Compositio Mathematica **107:** 339–353, 1997.

Hodge cycles on the jacobian variety of the Catalan curve

FUMIO HAZAMA
Department of Natural Sciences, College of Science and Engineering, Tokyo Denki University, Hatoyama, Hiki-gun, Saitama 350-03, Japan

Received 28 August 1995; accepted in final form 3 July 1996

Abstract. The jacobian variety of the Catalan curve $y^q = x^p - 1$ is shown to be nondegenerate. As an application, a 0-1-matrix whose determinant computes the relative class number of the pq-th cyclotomic field is constructed.

Mathematics Subject Classifications (1991): 14C30, 11R29.

Key words: Catalan curve, Hodge group, class number.

1. Introduction

In [4], Kubota showed that the jacobian variety of the hyperelliptic curve defined by $y^2 = x^p - 1$ with p an odd prime is nondegenerate,' namely the dimension of its Hodge group is as large as possible. The purpose of the present paper is to generalize this result and to show that the jacobian variety of 'the Catalan curve' $y^q = x^p - 1$ with p, q distinct odd primes is nondegenerate. Nondegeneracy of an abelian variety with abelian CM-field is known to be equivalent to non-vanishing of certain character sums attached to it. And Kubota's proof is based on a certain elementary but ingenious manipulation of those character sums arising from the CM-type of the hyperelliptic curve. For the Catalan curve, however, a similar argument does not seem to work well. Generally the problem to determine whether such character sums vanish or not is highly nontrivial, as is seen in [6], where certain examples of degenerate abelian varieties of CM-type having the cyclotomic field as their endomorphism algebra, are given. Therefore, even if we restrict our attention to such abelian varieties, we become aware that the nondegeneracy is a delicate property depending on the arithmetic of the underlying fields and their CM-types. In the present paper, we proceed to express the character sums directly as linear combinations of the values at $s = 1$ of certain L-series. For our computation we owe much to the article [1]. From the standpoint that the Catalan curve is a quotient of the Fermat curve of degree pq, one can identify the character sums in question as certain factors of the Hasse zeta function of the Fermat curve (see [11]). Therefore our method can be considered as giving a direct computation of these factors. Moreover, in view of the fact that the nondegeneracy of the jacobian variety of the hyperelliptic curve $y^2 = x^p - 1$ is one of the starting points of the 'inductive structure' of the Fermat varieties [8], our result may give another initial step which extends the scope of the method employed in [loc. cit.].

As an application of our computation, we obtain a class number formula for the pq-th cyclotomic field. It is expressed essentially as the determinant of a 0-1-matrix which is easily computed once we are given the prime numbers p, q. This result is considered as a natural generalization of the class number formula for the p-th cyclotomic field, given in our previous article [3]. In view of the fact that our previous formula plays a certain role in the study of this field (see [7], [9], [10]), we believe the present formula would give some insight in the investigation of the arithmetic of the pq-th cyclotomic field.

The plan of this paper is as follows. In Section 2, we compute the CM-type of the jacobian variety of the Catalan curve. In Section 3, we recall the definition of the Hodge group of an abelian variety, when it is of CM-type, and we state the main theorem of this paper. Section 4 is devoted to the proof of the theorem. And in Section 5, we give the class number formula mentioned above.

The author would like to thank the referee for his/her valuable suggestions and corrections.

2. CM-type of the Catalan curve

Let p, q be distinct odd prime numbers. Let C denote the nonsingular curve defined by $y^q = x^p - 1$. The genus $g = g(C)$ of C is given by the formula $g = (p-1)(q-1)/2$. For any positive integer n, let $\zeta = \exp(2\pi\sqrt{-1}/n)$. Let σ denote the automorphism of C defined by $\sigma(x, y) = (\zeta_p x, \zeta_q y)$. It defines an action of the group μ_{pq} of the pq-th roots of unity on C. By functoriality, it also defines an action of μ_{pq} on the jacobian variety $J(C)$ of C. Thus $J(C)$ is an abelian variety of CM-type with endomorphism algebra $\mathbf{Q}(\zeta_{pq})$. (Note that the degree of the extension is $\mathbf{Q}(\zeta_{pq}) : \mathbf{Q}] = (p-1)(q-1) = 2g$). In order to describe the CM-type of $J(C)$, we introduce some notation. Let $G = \mathrm{Gal}(\mathbf{Q}(\zeta_{pq})/\mathbf{Q})$ denote the Galois group of the extension $\mathbf{Q}(\zeta_{pq})/\mathbf{Q}$, which we identify with the product $(\mathbf{Z}/p\mathbf{Z})^* \times (\mathbf{Z}/q\mathbf{Z})^*$. With this identification, the CM-type of $J(C)$ is given as follows

PROPOSITION 2.1. *Notation being as above, the CM-type of $J(C)$ is given by the subset*

$$S = \{(qc \bmod p, -pd \bmod q) \in G; 1 \leqslant d \leqslant q-1, 1 \leqslant c < pd/q\}$$

of G.

