K
\]
such that \( \mathcal{Z}(B) \) is a generator of \( B^c \) for all \( B \in H(p) \).

Proof. We define \( \mathcal{Z} \) separately for each \( G \)-orbit \( O \subset H(p) \). Pick \( B_O \in O \) and choose a generator \( z_O \) of the principal ideal \( B^c_O \). In light of Lemma 3.4, if \( B \in O \) then there is precisely one \( \sigma \in G \) such that \( B = \sigma(B_O) \). This implies that
\[
B^c = \sigma(B_O)^c = \sigma(B_O) = \sigma(z_O) \mathcal{O}_K,
\]
i.e., \( \sigma(z_O) \) is a generator of \( B^c \). It remains to put
\[
\mathcal{Z}(B) := \sigma(z_O).
\]
□

Theorem 3.6. Let us put
\[
c := \exp(K), \quad q := p^c.
\]
Let \( K_0 = K^p \) be the maximal totally real subfield of \( K \).

(1) There exists an injective map
\[
\Pi : H(p) \to W(q^2, K), \quad B \mapsto \Pi(B)
\]
that enjoys the following properties.

(0) \( \Pi \) is \( G \)-equivariant, i.e.,
\[
\Pi(\sigma(B)) = \sigma(\Pi(B)) \forall \sigma \in G, B \in H(p).
\]
(i) For all $B \in H(p)$ the ideal $\Pi(B)O_K$ coincides with $B^{2c}$.

(ii) The image $\Pi(H(p))$ consists of ordinary Weil’s $q^2$-numbers.

(iii) If $\pi'$ is an ordinary Weil’s $p^m$-number in $K$ then there exists precisely one $B \in H(p)$ such that the ratio $(\pi')^{2c}/\Pi(B)^m$ is a root of unity.

(iv) Let $B_1, B_2 \in H(p)$. Then Weil’s $q^2$-numbers $\Pi(B_1)$ and $\Pi(B_2)$ are equivalent if and only if $B_1$ and $B_2$ lie in the same $G$-orbit.

(v) If $h$ is a positive integer then the subfield $\mathbb{Q}(\Pi(B)^h)$ of $K$ generated by $\Pi(B)^h$ coincides with $K$.

(vi) Suppose that every totally positive unit in $U_{K_0}$ is a square in $K_0$ (and therefore in $U_{K_0}$). Then there exists a map

$$\Pi_0 : H(p) \to W(q, K)$$

that enjoys the following properties.

(a) $\Pi_0(B)^2 = \Pi(B)$ for all $B$.

(b) $\Pi_0$ is $G$-equivariant “up to sign”, i.e.,

$$\Pi_0(\sigma(B)) = \pm \sigma(\Pi_0(B)) \quad \forall \sigma \in G, B \in H(p).$$

(c) If $h$ is a positive integer then the subfield $\mathbb{Q}(\Pi_0(B)^h)$ of $K$ generated by $\Pi_0(B)^h$ coincides with $K$.

(d) $\Pi_0(B)$ is an ordinary Weil’s $q$-number for all $B \in H(p)$.

**Proof.** Let us choose $Z : H(p) \to \mathcal{O}_E \setminus \{0\}$ that enjoys the properties described in Corollary 3.5. Let $B \in H(p)$. In order to define $\Pi(B)$, notice that

$$B \cdot \rho(B) = p\mathcal{O}_K; \quad B^c = z\mathcal{O}_K$$

where

$$z = Z(B) \in \mathcal{O}_K \setminus \{0\}. \quad (28)$$

Then $z\rho(z)$ is a generator of the ideal

$$B^c \cdot \rho(B^c) = (B \cdot \rho(B))^c = p^c \cdot \mathcal{O}_K = q\mathcal{O}_K.$$

Since $\rho$ is the complex conjugation, $z\rho(z)$ is a real (i.e., $\rho$-invariant) totally positive element of $\mathcal{O}_K$. Clearly,

$$u := \frac{z\rho(z)}{q}$$

is an invertible element of $\mathcal{O}_K$ that is also $\rho$-invariant and totally positive unit in $U_{K_0}$. Obviously,

$$q = \frac{z \cdot \rho(z)}{u}.$$
Now let us put
\[ \Pi(\mathfrak{B}) := q \cdot \frac{z}{\rho(z)} = \frac{z^2}{z\rho(z)/q} = \frac{z^2}{u} \in \mathcal{O}_K. \tag{29} \]

