Honda, T.
Osaka J. Math.
3 (1966), 189-194

ON THE JACOBIAN VARIETY OF THE ALGEBRAIC CURVE $y^2=1-x^l$ OVER A FIELD OF CHARACTERISTIC $p>0$

TAIRA HONDA

(Received July 6, 1966)

Let l be an odd prime number and let J be a Jacobian variety of the curve defined by the equation $y^2=1-x^l$ over a field of characteristic $p>0$. If $p\neq 2, l$, J is an abelian variety of dimension $(l-1)/2$. Our aim in the present paper is to study its endomorphism algebra, its zeta-function and its formal structure. Denote by $\mathcal{A}(J)$ the endomorphism ring of J and put $\mathcal{A}_0(J)=\mathcal{A}(J)\otimes\boldsymbol{Q}$. Let f be the least natural number such that $p^f\equiv 1$ (mod. l) and ζ_p be a primitive l-th root of 1 in $GF(p^f)$. Denote by Z the endomorphism of J corresponding to the birational automorphism of the curve: $(x, y)\to(\zeta_p x, y)$. As for $\mathcal{A}_0(J)$, our idea consists in investigating the subalgebra $R=\boldsymbol{Q}(\Pi, \mathrm{Z})$ of $\mathcal{A}_0(J)$ generated by Z and the p-th power endomorphism Π of J. The arithmetic characterization of Π^f obtained in Davenport-Hasse [1] and in Shimura-Taniyama [6] makes it possible. It turns out that there exists a sharp difference according as f is even or odd. In the first case the structure of R is fairly simple (Theorem 1). The zeta-function of J coincides essentially with that of a direct product of elliptic curves whose Hasse invariants are zero. It is plausible that J is isogenous to a direct product of elliptic curves though R is in general smaller than the endomorphism algebra of the latter. In the second case $\mathcal{A}_0(J)$ coincides with R and is a cyclic algebra over the decomposition field of p in $\boldsymbol{Q}(\mathrm{Z})$. Its local invariants are determined completely by the prime ideal decomposition of Π^f (Theorem 2). On the other hand the prime ideal decomposition of Π^f determines also the formal structure of J (Manin [5]). In this way we obtain simple abelian varieties with various formal structures. (Note that J itself is not always simple when f is odd.)

The method employed here would be applicable to more general types of abelian varieties to some extent. We hope that our results suggest something general for the theory of abelian varieties over finite fields.

1. Let l be an odd prime and let p be another odd prime. Denote by C a complete non-singular model of the function field defined by the equation $y^2=1-x^l$ over the field $GF(p)$ of p elements. It is well known that C has genus

$n=(l-1)/2$. Let J be a Jacobian variety of C. We may assume that J as well as a canonical map φ: $C\to J$ is defined over $GF(p)$.

Let Z, Π and R be as defined before. Z is a primitive l-th root of 1:

$$\mathrm{Z}^l = 1\,. \tag{1}$$

Put $K=\boldsymbol{Q}(\mathrm{Z})$ and let K_0 be the decomposition field of p in K. Putting $g=[K_0:\boldsymbol{Q}]$, we have $[K:K_0]=f$ and $[K:\boldsymbol{Q}]=2n=fg$. By Proposition 1 of [6], Chap. II, the commutor of K in $\mathcal{A}_0(J)$ coincides with K. As we have clearly

$$\Pi\mathrm{Z} = \mathrm{Z}^p\Pi\,, \tag{2}$$

Π^f is contained in K. Moreover we have

$$\Pi^f\in K_0\,, \tag{3}$$

since the map τ: $\alpha\to\Pi\alpha\Pi^{-1}$ is a generating automorphism of K/K_0 and Π^f is fixed by this map. From (1), (2), (3), R is a cyclic algebra (Π^f, K, τ).

