Canad. Math. Bull. Vol. **42** (1), 1999 pp. 78–86

Fermat Jacobians of Prime Degree over Finite Fields

Josep González

Abstract. We study the splitting of Fermat Jacobians of prime degree ℓ over an algebraic closure of a finite field of characteristic p not equal to ℓ. We prove that their decomposition is determined by the residue degree of p in the cyclotomic field of the ℓ-th roots of unity. We provide a numerical criterion that allows to compute the absolutely simple subvarieties and their multiplicity in the Fermat Jacobian.

Introduction

Let $\ell > 2$ be an integer. We denote by $\mathcal{C}_\ell$ the Fermat curve of degree ℓ and by $J(\mathcal{C}_\ell)$ its jacobian. Let p be a prime not dividing ℓ and let $q = p^f$, where f is the residue degree of p in $\mathbf{Q}(\mu_\ell)$. The splitting of $J(\mathcal{C}_\ell)$ over $\overline{\mathbf{Q}}$ was studied by Koblitz and Rohrlich in [Ko-Ro 78] and over a finite field $\mathbf{F}_q$ it was treated by Yui in [Yu 80]. The purpose of this paper is to determine the splitting of $J(\mathcal{C}_\ell)$ over $\overline{\mathbf{F}}_p$ when ℓ is prime.

It is known that $J(\mathcal{C}_\ell)$ is $\mathbf{Q}$-isogenous to the product of the $\ell - 2$ jacobians of curves, which we denote by $\mathcal{C}_{\ell,k}$, for $2 \le k \le \ell - 1$ (*cf.* [Sch 84]). We determine the splitting of $J(\mathcal{C}_{\ell,k})$ over $\overline{\mathbf{F}}_p$ and we give a criterion to determine when two absolutely simple factors of $J(\mathcal{C}_{\ell,k})$, $J(\mathcal{C}_{\ell,k'})$ are $\overline{\mathbf{F}}_p$-isogenous.

In Section 1, we describe some facts about abelian varieties over finite fields. In Section 2, we begin summarizing known facts concerning to the zeta function of the curves $\mathcal{C}_\ell/\mathbf{F}_q$ and we give some results about the Hasse-Witt invariants of the curves $\mathcal{C}_{\ell,k}/\overline{\mathbf{F}}_q$, which will be used in the last section to obtain the main result of the paper.

I would like to end this introduction by expressing my gratitude to Pilar Bayer for her help.

1 On the Abelian Varieties over Finite Fields

Let p be a prime integer. We fix a positive integer n and consider the power $q = p^n$. Throughout this paper, A denotes an abelian variety defined over the finite field $\mathbf{F}_q$. Let $\varphi \in \operatorname{End}_{\mathbf{F}_q}(A)$ be the relative Frobenius endomorphism, whose action on the variety raises to the q-th power the coordinates of the points of A. We denote by $\operatorname{End}_{\mathbf{F}_q}(A)$ the ring of endomorphisms of A which are defined over $\mathbf{F}_q$. The $\mathbf{Q}$-algebra $\operatorname{End}^0_{\mathbf{F}_q}(A) := \mathbf{Q} \otimes_{\mathbf{Z}} \operatorname{End}_{\mathbf{F}_q}(A)$ has $\mathbf{Q}(\varphi)$ as its center. For a given prime number $\ell \neq p$, we denote by $T_\ell(A)$ the Tate module of A and by $V_\ell(A) := \mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} T_\ell(A)$.

If A is $\mathbf{F}_q$-simple, then $\mathbf{Q}(\varphi)$ is a number field. In this case, the class in the Brauer group of $\mathbf{Q}(\varphi)$ of the simple algebra $\operatorname{End}^0_{\mathbf{F}_q}(A)$ is characterized by the local invariants

Received by the editors June 11, 1997; revised September 24, 1997.
This research has been partially supported by DGICYT, PB-93-0034.
AMS subject classification: Primary 11G20; Secondary 14H40.

$i_{\mathfrak{p}} = f_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(\varphi)/n$ at each prime $\mathfrak{p}$ over p in $\mathbb{Q}(\varphi)$ (here, $f_{\mathfrak{p}}$ stands for the residue degree at $\mathfrak{p}$); on each real prime, the local invariant is equal to $1/2$; on the remaining primes, the algebra splits. The lowest common denominator e of all the invariants $i_{\mathfrak{p}}$ is the period of the endomorphism algebra $\operatorname{End}^0_{\mathbb{F}_q}(A)$; the characteristic polynomial of φ on $V_\ell(A)$ equals the e-th power of the $\mathbb{Q}$-irreducible polynomial of φ and $\dim A = [\mathbb{Q}(\varphi) : \mathbb{Q}]e/2$ (*cf.* [Ta 66], [Wa 69]).

Fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$; each Weil q-number $\alpha \in \bar{\mathbb{Q}}$ determines, up to isogenies, an $\mathbb{F}_q$-simple abelian variety $A/\mathbb{F}_q$ such that the $\mathbb{Q}$-irreducible polynomial of φ equals the $\mathbb{Q}$-irreducible polynomial of α. This assignment establishes a one to one correspondence between the conjugacy classes of Weil q-numbers and the $\mathbb{F}_q$-isogeny classes of $\mathbb{F}_q$-simple abelian varieties defined over $\mathbb{F}_q$ (*cf.* [Ta 68]).