If \( u \) is a square in \( K_0 \) then there is a unit \( u_0 \) in \( K_0 \) such that \( u = u_0^2 \).
If this is the case then let us put
\[ \Pi_0(\mathfrak{B}) := \frac{z}{u_0} \in \mathcal{O}_K \quad \text{and get} \quad \Pi_0(\mathfrak{B})^2 = \left( \frac{z}{u_0} \right)^2 = \frac{z^2}{u} = \Pi(\mathfrak{B}). \tag{30} \]

Clearly,
\[ \Pi(\mathfrak{B}) \cdot \mathcal{O}_K = z^2 \cdot \mathcal{O}_K = (z \cdot \mathcal{O}_K)^2 = \mathfrak{B}^{2e}, \tag{31} \]

which proves (i). In order to check that \( \Pi(\mathfrak{B}) \) is a Weil’s \( q^2 \)-number, notice that
\[ \Pi(\mathfrak{B}) \cdot \rho(\Pi(\mathfrak{B})) = q \cdot \frac{z}{\rho(z)} \cdot \rho \left( q \cdot \frac{z}{\rho(z)} \right) = q^2 \cdot \frac{z}{\rho(z)} \cdot \frac{\rho(z)}{z} = q^2. \]

In light of Remark 2.2, this proves that \( \Pi(\mathfrak{B}) \) is a Weil’s \( q^2 \)-number. It follows from (30) that if \( \Pi_0(\mathfrak{B}) \) is defined then it is a Weil’s \( q \)-number. By construction,
\[ \Pi(\mathfrak{B}) \mathcal{O}_K = \mathfrak{B}^{2e}, \]

which also implies that \( \Pi(\mathfrak{B}) \) is \( p^{2e} = q^2 \)-ordinary Weil’s number. The \( G \)-invariance of \( \mathcal{O} \) (see Corollary 3.5) combined with (28) and (29) implies the \( G \)-equivariance of \( \Pi \), which proves (i). The injectiveness of \( \Pi \) follows from (31). This proves (i) and (ii).

In order to prove (v), notice that if \( \mathcal{Q}(\Pi(\mathfrak{B})^h) \) does not coincide with \( K \) then it consists of \( \rho \)-invariants (Subsection 2.4). In particular, the ideal \( \Pi(\mathfrak{B})^h \mathcal{O}_K = \mathfrak{B}^{2eh} \) coincides with its complex-conjugate
\[ \rho \left( \Pi(\mathfrak{B})^h \mathcal{O}_K \right) = \rho \left( \mathfrak{B}^{2eh} \right) = \rho(\mathfrak{B})^{2eh}. \]

This implies that \( \mathfrak{B} = \rho(\mathfrak{B}) \), which is not the case, since \( \mathfrak{B} \in H(p) \).

The obtained contradiction proves (v).

In order to prove (iii), we need to check that if \( \pi' \) is an ordinary Weil’s \( p^m \)-number in \( K \) then it is equivalent to \( \Pi(\mathfrak{B}) \) for some \( \mathfrak{B} \in H(p) \). In order to do that, let us consider the ideal \( \mathfrak{M} := \pi' \mathcal{O}_K \) in \( \mathcal{O}_K \). Since \( \pi' \cdot \rho(\pi') = p^m \), we get \( \mathfrak{M} \cdot \rho(\mathfrak{M}) = p^m \mathcal{O}_K \). It follows that
\[ \mathfrak{M} = \prod_{\mathfrak{P} \in S(p)} \mathfrak{P}^{d(\mathfrak{P})}, \quad d(\mathfrak{P}) + d(\rho(\mathfrak{P})) = m \quad \forall \mathfrak{P} \in S(p). \]

The ordinarity of \( \mathfrak{M} \) implies that
\[ d(\mathfrak{P}) = 0 \quad \text{or} \quad m \quad \forall \mathfrak{P} \in S(p). \]
This implies that if we put
\[ \Phi = \{ \mathfrak{P} \in S(p) \mid d(\mathfrak{P}) = m \} \subset S(p) \]
then \( \Phi \) is a \( p \)-type and
\[
\mathfrak{m} = \prod_{\mathfrak{P} \in \Phi} \mathfrak{P}^m = \left( \prod_{\mathfrak{P} \in \Phi} \mathfrak{P} \right)^m.
\]
It is also clear that
\[ \mathfrak{B} := \prod_{\mathfrak{P} \in \Phi} \mathfrak{P} \in H(p), \]
and
\[ (\pi')^{2c} \mathcal{O}_K = \mathfrak{m}^{2c} = \mathfrak{B}^{2cm} = (\Pi((\mathfrak{B}) \mathcal{O}_K)^m = \Pi(\mathfrak{B}^m) \mathcal{O}_K). \]
It follows from Remark 2.3 that the ratio \( \Pi(\mathfrak{B})^m / (\pi')^{2c} \) is a root of unity. The uniqueness follows from the already proven (i).