The prime ideal decomposition of Π^f is already obtained in Davenport-Hasse [1], but it is more convenient to use results of Shimura-Taniyama [6]. Let C_0 be a complete non-singular model of the function field defined by the equation $y^2=1-x^l$, J_0 its Jacobian, and let φ_0 be a canonical map $C_0\to J_0$, all defined over $\boldsymbol{Q}$. By Theorem 3 of Igusa [3], we may assume that the reductions of C_0, J_0 and φ_0 modulo p are C, J and φ respectively. Put $\zeta=e^{2\pi i/l}$ and let $\iota(\zeta)$ be the endomorphism of J_0 corresponding to the birational automorphism of C_0: $(x, y)\to(\zeta x, y)$. This determines an injection ι: $\boldsymbol{Q}(\zeta)\to\mathcal{A}_0(J_0)$. Denoting by φ_i the element of the Galois group $\mathrm{G}(K/\boldsymbol{Q})$ such that $\varphi_i(\zeta)=\zeta^i$, (J_0, ι) belongs to the simple CM-type $(K;\{\varphi_1,\cdots,\varphi_n\})$ ([6], Chap. II). By Theorem 1 of [6], Chap. III, there exists a prime ideal $\mathfrak{p}$ in K_0 dividing p such that

$$(\Pi^f) = \prod_{i=1}^{n}\mathfrak{p}^{\psi_i} \qquad (\psi_i = \varphi_i^{-1})\,. \tag{4}$$

Now Riemann hypothesis implies that

$$|\Pi^f| = p^{f/2}\,. \tag{5}$$

Finally it is easy to see that

$$\Pi^f \equiv 1 \pmod{2(\mathrm{Z}-1)} \tag{6}$$

from the expression of Π^f by Gaussian sums

$$\Pi^f = \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)}$$

(cf. Davenport-Hasse [1]). The relations (3), (4), (5), (6) characterize Π^f as an algebraic integer.

For later use, we transform (4) into a more convenient form for our purpose. Let ρ be a primitive root modulo l. $G(K/\boldsymbol{Q})$ is generated by σ such that $\sigma(Z)=Z^{\rho^{-1}}$. For $1\leqq i\leqq l-1$, choose k_i $(1\leqq k_i\leqq l-1))$ so that

$$\rho^{k_i}\equiv i \pmod{l}.$$

As $\varphi_i=\sigma^{-k_i}$, we have $\psi_i=\sigma^{k_i}$. Therefore we can rewrite (4) in the form

$$(\Pi^f)=\prod_{i=1}^{n}\mathfrak{p}^{\sigma^{k_i}}. \tag{4'}$$

For $1\leqq j\leqq g$, let ν_j be the number of i such that $1\leqq i\leqq n$ and $k_i\equiv j \pmod{g}$. Since the Galois group of K/K_0 is generated by σ^g, we have

$$(\Pi^f)=\prod_{j=1}^{g}\mathfrak{p}^{\nu_j\sigma^j}. \tag{4''}$$

2. First we shall treat the case where f is even. For $1\leqq j\leqq g$, let ν'_j be the number of i such that $n+1\leqq i\leqq l-1$ and $k_i\equiv j \pmod{g}$. As -1 is a power of $\rho^g \bmod l$ in this case, we have $k_{l-i}\equiv k_i \pmod{g}$. So we have $\nu'_j=\nu_j$. Considering that $\nu_j+\nu'_j=f$, we obtain

$$\nu_j=\frac{f}{2} \quad \text{for} \quad 1\leqq j\leqq g. \tag{7}$$

Therefore, if f is even, we have

$$\Pi^f=-p^{f/2}, \tag{8}$$

because (8) satisfies (3), (4''), (5) ,(6). The local invariants of the cyclic algebra $R=(-p^{f/2}, K, \tau)$ can be determined without difficulty. Let $\mathfrak{q}$ be a prime ideal of K_0 dividing neither p nor l. Then $\mathfrak{q}$ is unramified in K and Π^f is a $\mathfrak{q}$-unit. Therefore $\mathfrak{q}$ is unramified in R. Let $\mathfrak{l}$ be the prime divisor of l in K_0. Since Π^f is a local norm for K/K_0 at $\mathfrak{l}$ from (6), $\mathfrak{l}$ is also unramified in R. As for the prime divisors of p, we have

$$\left(\frac{R}{\mathfrak{p}^{\sigma^j}}\right)\equiv\frac{f}{2}\Big/f\equiv\frac{1}{2} \pmod{1} \quad \text{for} \quad 1\leqq j\leqq g.$$