Let α be a Weil q-number. For each positive integer m, we denote by A_m an abelian variety associated to the Weil q^m-number α^m. There exists an integer $t > 0$ such that $\mathbb{Q}(\alpha^t) = \mathbb{Q}(\alpha^{tm})$ for all integers $m > 0$. For this t, we have that A_t is absolutely simple, $\operatorname{End}^0_{\mathbb{F}_q}(A_t) = \operatorname{End}^0_{\mathbb{F}_{q^t}}(A_t)$ and A_1 is $\mathbb{F}_{q^t}$-isogenous to $A_t^{\dim A_1/\dim A_t}$.

Let α_1, α_2 be two Weil q-numbers such that $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) =: K$, and let A_1, A_2 be abelian varieties associated to α_1 and α_2, respectively. Then the following properties hold:

i) If the ideals (α_1), (α_2) in the ring of integers of K coincide, then A_1 and A_2 are $\bar{\mathbb{F}}_q$-isogenous (*cf.* [Go 98]).
ii) If $K/\mathbb{Q}$ is a galois extension, then A_1 and A_2 are $\bar{\mathbb{F}}_q$-isogenous if and only if there exists $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ such that $(\alpha_2) = \big(\sigma(\alpha_1)\big)$.

We note that the abelian variety associated to a Weil q-number α is $\bar{\mathbb{F}}_q$-isogenous to a power of a supersingular elliptic curve if and only if the ideals (α^2) and (q) do coincide or, equivalently, the ideal (α) is invariant under complex conjugation.

2 The Fermat Curves of Prime Degree

In what follows, K denotes the prime field $\mathbb{Q}$ or $\mathbb{F}_p$, and $\bar{K}$ is a fixed algebraic closure of K. We denote by $\mathcal{C}_\ell/K$ the Fermat curve, defined as the projective plane curve

$$Y^\ell = X^\ell + Z^\ell,$$

where $\ell \neq p$ is an odd prime number. The curve $\mathcal{C}_\ell$ is non-singular and has genus $g = (\ell-2)(\ell-1)/2$. For $2 \le k \le \ell - 1$, let $C_{\ell,k}/\bar{K}$ be the projective plane curve

$$V^\ell = UW^{k-1}(U+W)^{\ell-k},$$

which has singularities at the points

$$(u,v,w) = \begin{cases} (1,0,0) & \text{if } k > 2 \\ (-1,0,1) & \text{if } k < \ell - 1. \end{cases}$$

Let $\phi_k \colon \mathcal{C}_\ell \to C_{\ell,k}$ be the morphism defined by $u = x^\ell$, $v = xy^{\ell-k}z^{k-1}$, $w = z^\ell$ and $\psi_k \colon \mathcal{C}_{\ell,k} \to C_{\ell,k}$ be the normalization of the curve $C_{\ell,k}$.

Let $\zeta \in \bar{K}$ be a primitive ℓ-th root of unity and $\gamma_k\colon \mathcal{C}_\ell \to \mathcal{C}_\ell$ be the automorphism defined by $(x, y, z) \mapsto (x\zeta^k, y\zeta, z)$, which does not have fixed points and is of order ℓ. We have that $\phi_k = \phi_k \circ \gamma_k$ and the curve $\mathcal{C}_{\ell,k}$ is isomorphic to the quotient curve of $\mathcal{C}_\ell$ by the group of order ℓ generated by γ_k. Let $\pi_k\colon \mathcal{C}_\ell \to \mathcal{C}_{\ell,k}$ be the corresponding projection. We have that π_k is unramified and ψ_k is a morphism such that $\psi_k \circ \pi_k = \phi_k$. By the Hurwitz formula, the genus of $\mathcal{C}_{\ell,k}$ is $(\ell - 1)/2$. Note that π_k is defined on any extension of K containing the ℓ-th roots of unity. Thus, if $K = \mathbb{F}_p$ and $p^m \equiv 1 \pmod{\ell}$, then π_k and ψ_k are both defined over $\mathbb{F}_{p^m}$; in this case, it is easy to see that the number of $\mathbb{F}_{p^m}$-rational points of $\mathcal{C}_{\ell,k}/\bar{K}$ and that of $C_{\ell,k}/\bar{K}$ coincide.

Let $\mathbb{Q}(\mu_\ell)$ be the field of ℓ-th roots of unity, f the residue degree of p in $\mathbb{Q}(\mu_\ell)$, and $q = p^f$. We denote $G := (\mathbb{Z}/\ell\mathbb{Z})^*$ and let H be the subgroup of G of order f. Given a generator $g \in G$, we identify G with $\mathrm{Gal}\big(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\big)$. Then H can be identified with the decomposition group of p in $\mathbb{Q}(\mu_\ell)$.