Let us prove (iv). The already proven (0) tells us that if \( \mathfrak{B}_2 = \sigma(\mathfrak{B}_2) \) for \( \sigma \in G \) then \( \Pi(\mathfrak{B}_2) = \sigma(\Pi(\mathfrak{B}_1)) \) and therefore Weil’s numbers \( \Pi(\mathfrak{B}_1) \) and \( \Pi(\mathfrak{B}_2) \) are equivalent.

Conversely, suppose that \( \Pi(\mathfrak{B}_1) \) and \( \Pi(\mathfrak{B}_2) \) are equivalent. This means that there are positive integers \( a, b \), a Galois automorphism \( \sigma \in G \), and a root of unity \( \zeta \in \mu_K \) such that
\[ \Pi(\mathfrak{B}_2)^a = \zeta \cdot \sigma(\Pi(\mathfrak{B}_1))^b. \]
This implies the equality of the corresponding ideals in \( \mathcal{O}_K \):
\[ \Pi(\mathfrak{B}_2)^a \mathcal{O}_K = \sigma(\Pi(\mathfrak{B}_1))^b \mathcal{O}_K = \Pi(\sigma(\mathfrak{B}_1))^b. \]
This means (in light of already proven (i)) that
\[ \mathfrak{B}_2^{2ca} = (\sigma(\mathfrak{B}_1))^{2cb}, \]
which implies \( \mathfrak{B}_2 = \sigma(\mathfrak{B}_1) \). Hence \( \mathfrak{B}_1 \) and \( \mathfrak{B}_2 \) lie in the same \( G \)-orbit.

Let us prove (vi). Actually, we have already constructed the map \( \Pi_0 : H(p) \to \mathcal{O}_K \), checked that its image lies in \( W(q, K) \); we have also proven property (vi)(a). As for (vi)(b), it follows readily from (30) combined with the \( G \)-equivariance of \( \Pi \). As for (vi)(c), it follows readily from (v) combined with (30). In order to prove (vi)(d), it suffices to recall that \( \Pi(\mathfrak{B}) \) is an ordinary Weil’s \( q^2 \)-number and notice that in light of (30), the integer
\[
\frac{\text{ord}_p(\Pi(\mathfrak{B}))}{\text{ord}_p(q^2)} = \frac{2\text{ord}_p(\Pi_0(\mathfrak{B}))}{2\text{ord}_p(q^2)} = \frac{\text{ord}_p(\Pi_0(\mathfrak{B}))}{\text{ord}_p(q^2)}. \]
\( \square \)
4. Abelian varieties with Weil’s numbers in $K$

As above, $p$ is a prime, $m$ a positive integer and $q = p^m$.

**Theorem 4.1.** Let $A$ be a simple abelian variety over $k = \mathbb{F}_q$ such that the corresponding Weil’s $q$-number 

$$\pi_A \in K.$$ 

Let $\mathbb{Q}(\pi_A)$ be the subfield of $K$ generated by $\pi_A$.

(i) Suppose that either $\mathbb{Q}(\pi_A) \neq K$ or $p$ does not split completely in $K$.

Then $A$ is supersingular.

(ii) If $p$ splits completely in $K$, $\mathbb{Q}(\pi_A) = K$ and $\pi_A$ is not ordinary then the division $\mathbb{Q}$-algebra $\text{End}_k^0(A)$ is not commutative.

(iii) If $\pi_A$ is ordinary then $K = \mathbb{Q}(\pi_A)$, and $\text{End}_k^0(A) \cong K$; in particular, $\text{End}_k^0(A)$ is commutative.

**Proof.** (i) It follows from Lemmas 2.7 and 2.8 that $\pi_A^2/q$ is a root of unity. This means that $A$ is supersingular.