Proof. In order to determine the CM-type of $J(C)$, it suffices to consider the induced action of the automorphism σ, on the vector space $\Omega^1(C)$ of differential forms of the first kind on C. One can check that a basis of $\Omega^1(C)$ is given by

$$x^a dx/y^b \quad \text{with} \quad 0 \leqslant a < p, 1 \leqslant b \leqslant q-1, pb - qa - q - 1 \geqslant 0.$$

Note that the condition for a, b is equivalent to the condition

$$1 \leqslant b \leqslant q-1, 1 \leqslant a+1 < pb/q.$$

The effect of the automorphism σ^* of $\Omega^1(C)$ on the above basis, is computed as follows

$$\sigma^*(x^a dx/y^b) = \zeta_{pq}^{q(a+1)-pb} x^a dx/y^b.$$

Considering the natural isomorphism $(\mathbf{Z}/pq\mathbf{Z})^* \cong (\mathbf{Z}/p\mathbf{Z})^* \times (\mathbf{Z}/q\mathbf{Z})^*$, and putting $c = a+1, d = b$, we obtain the assertion of the proposition.

3. The Hodge group of $J(C)$: main theorem

Let $\mathrm{Hg}(J(C))$ denote the Hodge group of $J(C)$ (see [2] for the definition and its basic properties). Since our $J(C)$ is an abelian variety of CM-type, its Hodge group is a $\mathbf{Q}$-torus and its dimension is equal to $\dim_{\mathbf{Q}} \mathbf{Q}[G].S$, where $\mathbf{Q}[G]$ denote the group ring of G over $\mathbf{Q}$ and the CM-type S is identified with the element $\Sigma_{s\in S} s$ of $\mathbf{Q}[G]$ (see [6]). It is known that, for any abelian variety A we have dim $\mathrm{Hg}(A) \leqslant A$, and that, if the equality holds, then the ring of Hodge classes on any power A^n is generated by its divisor classes (see [2]). We say an abelian variety A is *nondegenerate* if dim $\mathrm{Hg}(A) =$ dim A. Our purpose is to show the following

MAIN THEOREM. *The jacobian variety $J(C)$ of the Catalan curve $C: y^q = x^p - 1$ is nondegenerate. Hence, the ring of Hodge classes on any power $J(C)^n$ is generated by its divisor classes. In particular, the Hodge Conjecture holds for $J(C)^n$ for any $n \geqslant 1$.*

4. Proof of main theorem

For the computation of the dimension of the Hodge group, we use the following

PROPOSITION 4.1. ([6]). *Let A be an abelian variety of* CM-*type (K, T) with K an abelian number field and T a* CM-*type. Then* dim $\mathrm{Hg}(A) = \#\{\varphi : \varphi$ *an odd character of* $\mathrm{Gal}(K/\mathbf{Q})$ *such that* $\Sigma_{t\in T}\varphi(t) \neq 0\}$.

Let r_p (resp. r_q) denote a primitive root of $(\mathbf{Z}/p\mathbf{Z})^*$ (resp. $(\mathbf{Z}/q\mathbf{Z})^*$). For each i with $o \leqslant i \leqslant p-2$ (resp. each j with $0 \leqslant j \leqslant q-2$), let χ_i (resp. ψ_j) denote the character of $(\mathbf{Z}/p\mathbf{Z})^*$ (resp. $(\mathbf{Z}/q\mathbf{Z})^*$) defined by

$$\chi_i(r_p) = \zeta_{p-1}^i, \qquad \psi_j(r_q) = \zeta_{q-1}^j.$$

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

Then the set of odd characters of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_{pq})/\mathbf{Q})$ is equal to the set $\Phi = \{\chi_i\psi_j; i+j = \text{odd}\}$. Therefore our task is to compute the character sum $\Sigma_{s\in S}\varphi(s)$ for any $\varphi \in \Phi$. To compute this, we fix some notation. For a character $\varphi \in \Phi$, we denote by f_φ the conductor of φ, and by φ_f the associated primitive character. Let $G(\varphi)$ denote the Gauss sum

$$G(\varphi) = \sum_{i=1}^{f_\varphi - 1} \varphi_f(i)\zeta_{f_\varphi}^i.$$

For $\varphi \in \Phi$, we denote by $L(1, \varphi)$ the value at $s = 1$ of the L-function

$$L(s, \varphi) = \sum_{(n,pq)=1} \varphi(n)/n^s,$$

and we let

$$L_0(s, \varphi) = \sum_{(n,f_\varphi)=1} \varphi(n)/n^s.$$

When φ is nonprimitive, comparing Euler products we have

$$L(1, \varphi) = (1 - \varphi(q)/q)L_0(1, \varphi). \tag{1}$$

PROPOSITION 4.2. *Let $\varphi = \chi\psi$ be an element of Φ. For any d with $1 \leqslant d \leqslant (q-1)/2$, let $T_{q,d}(\chi) = \sum_{1\leqslant \ell < pd/q} \chi(\ell)$. If χ is nontrivial, then*

$$\sum_{s\in S} \varphi(s) = 2\chi(q)\psi(-p) \sum_{1\leqslant d\leqslant (q-1)/2} \psi(d)T_{q,d}(\chi). \tag{2}$$