The roots α_i, $1 \le i \le 2g$, of characteristic polynomial of the relative Frobenius of the curve $\mathcal{C}_\ell/\mathbb{F}_q$ acting on the Tate module of its Jacobian can be determined in the following way (*cf.* [Da-Ha 35]). Let

$$\mathcal{D} := \{\bar{a} = (a_1, a_2) \in (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^* \mid a_1 + a_2 \not\equiv 0 \pmod{\ell}\}.$$

Then $\#\mathcal{D} = (\ell - 1)(\ell - 2) = 2g$. Let us choose a character χ of order ℓ of the multiplicative group $\mathbb{F}_q^*$, extended to $\mathbb{F}_q$ with $\chi(0) = 0$. For each $\bar{a} = (a_1, a_2) \in \mathcal{D}$, let us consider the Jacobi sum

$$j(\bar{a}) := -\sum_{(v_1,v_2)} \chi(v_1)^{a_1} \chi(v_2)^{a_2},$$

where $(v_1, v_2) \in \mathbb{F}_q \times \mathbb{F}_q$ with $v_2 = v_1 + 1$. Then,

$$\prod_{i=1}^{2g} (x - \alpha_i) = \prod_{\bar{a} \in \mathcal{D}} \big(x - j(\bar{a})\big).$$

The group G acts on $\mathcal{D}$ as follows: $G \times \mathcal{D} \to \mathcal{D}$, $(m, \bar{a}) \mapsto m\bar{a} = (ma_1, ma_2)$. Given $c \in G$, we denote by $\langle c \rangle$ the least natural number such that $\langle c \rangle \equiv c \pmod{\ell}$. The decomposition of the ideal $\big(j(\bar{a})\big)$ into prime ideals in $\mathbb{Q}(\mu_\ell)$ is as follows (*cf.* [Shi-Ka 79]). Given a prime ideal $\mathfrak{p} | (p)$, we write $\mathfrak{p}_i := \mathfrak{p}^{\sigma_{-i}}$. For each $\bar{a} = (a_1, a_2) \in \mathcal{D}$, let us define

$$E(\bar{a}) := \sum_{h \in H} \left[\frac{\langle ha_1 \rangle + \langle ha_2 \rangle}{\ell} \right] = \sum_{k=1}^{f} \left[\frac{\langle g^{k(\ell-1)/f} a_1 \rangle + \langle g^{k(\ell-1)/f} a_2 \rangle}{\ell} \right],$$

where [ ] denotes the integer part. Then, there exists a prime ideal $\mathfrak{p} | (p)$ in $\mathbb{Q}(\mu_\ell)$ such that

$$\big(j(\bar{a})\big) = \prod_{i=1}^{(\ell-1)/f} \mathfrak{p}_i^{E(g^i \bar{a})}, \quad \text{for all } \bar{a} \in \mathcal{D}.$$

Note that $\mathfrak{p}_i^{\sigma_{-j}} = \mathfrak{p}_{i+j}$, $\mathfrak{p}_{\frac{\ell-1}{2}} = \mathfrak{p}^c$ and $\mathfrak{p}_i = \mathfrak{p}_j$ if and only if $i \equiv j \pmod{\frac{\ell-1}{f}}$. On the other hand, if the $\mathfrak{p}_i$-adic order of $j(\bar{a})$ is $E(m\bar{a})$, then the $\mathfrak{p}_i^c$-adic order of $j(\bar{a})$ is $E(-m\bar{a})$. One has always $E(\bar{b}) + E(-\bar{b}) = f$.

For $2 \leq k \leq \ell - 1$ we write $\mathcal{D}_k := \{(a_1, a_2) \in \mathcal{D} \mid \langle a_1/a_2 \rangle = k-1\} = \{m(k-1, 1) \mid m \in G\}$. Then the set $\mathcal{D}$ is the disjoint union of the sets $\mathcal{D}_k$, since these sets are the equivalence classes defined in $\mathcal{D}$ by the relation $\bar{a} \sim \bar{b}$ if and only if there exists $m \in G$ such that $\bar{a} = m\bar{b}$.

Let $T, S \colon \mathcal{D} \to \mathcal{D}$ be the bijective maps defined by

$$T(a_1, a_2) := (a_1, \ell - a_1 - a_2), \quad S(a_1, a_2) := (a_2, a_1).$$

T, S are compatible with the equivalence relation above. Thus, $T(\mathcal{D}_k) = \mathcal{D}_{\langle 1/k \rangle}$ and $S(\mathcal{D}_k) = \mathcal{D}_{\langle \frac{k}{k-1} \rangle}$. Since S, T are involutions and $(S \circ T)^3(k) = k$, S and T generate the dihedral group D_3. If we write $T(k) := \langle 1/k \rangle$ and $S(k) := \langle k/(k-1) \rangle$, then the group D_3 acts also on the set of indices $2 \leq k \leq \ell - 1$. We have $M(\mathcal{D}_k) = \mathcal{D}_{M(k)}$ for all $M \in D_3$. The curves $\mathcal{C}_{\ell, M(k)}/\bar{K}$, with M running over D_3, are isomorphic (*cf.* [Go 97]).

Proposition 2.1

i) Given $\bar{a} \in \mathcal{D}$ and $M \in D_3$, we have that $j(\bar{a}) = j\big(M(\bar{a})\big)$. In particular,

$$\prod_{\bar{a} \in \mathcal{D}_k} \big(x - j(\bar{a})\big) = \prod_{\bar{a} \in \mathcal{D}_{M(k)}} \big(x - j(\bar{a})\big).$$

ii) The values $j(\bar{a})$, with $\bar{a} \in \mathcal{D}_k$, are the roots of the characteristic polynomial of the Frobenius of the curve $\mathcal{C}_{\ell,k}/\mathrm{F}_q$ acting on the Tate module of its jacobian.