(ii-iii) Recall [11, 12] that $E := \text{End}_k^0(A)$ is a central division algebra over the field $\mathbb{Q}(\pi_A) = K$. Since $p$ splits completely in $K$, the $\mathfrak{P}$-adic completion $K_{\mathfrak{P}}$ of $K$ coincides with $\mathbb{Q}_p$, i.e.,

$$[K_{\mathfrak{P}} : \mathbb{Q}_p] = 1 \quad \forall \mathfrak{P} \in S(p).$$

By [12, Th. 1], the local $\mathfrak{P}$-adic invariant

$$\text{inv}_{\mathfrak{P}}(E) \in \mathbb{Q}/\mathbb{Z}$$

of the central division $K$-algebra $E$ is given by the formula

$$\text{inv}_{\mathfrak{P}}(E) = \frac{\text{ord}_{\mathfrak{P}}(\pi_A)}{\text{ord}_{\mathfrak{P}}(q)} [K_{\mathfrak{P}} : \mathbb{Q}_p] \mod \mathbb{Z} = \frac{\text{ord}_{\mathfrak{P}}(\pi_A)}{\text{ord}_{\mathfrak{P}}(q)} \mod \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}. \quad (32)$$

All other local invariants of $E$ (outside $S(p)$) are 0 (ibid).

Suppose that $\pi_A$ is ordinary. Then $\mathbb{Q}(\pi_A) = K$, because otherwise $\mathbb{Q}(\pi_A) \subset \mathbb{R}$ and therefore $\pi_A$ is real, i.e., $A$ is supersingular [12, Examples], which is not the case. Since $\pi_A$ is ordinary, all the slopes $\text{ord}_{\mathfrak{P}}(\pi_A)/\text{ord}_{\mathfrak{P}}(q)$ are integers and therefore $\text{inv}_{\mathfrak{P}}(E) = 0$ for all $\mathfrak{P} \in S(p)$. This implies that the division algebra $E = \text{End}_k^0(A)$ is actually a field, i.e., is isomorphic to $K$. This proves (iii).

In order to prove (ii), assume that $\pi_A$ is not ordinary. Then there is a maximal ideal $\mathfrak{P} \in S(p)$ such that the ratio $\text{ord}_{\mathfrak{P}}(\pi_A)/\text{ord}_{\mathfrak{P}}(q)$ is not an integer, i.e.

$$\frac{\text{ord}_{\mathfrak{P}}(\pi_A)}{\text{ord}_{\mathfrak{P}}(q)} \mod \mathbb{Z} \neq 0 \quad \text{in} \quad \mathbb{Q}/\mathbb{Z}. \quad (33)$$
Combining (33) with (32), we obtain that $\text{inv}_E(E) \neq 0$. It follows that $E = \text{End}_k^0(A)$ does not coincide with its center, i.e., is noncommutative. This proves (ii).

**Remark 4.2.** Let $A$ be a simple abelian variety over $\mathbb{F}_q$ such that $\pi_A \in K$. Obviously, $A$ is ordinary if and only if $\pi_A$ is ordinary.

5. **Honda-Tate theory for ordinary abelian varieties**

As above, $p$ is a prime that splits completely in $K$, $m$ a positive integer and $q = p^m$.

Let $\pi \in K$ be a Weil’s $q$-number. The Honda-Tate theory [11, 6, 12] attaches to $\pi$ a simple abelian variety $\mathcal{A}$ over $\mathbb{F}_q$ that is defined up to an $\mathbb{F}_q$-isogeny and enjoys the following properties.

Let $\text{Fr}_\mathcal{A} : \mathcal{A} \to \mathcal{A}$ be the Frobenius endomorphism of $\mathcal{A}$ and $F := \mathbb{Q}[\text{Fr}_\mathcal{A}]$ be the $\mathbb{Q}$-subalgebra of the division $\mathbb{Q}$-algebra $E := \text{End}_{\mathbb{F}_q}^0(\mathcal{A})$ (which is actually a subfield). Then $F$ is the center of $E$ and there is a field embedding

$$i : F \hookrightarrow \mathbb{C} \text{ such that } i(\text{Fr}_\mathcal{A}) = \pi.$$

**Lemma 5.1.** Suppose $\pi$ is ordinary and $\mathbb{Q}(\pi^h) = K$ for all positive integers $h$. Then $\mathcal{A}$ is an absolutely simple $2^{n-1}$-dimensional ordinary abelian variety, $\text{End}_0^0(A) \cong K$, and all endomorphisms of $\mathcal{A}$ are defined over $\mathbb{F}_q$.