Finally all the infinite places of K_0 are ramified in R, since K_0 is totally real. Denote by $D_{\infty,p}$ the quaternion algebra over $\boldsymbol{Q}$ whose ramified places are the infinite place and p. We have

$$R=M_{f/2}(D_{\infty,p}\otimes K_0), \tag{9}$$

because the both sides of (9) have the same local invariants. ($M_t(*)$ denotes the total matrix algebra of degree t.)

Theorem 1. *If f is even, the characteristic polynomial $P^{(f)}(X)$ of Π^f is given by*

$$P^{(f)}(X) = (X+p^{f/2})^{2n} \tag{10}$$

and $\boldsymbol{Q}(\Pi, Z)$ is the simple algebra $M_{f/2}(D_{\infty,\mathfrak{p}}\otimes K_0)$. Denoting by $\hat{J}$ the formal completion of J, we have

$$\hat{J}\sim nG_{1,1}\,. \tag{11}$$

The last assertion follows immediately from Theorem 4.1 of Manin [5].

It is easy to see that R coincides with $\mathcal{A}_0(J)$ in the case $g=1$. Is this true in other cases? In view of Tate's conjecture (8) of [7], it seems that J is isogenous to the direct product of n copies of an elliptic curve whose Hasse invariant is zero. Then we should have

$$\mathcal{A}_0(J) = M_n(D_{\infty,\mathfrak{p}})\,, \tag{12}$$

which would imply that $\mathcal{A}_0(J)$ is larger than R if $g>1$.

3. Now let us consider the case where f is odd. First we shall prove

Lemma. *If f is odd, we have $\boldsymbol{Q}(\Pi^{fs})=K_0$ for all $s\geqq 1$.*

Proof. As $\mathfrak{p}$ is unramified in K, it suffices to prove that (Π^f) is not an ideal of a proper subfield of K_0. Assume that

$$(\Pi^f)^{\sigma^a} = (\Pi^f)\,,$$

i.e.

$$\prod_{j=1}^{p}\mathfrak{p}^{v_{j^{\sigma^j+a}}} = \prod_{j=1}^{g}\mathfrak{p}^{v_{j^{\sigma^j}}}\,. \tag{13}$$

Put $\rho^a=b$ and let ξ be a character of order g modulo l. As (13) implies that $\{\xi(1),\cdots,\xi(n)\}=\{\xi(1\cdot b),\cdots,\xi(n\cdot b)\}$, we have

$$\sum_{i=1}^{n}\xi(i) = \sum_{i=1}^{n}\xi(i)\xi(b)$$

and so

$$(\xi(b)-1)\sum_{i=1}^{n}\xi(i) = 0\,.$$

Here it is classical that

$$\sum_{i=1}^{n}\xi(i) \neq 0\,. \tag{14}$$

Therefore we have $\xi(b)=1$, $a\equiv 0\,(\mathrm{mod}.\,g)$ and so $\sigma^a\in \mathrm{G}(K/K_0)$. This completes our proof.

Proof of (14). As f is odd, $\xi(-1)=-1$. Put

$$U=\sum_{i=1}^{n}\xi(i)\,,\qquad V=\sum_{i=1}^{l-1}\xi(i)i\,.$$

Since V appears in the first factor of the class number formula of K, it is not zero. We have on one hand

$$V=\sum_{i=1}^{n}\xi(i)i+\sum_{i=1}^{n}\xi(l-i)(l-i)$$

and hence

$$V=2\sum_{i=1}^{n}\xi(i)i-lU\,. \tag{15}$$

On the other hand, we have

$$V=\sum_{i=1}^{n}\xi(2i)2i+\sum_{i=1}^{n}\xi(l-2i)(l-2i)$$

and hence

$$V=4\xi(2)\sum_{i=1}^{n}\xi(i)i-l\xi(2)\,U\,. \tag{16}$$

By eliminating $\sum_{i=1}^{n}\xi(i)i$ from (15) and (16), we have

$$(2\xi(2)-1)\,V=-l\xi(2)\,U\,,$$

which implies $U\neq 0$.