Proof Given two characters χ_1, χ_2 of F_q^*, the generalized Jacobi sum is defined by $J(\chi_1, \chi_2) := -\sum_x \chi_1(x)\chi_2(1-x)$. It satisfies $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$. In our case, if χ denotes a character of order ℓ, then $\chi(-1) = 1$ and $j(a_1, a_2) = J(\chi^{a_1}, \chi^{a_2})$. It is easy to prove that $j\big(S(a_1, a_2)\big) = j(a_1, a_2)$ and $j\big(T(a_1, a_2)\big) = j(a_1, a_2)$.

Let now prove the assertion ii). The number N_m of F_{q^m}-rational points of $\mathcal{C}_{\ell,k}/\mathrm{F}_{q^m}$ is the same as the number of F_{q^m}-rational points of the projective singular curve associated to the affine curve

$$V^\ell = U(U+1)^{\ell-k},$$

which has only one point at infinity that is F_p-rational. Let be a positive integer m and let be a character χ_m of order ℓ of the multiplicative group $\mathrm{F}_{q^m}^*$. Using the Davenport-Hasse theorem, we obtain

$$N_m = 1 + q^m - \sum_{(a_1,a_2) \in \mathcal{D}_{\langle (k-1)/k \rangle}} J(\chi_m^{a_1}, \chi_m^{a_2}) = 1 + q^m - \sum_{\bar{a} \in \mathcal{D}_{\langle (k-1)/k \rangle}} j(\bar{a})^m,$$

and the proposition follows. ■

The curve $\mathcal{C}_\ell/\mathrm{Q}$ has good reduction at p. Let us denote by $r_p(\mathcal{C}_\ell)$, resp. $r_p(\mathcal{C}_{\ell,k})$, the Hasse-Witt invariant of $\mathcal{C}_\ell/\mathrm{F}_p$, resp. $\mathcal{C}_{\ell,k}/\mathrm{F}_p$. These invariants satisfy $r_p(\mathcal{C}_\ell) = \sum_k r_p(\mathcal{C}_{\ell,k})$. We have that (*cf.* [St 79]):

$$r_p(\mathcal{C}_\ell) = \#\{\bar{a} \in \mathcal{D} \mid j(\bar{a}) \notin \mathrm{p}\}, \quad r_p(\mathcal{C}_{\ell,k}) = \#\{\bar{a} \in \mathcal{D}_k \mid j(\bar{a}) \notin \mathrm{p}\}.$$

Therefore,

$$r_p(\mathcal{C}_\ell) = \#\{\bar{a} \in \mathcal{D} \mid E(\bar{a}) = 0\} = \#\{\bar{a} \in \mathcal{D} \mid \langle ha_1\rangle + \langle ha_2\rangle < \ell \text{ for all } h \in H\},$$
$$r_p(\mathcal{C}_{\ell,k}) = \#\{\bar{a} \in \mathcal{D}_k \mid E(\bar{a}) = 0\} = \#\{\bar{a} \in \mathcal{D}_k \mid \langle ha_1\rangle + \langle ha_2\rangle < \ell \text{ for all } h \in H\}.$$

This result coincides with the one obtained in [Go 97] by using Hasse-Witt matrices. It is easy to check that f divides $r_p(\mathcal{C}_{\ell,k})$ and $r_p(\mathcal{C}_\ell)$, and that $J(\mathcal{C}_\ell/\bar{\mathrm{F}}_p)$ is ordinary if and only if $f = 1$.

It is known that the Fermat curves such that their jacobian $J(\mathcal{C}_\ell/\bar{\mathrm{F}}_p)$ is isogenous to the power of a supersingular elliptic curve are those for which f is even (*cf.* [Shi-Ka 79, Proposition 3.10]). This result can be generalized as follows.

Proposition 2.2 *$J(\mathcal{C}_{\ell,k}/\bar{\mathrm{F}}_p)$ has a factor equal to a supersingular elliptic curve if and only if $J(\mathcal{C}_\ell/\bar{\mathrm{F}}_p)$ is isogenous to the power of a supersingular elliptic curve.*

Proof If $J(\mathcal{C}_{\ell,k}/\bar{\mathrm{F}}_p)$ has a supersingular elliptic curve factor, then a power of $j(\bar{a})$ is a power of q, for some $\bar{a} \in \mathcal{D}_k$. Thus, the order of $j(\bar{a})$ at an ideal p is equal to the order at p^c, where c denotes complex conjugation. It follows that f is even. ■

Proposition 2.3 *If $J(\mathcal{C}_{\ell,k}/\bar{\mathrm{F}}_p)$ is ordinary and $f > 1$, then $k-1$ is a primitive cubic root of unity in $(\mathrm{Z}/\ell\mathrm{Z})^*$. If $k-1$ is a primitive cubic root of unity in $(\mathrm{Z}/\ell\mathrm{Z})^*$ and $f = 3$, then $J(\mathcal{C}_{\ell,k}/\bar{\mathrm{F}}_p)$ is ordinary.*