**Proof.** Since $\mathbb{Q}(\pi) = K$, we get $i(F) = K$. In particular, number fields $K$ and $F$ are isomorphic. In light of Theorem 4.1, $\mathcal{A}$ is an ordinary abelian variety with commutative endomorphism algebra $E = F \cong K$.

By Theorem 2(c) of [11, Sect. 3],

$$\dim(\mathcal{A}) = \frac{[E : \mathbb{Q}]}{2} = \frac{[K : \mathbb{Q}]}{2} = 2^{n-1}.$$ 

We are going to prove that $\mathcal{A}$ is absolutely simple and all its endomorphisms are defined over $\mathbb{F}_q$. Let $h$ be a positive integer and $k = \mathbb{F}_q^h$ a degree $h$ field extension of $\mathbb{F}_q$. Let $\mathcal{A}_k = \mathcal{A} \times_{\mathbb{F}_q} k$ be the abelian variety over $k$ obtained from $\mathcal{A}$ by the extension of scalars. There is the natural embedding (inclusion) of $\mathbb{Q}$-algebras

$$\text{End}_{\mathbb{F}_q}^0(\mathcal{A}) \subset \text{End}_{k}^0(\mathcal{A}_k)$$

such that the Frobenius endomorphism $\text{Fr}_{\mathcal{A}_k}$ coincides with $\text{Fr}_{\mathcal{A}}^h$. In particular,

$$\mathbb{Q}[\text{Fr}_{\mathcal{A}_k}] \subset \mathbb{Q}[\text{Fr}_{\mathcal{A}}] = F.$$

In addition,

$$i(\text{Fr}_{\mathcal{A}_k}) = i(\text{Fr}_{\mathcal{A}}^h) = i(\text{Fr}_{\mathcal{A}})^h = \pi^h.$$
Since $\mathbb{Q}[\pi^h] = K = \mathbb{Q}(\pi)$, we get
\[ i(\mathbb{Q}[\text{Fr}_{A_k}]) = K = i(\mathbb{Q}[\text{Fr}_A]). \]
Hence, $\mathbb{Q}[\text{Fr}_{A_k}] = \mathbb{Q}[\text{Fr}_A]$ is a number field of degree $2\dim(A) = 2\dim(A_k)$. Applying again Theorem 2(c) of [11, Sect. 3] to $A_k$, we conclude that
\[ \text{End}^0(A_k) = \mathbb{Q}[\text{Fr}_{A_k}] = \mathbb{Q}[\text{Fr}_A] = \text{End}^0_{F_q}(A) \]
for all finite overfields $k$ of $F_q$. This implies that $\text{End}^0(A_k) = \text{End}^0_{F_q}(A)$, i.e., all the endomorphisms of $A$ are defined over $F_q$. In particular, $A$ is absolutely simple and $\text{End}^0(A) \cong K$.

\[ \square \]

6. Proofs of main results

As above, $c = \exp(K)$, a prime $p$ splits completely in $K$ and $q = p^c$.

Proof of Theorem 1.6. Let $\Pi : H(p) \to W(q^2, K)$ be as in Theorem 3.6. Let $A \in H(p)$ and let $\Pi(A)$ be the corresponding ordinary Weil's $q^2$-number in $K$. In light of Theorem 3.6(v), $\mathbb{Q}[\Pi(A)] = K$ for all positive integers $h$. In light of Lemma 5.1 applied to $q^2$ and $\Pi(A)$, the Honda-Tate theory [11, 6, 12] attaches to $\Pi(A)$ an absolutely simple $2^{n-1}$-dimensional abelian variety $A = A(A)$ over $\mathbb{F}_{q^2}$ (that is defined up to an $\mathbb{F}_{q^2}$-isogeny) such that $\text{End}^0(A) \cong K$, and all endomorphisms of $A(A)$ are defined over $\mathbb{F}_{q^2}$.

By Theorem 3.6(iv), if $B_1, B_2 \in H(p)$ then the Weil numbers $\Pi(B_1)$ and $\Pi(B_2)$ are equivalent if and only if $B_1$ and $B_2$ belong to the same $G$-orbit. In light of [11, Theorem 1], [6, p. 84] combined with Lemma 3.4, all the $A(A)$ lie in precisely $2^{n-1-n}$ isogeny classes of abelian varieties over $\overline{\mathbb{F}}_p$. We also know that each of these varieties is ordinary, has dimension $2^{n-1}$ and their endomorphism algebras are isomorphic to $K$.

