S. Turner
Nagoya Math. J.
Vol. 77 (1980), 1-4

PRINCIPAL POLARIZATIONS OF ABELIAN SURFACES OVER FINITE FIELDS

STUART TURNER

In § 1 of this note we construct abelian varieties of dimension two defined over F_{p^n}, n odd, which admit infinitely many distinct principal polarizations. These polarizations determine an infinite family of geometrically non-isomorphic complete singular curves defined and irreducible over F_{p^n} which have isomorphic Jacobian varieties. In § 2 we calculate the zeta function of these curves.

§ 1.

Let $q = p^n$, n odd, and $\pi = q^{1/2}$. Then $\{\pm\pi\}$ is a conjugacy class of Weil numbers for q which corresponds to an isogeny class of simple abelian varieties defined over F_q([1], [5]). Let A be a member of this isogeny class, $\mathrm{End}(A)$ be the ring of F_q-endomorphisms of A and $E = \mathrm{End}(A) \otimes \boldsymbol{Q}$. E is a division algebra with center $\Phi = \boldsymbol{Q}(\pi)$. E has invariant 1/2 at each of the real places of Φ, invariant zero at each finite place of Φ prime to p, and invariant

$$\mathrm{ord}_v(\pi) \cdot [\Phi_v : \boldsymbol{Q}_p] / \mathrm{ord}_v(q) \pmod 1$$

at the one place v of Φ which lies over p; v is ramified so this last invariant is zero. Finally, $2 \dim A = [E:\Phi]^{1/2}[\Phi:\boldsymbol{Q}]$, ([5], [6], [8]). Since $[E:\Phi]^{1/2}$ is the least common multiple of the denominators of the invariants, $\dim A = 2$.

$\mathrm{End}(A)$ contains π ([7], Prop. 3.5), so $Z[p^{1/2}] \subset \mathrm{End}(A)$. $Z[p^{1/2}]$ is an order in Φ (the maximal order if $p \equiv 2, 3 \pmod 4$), so by Dirichlet's theorem, the units in $Z[p^{1/2}]$ form a group isomorphic to $\{\pm 1\} \times Z$. Hence $\mathrm{Aut}\, A$, the group of F_q-automorphisms of A, contains an element of infinite order.

$A \times \mathrm{Spec}\, F_{q^2}$ has Weil number $\pi^2 = q$. Using the theorem of Tate cited above one sees that the isogeny class of simple abelian varieties

Received February 24, 1978.

defined over F_{q^2} with Weil number q consists of elliptic curves. Since their endomorphism algebra is a quaternion algebra over $\boldsymbol{Q}$ with invariants 1/2 at the real place of $\boldsymbol{Q}$ and at the p-adic place, they are supersingular curves ([4], p. 217). So $A \times \operatorname{Spec} F_{q^2}$ is F_{q^2}-isogenous to a product of isomorphic supersingular elliptic curves. Let E be a curve in this isogeny class. The Frobenius automorphism $F \in \operatorname{Gal}(F_{q^2}/F_q)$ transforms E into an elliptic curve $E^{(q)}$ and there is a canonical purely inseparable isogeny $i: E \to E^{(q)}$. $E \times E^{(q)}$ is F_{q^2}-isogenous to $A \times \operatorname{Spec} F_{q^2}$.

Let 0 (resp. 0′) be a rational point on E (resp. $E^{(q)}$). Define a group law on E (resp. $E^{(q)}$) such that 0 (resp. 0′) is the identity for this addition. Let $X = E \times \{0'\} + \{0\} \times E^{(q)}$. X is a divisor on $E \times E^{(q)}$, rational over F_{q^2}. X determines a principal polarization $\mathscr{C}(X)$ on $E \times E^{(q)}$.

PROPOSITION. *F_q is a field of definition for the principally polarized abelian variety $(E \times E^{(q)}, \mathscr{C}(X))$.*

Proof. The proposition asserts the existence of an abelian variety B defined over F_q, of a F_q-rational divisor Y on B, and of a F_{q^2}-isomorphism $\psi: B \times \operatorname{Spec} F_{q^2} \to E \times E^{(q)}$ such that $\psi(Y \times F_{q^2}) = X$. To show that this descent is possible it suffices to construct a cocycle $h \in Z^1(G, \operatorname{Aut}(E \times E^{(q)}))$ and an F_q-isomorphism $\phi: h_F(E \times E^{(q)}) \to (E \times E^{(q)})^F$ such that $\phi(h_F(X)) = X^F$.

Let e be the identity of G and h_e be identity automorphism of $E \times E^{(q)}$. Let $h_F: E \times E^{(q)} \to E^{(q)} \times E$ be the automorphism which interchanges the factors of the product. One verifies immediately that h is a cocycle. Let

$$\phi: E^{(q)} \times E \to (E \times E^{(q)})^F = E^{(q)} \times E$$

be the identity morphism;

$$\phi(h_F(X)) = \{0\} \times E^{(q)} + E \times \{0'\} = X^F .$$

COROLLARY. *B is a F_q-simple abelian variety and Y is a curve of genus two, irreducible over F_q.*

Proof. B has Weil numbers $\pm q^{1/2}$ and is therefore F_q-isogenous to A, hence F_q-simple. Y is an F_q-irreducible curve on B because the action of h_F on $E \times E^{(q)}$ interchanges the two components of X and Y is the quotient of X by this action. Y has genus two because $Y \times F_{q^2} \cong X$.