Proof We write $c = k-1$ and $M_c = \{m \in G \mid \langle mc\rangle + \langle m\rangle < \ell\}$. The cardinality of M_c equals the genus of $\mathcal{C}_{\ell,k}/\bar{\mathrm{F}}_p$, since for all $m \in G$ we have that $m \in M_c$ if and only if $-m \notin M_c$. Thus, $J(\mathcal{C}_{\ell,k}/\bar{\mathrm{F}}_p)$ is ordinary if and only if $HM_c = M_c$, since

$$r_p(\mathcal{C}_{\ell,k}) = \#\{m \in G \mid \langle mhc\rangle + \langle mh\rangle < \ell \text{ for all } h \in H\}.$$

Given $m \in G$ and an integer i such that $0 \le i \le c-1$, we have

$$m \in M_c, \quad \langle m\rangle \in \Big(\frac{i\ell}{c}, \frac{(i+1)\ell}{c}\Big) \text{ if and only if } \langle m\rangle \in \Big(\frac{i\ell}{c}, \frac{(i+1)\ell}{c+1}\Big).$$

It follows that M_c coincides with the set of classes of integers mod ℓ in the following set

$$\bigcup_{i=0}^{c-1}\Big(\frac{i\ell}{c}, \frac{(i+1)\ell}{c+1}\Big) = \bigcup_{i=0}^{c-1}\Big[\Big[\frac{i\ell}{c}\Big]+1, \Big[\frac{(i+1)\ell}{c+1}\Big]\Big].$$

Therefore,

$$\sum_{m\in M_c}\langle m\rangle = \frac{\sum_{j=1}^{c}\big(\big[\frac{j\ell}{c+1}\big]^2 + \big[\frac{j\ell}{c+1}\big]\big) - \sum_{i=1}^{c-1}\big(\big[\frac{i\ell}{c}\big]^2 + \big[\frac{i\ell}{c}\big]\big)}{2}.$$

Let n be a positive integer prime to ℓ. We have that $\sum_{j=1}^{n-1}[j\ell/n] = (\ell-1)(n-1)/2 \equiv -(n-1)/2 \pmod{\ell}$. On the other hand, $\{j\ell-[j\ell/n]n \mid 1 \le j \le n-1\} = \{1,\dots,n-1\}$, since $\ell \in (\mathbb{Z}/n\mathbb{Z})^*$. Thus,

$$\sum_{j=1}^{n-1}\left[\frac{j\ell}{n}\right]^2 \equiv \frac{\sum_{j=1}^{n-1} j^2}{n^2} \equiv \frac{(2n-1)(n-1)}{6n} \pmod{\ell}.$$

Applying these results to $n = c$ and $n = c+1$, we have

$$\sum_{m\in M_c} m \equiv -\frac{c^2+c+1}{12c(c+1)} \pmod{\ell}.$$

If $J(\mathcal{C}_{\ell,k}/\bar{\mathbb{F}}_p)$ is ordinary, then M_c is the disjoint union of cosets of H and, therefore, $\sum_{m\in M_c} m \equiv 0 \pmod{\ell}$ since $f > 1$. Hence, $c^2+c+1 \equiv 0 \pmod{\ell}$.

For the second claim, let us assume that $c^2+c+1 \equiv 0 \pmod{\ell}$. Given $m \in M_c$, we have that

$$\langle c^2m\rangle + \langle cm\rangle = \ell - \langle (c+1)m\rangle + \langle cm\rangle = \ell - \langle m\rangle < \ell,$$

since $\langle (c+1)m\rangle = \langle cm\rangle + \langle m\rangle$. Thus, $mc \in M_c$ and $cM_c = M_c$.

Furthermore, if $f = 3$, then the subgroup H is generated by c and the condition $HM_c = M_c$ is equivalent to the condition $cM_c = M_c$. It follows that $J(\mathcal{C}_{\ell,k}/\bar{\mathbb{F}}_p)$ is ordinary. ∎

3 Splitting of Fermat Jacobians

In this section, we show that $J(\mathcal{C}_{\ell,k}/\mathbb{F}_q)$ is $\mathbb{F}_q$-isogenous to a power of an absolutely simple subvariety $A_k/\mathbb{F}_q$ and we determine its dimension. We characterize under which conditions A_k and $A_{k'}$ are $\mathbb{F}_q$-isogenous.

Lemma 3.1

i) If $\bar{a} \in \mathcal{D}_k$, then the characteristic polynomial of relative Frobenius of $\mathcal{C}_{\ell,k}$ acting on the Tate module of its jacobian is $\prod_{\sigma\in G}\Big(X - \sigma\big(j(\bar{a})\big)\Big)$.

ii) For all $\bar{a} \in \mathcal{D}$, we have $j(\bar{a}) \in \mathbb{Q}(\mu_\ell)^H$.