Now, let us prove that each abelian variety $B$ over $\overline{\mathbb{F}}_p$, whose endomorphism algebra is isomorphic to $K$, is isogenous to one of $A(A)$ over $\overline{\mathbb{F}}_p$.

In order to do that, first, notice that since $K$ is a field, $B$ is simple over $\overline{\mathbb{F}}_p$. Second, $B$ is defined with all its endomorphisms over a certain finite field $k = \mathbb{F}_{q^2h}$ (where $h$ is a certain positive integer), i.e., there is a simple abelian variety $B_k$ over $k$ such that
\[ B = B_k \times_k \overline{\mathbb{F}}_p, \quad \text{End}^0_k(B_k) = \text{End}^0(B) \cong K. \]
Applying Theorem 2(c) of [11, Sect. 3] to $\mathcal{B}_k$, we get

$$K \cong \text{End}^0_\mathbb{Q} (\mathcal{B}) = \text{End}^0_{\mathbb{Q}_k} (\mathcal{B}_k) = \mathbb{Q}[	ext{Fr}_{\mathcal{B}_k}]$$

where Fr$_{\mathcal{B}_k}$ is the Frobenius endomorphism of $\mathcal{B}_k$. This gives us a field isomorphism $\mathbb{Q}[	ext{Fr}_{\mathcal{B}_k}] \to K$; let us denote by $\pi_{\mathcal{B}_k}$ the image of Fr$_{\mathcal{B}_k}$ in $K$. Clearly, $\mathbb{Q}(\pi_{\mathcal{B}_k}) = K$; according to a classical result of Weil [7], $\pi_{\mathcal{B}_k}$ is a Weil’s $q^h$-number. It follows from Theorem 3.6(iii) that there is $\mathcal{B} \in H(p)$ such that Weil’s numbers $\pi_{\mathcal{B}_k}$ and $\Pi(\mathcal{B})$ are equivalent. This means (thanks to Theorem 1 of [11], see also [6, pp. 83–84]) that absolutely simple abelian varieties $\mathcal{B}_k$ and $A(\mathcal{B})$ become isogenous over $\overline{\mathbb{F}}_p$. It follows that absolutely simple abelian varieties $\mathcal{B} = \mathcal{B}_k \times_k \overline{\mathbb{F}}_p$ and $A(\mathcal{B})$ are isogenous over $\overline{\mathbb{F}}_p$.

This proves (i), (ii)(1) and (ii)(2). It remains to prove (ii)(3). It suffices to check that for each $\mathcal{B} \in H(p)$ there exists an abelian variety $A_0$ that is defined over $\mathbb{F}_q$ with all its endomorphism and such that $A(\mathcal{B})$ is isogenous to $A_0$ over $\overline{\mathbb{F}}_p$.

Let $\Pi_0 : H(p) \to W(q, K)$ be as in Theorem 3.6(vi) and $\Pi_0(\mathcal{B})$ be the corresponding ordinary Weil’s $q$-number in $K$. In light of Theorem 3.6(vi)(c), $\mathbb{Q}[\Pi_0(\mathcal{B})^h] = K$ for all positive integers $h$. In light of Lemma 5.1 applied to $q$ and $\Pi_0(\mathcal{B})$, the Honda-Tate theory [11, 6, 12] attaches to Weil’s $q$-number $\Pi_0(\mathcal{B})$ an absolutely simple $2^{n-1}$-dimensional abelian variety $\mathcal{A}_0$ over $\mathbb{F}_q$ (that is defined up to an $\mathbb{F}_q$-isogeny) such that $\text{End}^0(\mathcal{A}_0) \cong K$, and all endomorphisms of $\mathcal{A}_0$ are defined over $\mathbb{F}_q$.

Since $\Pi_0(\mathcal{B})^2 = \Pi(\mathcal{B})$, Weil’s numbers $\Pi_0(\mathcal{B})$ and $\Pi(\mathcal{B})$ are equivalent. As above, in light of Theorem 1 of [11] (see also [6, pp. 83–84]), the corresponding absolutely simple abelian varieties $\mathcal{A}_0$ and $A(\mathcal{B})$ are isogenous over $\overline{\mathbb{F}}_p$. This ends the proof.