THEOREM 1. *B admits infinitely many distinct principal polarizations defined over $\boldsymbol{F}_q$.*

Proof. For any $a \in \operatorname{Aut} B$, the group of $\boldsymbol{F}_q$-automorphisms of B, the $\boldsymbol{F}_q$-rational divisor $a^{-1}(Y)$ determines a principal polarization of B ([4], p. 63). The group of automorphisms of a polarized abelian variety is finite ([3], Proposition 8, p. 194), so there are only finitely many $b \in \operatorname{Aut} B$ such that $\mathscr{C}(b^{-1}(Y)) = \mathscr{C}(a^{-1}(Y))$. On the other hand, B has Weil numbers $\pm q^{1/2}$ so $\operatorname{Aut} B$ contains an element of infinite order and the theorem follows.

THEOREM 2. *For any $a \in \operatorname{Aut} B$, $a^{-1}(Y)$ is a curve of genus two, irreducible over $\boldsymbol{F}_q$. Let $b \in \operatorname{Aut} B$ such that $\mathscr{C}(a^{-1}(Y)) \neq \mathscr{C}(b^{-1}(Y))$, then $a^{-1}(Y)$ and $b^{-1}(Y)$ are geometrically non-isomorphic.*

Proof. $a^{-1}(Y) \times \boldsymbol{F}_{q^2} = a^{-1}(X) = a^{-1}(E \times \{0'\}) + a^{-1}(\{0\} \times E^{(q)})$. $E \times \{0'\}$ and $\{0\} \times E^{(q)}$ are abelian subvarieties of B so the two components of $a^{-1}(X)$ are abelian subvarieties of $B \times \boldsymbol{F}_{q^2}$. However, B is a $\boldsymbol{F}_q$-simple abelian variety so neither of these components can be defined over $\boldsymbol{F}_q$. Hence $a^{-1}(Y)$ is $\boldsymbol{F}_q$-irreducible and is clearly of genus two. The second assertion follows immediately from Theorem 1 of [2].

§ 2.

Let $B(\boldsymbol{F}_{q^m})$ denote the group of $\boldsymbol{F}_{q^m}$-rational points of B. Each $a \in \operatorname{Aut} B$ determines an isomorphism $a: B(\boldsymbol{F}_{q^m}) \to B(\boldsymbol{F}_{q^m})$ for each m. Hence the singular curves Y and $a(Y)$ have the same zeta function. Y has only one $\boldsymbol{F}_q$-rational point, the one point of X which is fixed under the action of h_F. This is the identity of B and is the unique singular point of Y. This same point is the unique singular point of $a(Y)$.

Let $\tilde{Y}$ be the $\boldsymbol{F}_q$-normalization of Y and $p: \tilde{Y} \to Y$ be the canonical projection. $\tilde{Y}$ is a complete, non-singular curve of genus two defined and irreducible over $\boldsymbol{F}_q$. $\tilde{Y}$ is geometrically disconnected because $Y \times \boldsymbol{F}_{q^2} = E \times \{0'\} + \{0\} \times E^{(q)}$, so $\tilde{Y} \times \boldsymbol{F}_{q^2} = E \times \{0'\} \amalg \{0\} \times E^{(q)}$. $\tilde{Y}$ can be recovered from $\tilde{Y} \times \boldsymbol{F}_{q^2}$ by a descent similar to the one used in the proof of the proposition. The action of G on $\tilde{Y} \times \boldsymbol{F}_{q^2}$ has no fixed points so $\tilde{Y}$ has no $\boldsymbol{F}_q$-rational points; the singular point of Y blows up to two $\boldsymbol{F}_{q^2}$-rational points on $\tilde{Y}$. Let ζ_Y denote the zeta function of Y. Then $\zeta_{\tilde{Y}}(T) = \zeta_Y(T)(1 - T)/(1 - T^2)$.

E has Weil number q, so $\zeta_E(T) = (qT - 1)^2/(1 - T)(1 - q^2T)$. Since $\tilde{Y}$ has no F_{q^r}-rational point for odd r, $\zeta_{\tilde{Y}}(T) = \zeta_E(T^2)$. Finally, $\zeta_Y(T) = (qT^2 - 1)^2/(1 + T)(1 - T^2)(1 - q^2T^2)$.

References

[1] Honda, T., Isogeny classes of abelian varieties over finite fields, J. Math. Soc. Japan **20** (1968), 83–95.
[2] Hoyt, W. L., On products and algebraic families of Jacobian varieties, Ann. of Math. **77** (1963), 415–423.
[3] Lang, S., Abelian Varieties, Interscience, New York, 1959.
[4] Mumford, D., Abelian Varieties, Oxford University Press, London, 1970.
[5] Tate, J., Classes d'isogénie des variétés abéliennes sur un corps fini, Sem. Bourbaki **21** (1968/69), no. 352.
[6] Tate, J., Endomorphisms of abelian varieties over finite fields, Invent. Math. **2** (1966), 134–144.
[7] Waterhouse, W., Abelian varieties over finite fields, Ann. scient. Éc. Norm. Sup. **4**, t. 2 (1969), 521–560.
[8] Waterhouse W. and Milne, J. S., Abelian varieties over finite fields, in Proc. Symp. Pure Math. **XX**, American Mathematical Society, Providence, (1971), 53–64.

Pontifícia Universidade Católica
do Rio de Janeiro