Proof The statement of i) follows from the Proposition 2.1 and the fact that $\sigma_i\big(j(\bar{a})\big) = j(g^i\bar{a})$ for all $1 \le i \le \ell-1$. In order to establish ii), it suffices to prove that $j(\bar{a})$ is invariant under $\sigma_{(\ell-1)/f}$. We take g in such a way that $p \equiv g^{(\ell-1)/f} \pmod{\ell}$ and

$$\sigma_{(\ell-1)/f}\, j(\bar{a}) = j(p\bar{a}) = -\sum_{v_2^p = v_1^p+1} \chi(v_1^p)^{a_1}\chi(v_2^p)^{a_2} = j(a_1,a_2). \qquad ∎$$

Given $\bar{a} \in \mathcal{D}$, we write

$$H_{\bar{a}} := \{\sigma \in G \mid \big(j(\bar{a})\big)^\sigma = \big(j(\bar{a})\big)\}, \quad H_{j(\bar{a})} := \{\sigma \in G \mid \sigma j(\bar{a}) = j(\bar{a})\}.$$

We have that $H \subseteq H_{j(\bar{a})} \subseteq H_{\bar{a}} \subseteq G$ and $\mathbb{Q}\big(j(\bar{a})\big) = \mathbb{Q}(\mu_\ell)^{H_{j(\bar{a})}}$. Let us remark that $H_{\bar{a}} = \{s \in G \mid E(g^i\bar{a}) = E(sg^i\bar{a}), 1 \le i \le (\ell-1)/f\}$ and, therefore, $H_{\bar{a}}$ can be easily computed.

Lemma 3.2 *Let $\bar{a} \in \mathcal{D}_k$. Then the groups $H_{j(\bar{a})}$ and $H_{\bar{a}}$ coincide. Furthermore $H_{j(\bar{a})} = H_{\bar{a}} = G$ if and only if the order of the group $H_{\bar{a}}$ is even.*

https://doi.org/10.4153/CMB-1999-009-7 Published online by Cambridge University Press

Proof If the order of the group $H_{\bar a}$ is even, then the complex conjugation $\sigma_{(\ell-1)/2} \in H_{\bar a}$. By the Proposition 2.2, we have that f is even and $\bigl(j(\bar a)\bigr) = (p^{f/2})$. Since $H \neq \{1\}$, the roots of unity of $\mathbf{Q}(\mu_\ell)^{H_{j(\bar a)}}$ are ± 1 and $j(\bar a)$ is integer. Thus, the groups $H_{j(\bar a)}$, $H_{\bar a}$ coincide with G.

In order to show the equality $H_{j(\bar a)} = H_{\bar a}$, we consider the following two cases: $H_{j(\bar a)} \neq \{1\}$, and $H_{j(\bar a)} = \{1\}$.

First we assume that $H_{j(\bar a)} \neq \{1\}$. If $\sigma \in H_{\bar a}$ then $\sigma j(\bar a) = \pm j(\bar a)$, because the only roots of unity in $\mathbf{Q}(\mu_\ell)^{H_{j(\bar a)}}$ are ± 1. Hence, the group $H_{\bar a}/H_{j(\bar a)}$ is a cyclic group of order 1 or 2. The order cannot be 2 so both groups coincide.

We assume, now, that $H = H_{j(\bar a)} = \{1\}$ and $H_{\bar a} \neq \{1\}$. Let $c = k-1$ and M_c be as in the Proposition 2.3. The group $H_{\bar a}$ is the group $\{h \in G \mid hM_c = M_{\underline{c}}\}$, since $H = \{1\}$. If p' is a prime for which the decomposition group is $H_{\bar a}$, then $J(\mathcal{C}_{\ell,k}/\mathbf{F}_{p'})$ is ordinary. By the Proposition 2.3, c is a cubic primitive root of unity in $(\mathbf{Z}/\ell\mathbf{Z})^*$ and $c \in H_{\bar a}$. We have

$$\bigl(j(c,1)\bigr) = \bigl(j(c^2,c)\bigr), \quad j(c,1) \neq j(c^2,c).$$

Thus there exists $\zeta \in \mu_{2\ell}$ such that $j(c,1) = \zeta j(c^2,c)$ and, hence, there exists a character χ of order ℓ of the group $\mathbf{F}_q^*$ such that

$$\frac{g(\chi)g(\chi^c)}{g(\chi^{-c^2})} = \zeta \frac{g(\chi^c)g(\chi^{c^2})}{g(\chi^{-1})},$$

where $g(\chi)$ denotes the Gauss sum of the character χ. Due to the fact that $g(\chi)g(\chi^{-1}) = g(\chi^{c^2})g(\chi^{-c^2}) = p$, we obtain that $\zeta = 1$, which contradicts $j(c,1) \neq j(c^2,c)$. ∎

Theorem 3.3 *The variety $J(\mathcal{C}_{\ell,k}/\mathbf{F}_q)$ is $\mathbf{F}_q$-isogenous to an m-th power of an $A_k/\mathbf{F}_q$ absolutely simple abelian variety. The $\mathbf{Q}$-algebra $\operatorname{End}^0(A_k)$ has $\mathbf{Q}(\mu_\ell)^{H_{\bar a}}$ as its center. Its local invariants at primes which divide p are $\{E(s\bar a)/f \mid s \in G/H\}$, for any $\bar a \in \mathcal{D}_k$, and the Brauer period e is the least common denominator of $E(s\bar a)/f$, with s running over G/H. We have that*

$$m = \frac{\#H_{\bar a}}{e} \quad \textit{and} \quad e|f|em|r_p(\mathcal{C}_{\ell,k}).$$