From this Lemma, we can deduce that R coincides with $\mathcal{A}_0(J)$. By Proposition 3 of [6], Chap. II, $\mathcal{A}_0(J)$ is a simple algebra. Let L be its center. Because Π^{fs} belongs to L for some s, we have $[L:\boldsymbol{Q}]\geqq g$ by our Lemma. As a maximal subfield of $\mathcal{A}_0(J)$ is of degree $2n$ over $\boldsymbol{Q}$, we have $[\mathcal{A}_0(J):\boldsymbol{Q}]\leqq f^2g$, which implies that $\mathcal{A}_0(J)=R$.

Now we consider the local invariants of R when f is odd. As in the case f is even, all the ramified prime ideals of R divide p. Moreover no infinite place is ramified in R, because K_0 is totally imaginary. As for the prime divisors of p, we have from (4″)

$$\left(\frac{R}{\mathfrak{p}^{\sigma^j}}\right)\equiv\frac{\nu_j}{f}\qquad(\mathrm{mod.}\ 1)\,. \tag{17}$$

Theorem 2. *If f is odd, R coincides with $\mathcal{A}_0(J)$. It is a central simple algebra over K_0 in which only prime divisors of p are ramified. The local invariants of R are given by* (17). *The characteristic polynomial of Π^{fs} is the f-th power of an irreducible polynomial of degree g with coefficients in $\boldsymbol{Z}$ for every $s\geqq 1$. Let r be*

the G. C. M. of $\nu_1, \cdots, \nu_g$. *Then the index of* $\mathcal{A}_0(J)$ *is* f/r *and* J *is isogenous to the direct product of* r *copies of a simple abelian variety.*

The last assertions follow from the fact that the subfield of K of degree $(l-1)/r$ is a splitting field of R.

In the case f is odd, the invariants $\{\nu_1, \cdots, \nu_g\}$ determine also the formal structure of J by Theorem 4.1 of Manin [5]. For $0 \leqq k \leqq f$, let μ_k be the number of ν_j such that $\nu_j = k$. Put $r_0 = f\mu_0$ and put $c = k/f$ for $k \neq 0$. We have $r_c = f\mu_k$, $n_c = k\mu_k$ and $m_c = (f-k)\mu_k$ in the notation of Theorem 4.1 of [5]. As $G_{1,1}$ is not a component of $\hat{J}$ in this case, the formal structure of J is given by

$$\hat{J} \sim r_0 G_{1,0} + \sum_{0<k<f/2} (G_{n_c, m_c} + G_{m_c, n_c}) . \tag{18}$$

OSAKA UNIVERSITY

References

[1] H. Davenport and H. Hasse: *Die Nullstellen der Kongruenzzetafunktionen im gewissen zyklischen Fällen*, J. Reine Angew. Math. **172**(1935), 151–182.

[2] M. Deuring: Algebren, Berlin, 1935.

[3] J. Igusa: *Fibre systems of Jacobian varieties*, Amer. J. Math. **78**(1956), 171–199.

[4] S. Lang: Abelian varieties, New York, 1959.

[5] Yu. I. Manin: *The theory of commutative formal groups over fields of finite characteristic*, Uspehi Mat. Nauk. (Russian Math. Surveys), **18**(1963), No. 6, 3–90.

[6] G. Shimura and Y. Taniyama: Complex multiplication of abelian varieties and its applications to number theory, Tokyo, 1961.

[7] J. Tate: *Algebraic cohomology classes*, Lecture notes prepared in connection with the Summer Institute on Algebraic Geometry, Woods Hole, 1964.