Proof of Corollary 1.14. Recall that $r$ is an odd prime and $\zeta_r$ is a primitive $r$th root of unity. Clearly, $\mathbb{Q}(\zeta_r)$ is a CM field. Hence, its subfield $K$ is either CM or a totally real. Since $H$ has odd order $m$, it does not contain the complex conjugation $\rho : \mathbb{Q}(\zeta_r) \to \mathbb{Q}(\zeta_r)$, because $\rho$ has order 2. Hence, $\rho$ acts nontrivially on $K = \mathbb{Q}(\zeta_r)^H = K^{(r)}$, which implies that $K$ is a CM field. (See also [2, p. 78].) Its degree

$$[K : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_r) : \mathbb{Q}]}{\#(H)} = \frac{m \cdot 2^n}{m} = 2^n.$$
We also know (Remark 1.15) that every totally positive unit in $K_0$ is a square in $K_0$.

Clearly, $K/Q$ is ramified at $r$ and unramified at every prime $p \neq r$. Let us find which $p \neq r$ split completely in $K$. Let

$$f_p \in \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}) = (\mathbb{Z}/r\mathbb{Z})^*$$

be the Frobenius element attached to $p$, which is characterized by the property

$$f_p(\zeta_r) = \zeta_p^r.$$ 

In other words,

$$f_p = p \mod r \in (\mathbb{Z}/r\mathbb{Z})^* = \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}).$$

Clearly, $p$ splits completely in $K$ if and only if $f_p \in H$. So, we need to find when $f_p$ lies in $H$. In order to do it, notice that

$$H = \{\sigma^{2^n} | \sigma \in \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}) = (\mathbb{Z}/r\mathbb{Z})^*\}.$$ 

This implies that $f_p$ lies in $H$ if and only if $p \mod r$ is a $2^r$th power in $\mathbb{Z}/r\mathbb{Z}$ = $F_r$. This ends the proof of (0).

The remaining assertions (i) and (ii) follow from Theorem 1.6 combined with (0).

Proof of Corollary 1.8. In the notation of Corollary 1.14, this is the case when $m = 1$ and $2^n = r - 1$. By little Fermat’s theorem, every nonzero $a \in \mathbb{Z}/r\mathbb{Z}$ satisfies

$$a^{2^n} = a^{r-1} = 1.$$ 

Now the desired result follows readily from Corollary 1.14.

References

[1] Z.I. Borevich, I.R. Shafarevich, Number Theory, 3rd edition (in Russian). Nauka, Moscow, 1985.
[2] P.E. Conner, J. Hurrelbrink, Class Number Parity. World Scientific, Singapore, 1988.
[3] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Semin. Univ. Hamburg 14 (1941), 197—272.
[4] M. Deuring, Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. III. Göttingen Nach. 1956, n 4, 37—76.
[5] H. Hasse, Über die Klassenzahl abelscher Zahlkörper. Akademie-Verlag, Berlin 1952; new edition: Springer-Verlag, Berlin Heidelberg New York, 1985.
[6] T. Honda, Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan 20 (1968), 83—95.
[7] D. Mumford, Abelian varieties, 2nd edition. Oxford University Press, 1974.
[8] F. Oort, The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field. J. Pure Appl. Algebra 3 (1973), 399–408.

[9] J.-P. Serre and J. Tate, Good reduction of abelian varieties. Ann. Math. (2) 88 (1968), 492–517.

[10] G. Shimura, Abelian varieties with complex multiplication and modular functions. Princeton University Press, Princeton, NJ, 1997.

[11] J. Tate, Endomorphisms of abelian varieties over finite fields. Invent. Math. 2 (1966), 134–144.

[12] J. Tate, Classes d’isogénie des variétés abéliennes sur un corps fini (d’après Honda). Séminaire Bourbaki, N 352 (1968). Springer Lecture Notes in Math. 179 (1971), 95–110.

[13] L. Washington, Introduction to cyclotomic fields, 2nd edition. Springer Verlag, New York, 1997.

[14] W.C. Waterhouse, Abelian varieties over finite fields. Annales scientifiques de l’É.N.S. 4e série, 2:4 (1969), 521–560.

[15] L. Watson, https://mathoverflow.net/questions/393506/isomorphic-endomorphism-algebras-implies-isogenous-for-abelian-varieties-over-f/ .

[16] A. Weil, Basic Number Theory, 3rd edition. Springer Verlag, New York, 1973.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

Email address: zarhin@math.psu.edu