Proof Let $\bar a \in \mathcal{D}_k$. By the Lemma 3.1, the characteristic polynomial of the relative Frobenius of $\mathcal{C}_{\ell,k}/\mathbf{F}_q$ acting on the Tate module of its jacobian is given by the $(\#H_{j(\bar a)})$-th power of the $\mathbf{Q}$-irreducible polynomial $\prod_{\sigma \in G/H_{j(\bar a)}} \bigl(X - \sigma\bigl(j(\bar a)\bigr)\bigr)$. Therefore, $J(\mathcal{C}_{\ell,k}/\mathbf{F}_q)$ is $\mathbf{F}_q$-isogenous to a power of a $\mathbf{F}_q$-simple variety, A_k. Given a positive integer t we denote by H_t the subgroup of G that leaves $j(\bar a)^t$ invariant. We have that $H_{j(\bar a)} \subseteq H_t \subseteq H_{\bar a}$. By the Lemma 3.2, it follows that $\mathbf{Q}\bigl(j(\bar a)^t\bigr) = \mathbf{Q}\bigl(j(\bar a)\bigr)$ and, thus, A_k is absolutely simple.

The computation of the local invariants and e can be done from the equality

$$\{f_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}} j(\bar a)/f \mid \mathfrak{p}|p\} = \{E(g^i \bar a)/f \mid 1 \le i \le (\ell-1)/f\}$$

and the fact that if f is even we get $E(g^i\bar a)/f = 1/2$.

Finally, we have that

$$m = \frac{\dim J(\mathcal{C}_{\ell,k})}{\dim A_k} = \frac{(\ell-1)/2}{[\mathbf{Q}(j(\bar a)) : \mathbf{Q}]e/2} = \frac{(\ell-1)/2}{(\ell-1)e/(2\#H_{\bar a})} = \frac{\#H_{\bar a}}{e}.$$

https://doi.org/10.4153/CMB-1999-009-7 Published online by Cambridge University Press

It is obvious that $e|f$. From the inclusion $H \subseteq H_{\bar{a}}$, it follows that $f|em$. We have that $em|r_p(\mathcal{C}_{\ell,k})$ since the characteristic polynomial of the relative Frobenius of $\mathcal{C}_{\ell,k}/\mathbb{F}_q$ acting on the Tate module of its jacobian is the (em)-th power of a $\mathbb{Q}$-irreducible polynomial. ■

Note that if f is odd then $\mathbb{Q}\big(j(\bar{a})\big)$ need not be equal to $\mathbb{Q}(\mu_\ell)^H$. For instance, if $f = 1$ and $\bar{a} \in \mathcal{D}_k$, where $c = k - 1$ is a primitive cubic root of unity, then $\mathbb{Q}\big(j(\bar{a})\big) \neq \mathbb{Q}(\mu_\ell)$, since $j(\bar{a}) \in \mathbb{Q}(\mu_\ell)^{H'}$ where $H' = \{c, c^2, 1\}$.

Theorem 3.4 *The abelian varieties A_k and $A_{k'}$ are $\bar{\mathbb{F}}_q$-isogenous if and only if there exists $t \in G$ such that*

$$E\big(g^i(k'-1,1)\big) = E\big(tg^i(k-1,1)\big) \quad \textit{for all } 1 \le i \le \frac{\ell-1}{f}.$$

In this case, $J(\mathcal{C}_{\ell,k})$ and $J(\mathcal{C}_{\ell,k'})$ are $\bar{\mathbb{F}}_q$-isogenous.

Proof If A_k and $A_{k'}$ are $\bar{\mathbb{F}}_q$-isogenous then $J(\mathcal{C}_{\ell,k})$ and $J(\mathcal{C}_{\ell,k'})$ are $\bar{\mathbb{F}}_q$-isogenous, since both jacobians have the same dimension. This fact happens if and only if there exist $\bar{a} \in \mathcal{D}_k$, $\bar{b} \in \mathcal{D}_{k'}$ such that $\big(j(\bar{a})\big) = \big(j(\bar{b})\big)$, since due to the Lemma 3.2 the condition $\big(j(\bar{a})\big) = \big(j(\bar{b})\big)$ implies that $\mathbb{Q}\big(j(\bar{a})\big) = \mathbb{Q}\big(j(\bar{b})\big)$. Without loss of generality, we can take $\bar{b} = (k'-1,1)$ and there exists $t \in G$ such that $\bar{a} = t(k-1,1)$. ■

3.5 Absolutely Simple Subvarieties of $J(\mathcal{C}_{13})/\bar{\mathbb{F}}_p$, $f = 3$

We are going to compute the decomposition of the jacobian of $\mathcal{C}_{13}/\mathbb{F}_p$, where p is a prime of residue degree $f = 3$, into a product of absolutely simple subvarieties. We can take 2 as generator of G. The decomposition group is $H = \{2^4 \equiv 3, 2^8 \equiv 9, 2^{12} \equiv 1\}$ and $G/H = \{\bar{2}, \bar{4}, \bar{8}, \bar{1}\}$. We have that $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_1^c\mathfrak{p}_2^c$, where the upperindex c denotes the complex conjugation σ_6. The computation of the exponents $E(a_1, a_2)$ corresponding to $\mathcal{C}_{13,2}$ gives the following table:

$\bar{a}$		$3\bar{a}$		$9\bar{a}$		$E(\bar{a})$	$E(-\bar{a})$
$(1,1)$		$(3,3)$		$(9,9)$	$*$	1	2
$(2,2)$		$(6,6)$		$(5,5)$	$*$	0	3
$(3,3)$		$(9,9)$	$*$	$(1,1)$		1	2
$(4,4)$		$(12,12)$	$*$	$(10,10)$	$*$	2	1
$(5,5)$		$(2,2)$		$(6,6)$		0	3
$(6,6)$		$(5,5)$		$(2,2)$		0	3

The number of asterisks yields $E(\bar{a})$. The Hasse-Witt invariant of $\mathcal{C}_{13,2}/\bar{\mathbb{F}}_p$ is the number of zeroes that appear in the $E(\bar{a})$, $E(-\bar{a})$ columns, thus $r_p(\mathcal{C}_{13,2}) = 3$.

On the other hand, $\big(j(1,1)\big) = \mathfrak{p}_1^{E(2,2)}\mathfrak{p}_2^{E(4,4)}\mathfrak{p}_3^{E(8,8)}\mathfrak{p}_4^{E(3,3)} = \mathfrak{p}_2^2(\mathfrak{p}_1^c)^3\mathfrak{p}_2^c$. The subgroup of homomorphisms of G that leaves the ideal $\big(j(1,1)\big)$ invariant is H. The Brauer period of the endomorphism algebra of the simple subvariety is $e = 3$. Therefore, $m = 1$ and $J(\mathcal{C}_{13,2}/\mathbb{F}_q)$ is absolutely simple. For $k = 2, 7, 12$ the corresponding jacobians are isogenous, since

$$\big(j(1,1)\big) = \big(j(1,11)\big) = \big(j(11,1)\big) = \mathfrak{p}_2^2(\mathfrak{p}_1^c)^3\mathfrak{p}_2^c.$$

For $k = 3, 5, 6, 8, 9, 11$ the jacobians are isogenous, since

$$\begin{aligned}\big(j(2,1)\big) = \big(j(4,1)^c\big) = \big(j(10,2)\big) = \big(j(1,2)\big)\\ = \big(j(2,10)\big) = \big(j(1,4)^c\big) = \mathrm{p}_1^2\mathrm{p}_2^2\mathrm{p}_1^c\mathrm{p}_2^c\end{aligned}$$

and $\mathcal{C}_{13,k}/\bar{\mathrm{F}}_p$ have zero Hasse-Witt invariant with $e = 3$ and $m = 1$.

For $k = 4, 10$ the corresponding jacobians are again isogenous, since

$$\big(j(3,1)\big) = \big(j(1,3)\big) = \mathrm{p}_2^3(\mathrm{p}_1^c)^3$$

and $\mathcal{C}_{13,k}/\bar{\mathrm{F}}_p$ have Hasse-Witt invariant equal to 6; therefore, they are ordinary with $e = 1$ and $m = 3$.

In this example the isogeny classes coincide with the isomorphy classes generated by the action of the dihedral group. Thus, we have the following isogeny relation

$$J(\mathcal{C}_{13}) \sim J(\mathcal{C}_{13,2})^3 \times J(\mathcal{C}_{13,3})^6 \times J(\mathcal{C}_{13,4})^2,$$

where the non-ordinary jacobians $J(\mathcal{C}_{13,3})$, $J(\mathcal{C}_{13,2})$ are absolutely simple and $J(\mathcal{C}_{13,4})$ is isogenous to a third power of an absolutely simple variety.

References

[Da-Ha 35] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen*. J. Reine Angew. Math. **172**(1935), 151–182.

[Go 97] J. González, *Hasse-Witt matrices for the Fermat curves of prime degree*. Tôhoku Math. J. **49**(1997), 149–163.

[Go 98] ———, *On the p-rank of an abelian variety and its endomorphism algebra*. Publ. Mat. **42**, to appear.

[Ko-Ro 78] N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*. Canad. J. Math. **6**(1978), 1183–1205.

[Sch 84] C. G. Chmidt, *Arithmetik Abelscher Varietäten mit komplexer Multiplikation*. Lecture Notes in Math. **1082**, Springer, 1984.

[Se 58] J. P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*. Symp. Int. Top. Alg. México (ed. J. P. Serre), ŒUVRES **I**, Springer, 1958, 24–53.

[Shi-Ka 79] T. Shioda and T. Katsura, *On Fermat Varieties.* Tôhoku Math. J. **31**(1979), 97–115.

[St 79] H. Stichtenoth, *Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers*. Arch. Math. **33** (1979), 357–360.

[Ta 66] J. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2**(1966), 134–144.

[Ta 68] ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*. Sém. Bourbaki (1968/69), 95–110.

[Wa 69] W. C. Waterhouse, *Abelian varieties over finite fields*. Ann. Sci. École Norm. Sup. **2**(1969), 521–560.

[We 49] A. Weil, *Number of solutions of equations in finite fields.* Bull. Amer. Math. Soc. **55**, Collected Papers **I**, Springer, 1949, 497–508.

[Yu 80] N. Yui, *On the Jacobian Variety of the Fermat curve*. J. Algebra **65**(1980), 1–45.

Escola Universitària Politècnica de Vilanova i la Geltrú
Departament de Matemàtica Aplicada i Telemàtica
Av. Victor Balaguer s/n
Vilanova i la Geltrú 08800
Spain
e-mail: josepg@mat.upc.es