Proof. It follows from Proposition 2.1 that

$$\begin{aligned}
\sum_{s\in S}(\chi\psi)(s) &= \sum_{1\leqslant d\leqslant q-1, 1\leqslant c<pd/q} \chi(qc)\psi(-pd) \\
&= \chi(q)\psi(-p) \sum_{1\leqslant d\leqslant q-1, 1\leqslant c<pd/q} \chi(c)\psi(d) \\
&= \chi(q)\psi(-p) \sum_{1\leqslant d\leqslant (q-1)/2} \\
&\qquad \left(\sum_{1\leqslant c<pd/q} \chi(c)\psi(d) + \sum_{1\leqslant c<p(q-d)/q} \chi(c)\psi(q-d) \right)
\end{aligned}$$

$$= \chi(q)\psi(-p) \sum_{1\leqslant d\leqslant (q-1)/2}$$

$$\left(\sum_{1\leqslant c<pd/q} \chi(c)\psi(d) - \sum_{1\leqslant c<p(q-d)/q} \chi(-c)\psi(d) \right)$$

(since $\chi\psi$ is odd)

$$= \chi(q)\psi(-p) \sum_{1\leqslant d\leqslant (q-1)/2}$$

$$\left(\sum_{1\leqslant c<pd/q} \chi(c)\psi(d) - \sum_{pd/q<c'\leqslant p-1} \chi(c')\psi(d) \right)$$

(we put $c' = p - c$)

$$= \chi(q)\psi(-p) \sum_{1\leqslant d\leqslant (q-1)/2}$$

$$\left(\sum_{1\leqslant c<pd/q} \chi(c)\psi(d) + \sum_{1\leqslant c'<pd/q} \chi(c')\psi(d) \right)$$

(since $\Sigma_{1\leqslant c'\leqslant p-1}\chi(c') = 0$ for χ nontrivial)

$$= \chi(q)\psi(-p) \sum_{1\leqslant d\leqslant (q-1)/2} \psi(d)T_{q,d}(\chi).$$

This completes the proof of Proposition 4.2.

Now we proceed to the proof of the Main Theorem. We divide it into two cases

(*Case* 1). χ is odd and ψ is even.
(*Case* 2). χ is even and ψ is odd.

(We will see below that (*Case* 2) is reduced to (*Case* 1) by a symmetry argument).

(*Case* 1). χ is odd and ψ is even.
The situations for ψ nontrivial and that for ψ trivial are somewhat different. We begin with the former case.

(*Case* 1.1). ψ is nontrivial.
We prove the following

PROPOSITION 4.3. *Notation being as above*

$$\sum_{a\in S} (\chi\psi)(s) = (\sqrt{-1}/\psi)G(\chi\psi)L(1, \overline{\chi\psi}).$$

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

In particular, the character sum $\Sigma_{s\in S}(\chi\psi)(s)$ *does not vanish.*

Proof. For convenience, we put $q_0 = (q-1)/2$. In this case we can put $\psi = \psi_{2k}$ for some k with $1 \leqslant k \leqslant q_0 - 1$. In order to compute $T_{q,d}(\chi)$ for $1 \leqslant d \leqslant q_0$, we introduce the following odd function $F_{q,d}(x)$, which is periodic with period 2π

$$F_{q,d}(x) = \begin{cases} 0 & -\pi \leqslant x < -2\pi d/q, \\ -1/2 & x = -2\pi d/q, \\ -1 & -2\pi d/q < x < 0, \\ 0 & x = 0, \\ 1 & 0 < x < 2\pi d/q, \\ 1/2 & x = 2\pi d/q, \\ 0 & 2\pi d/q < x \leqslant \pi. \end{cases}$$

One can compute its Fourier expansion as follows

$$F_{q,d}(x) = (-2/\pi) \sum_{1\leqslant m\leqslant q_0} (\cos(2\pi md/q) - 1) \sum_{n=m,-m(\bmod q)} (\sin nx)/n. \tag{3}$$

We recall the following lemma which is nothing other than the orthogonality relation of characters

LEMMA 4.3.1. *For any* $m.n \in (\mathbf{Z}/q\mathbf{Z})^*$,

$$\sum_{0\leqslant \ell\leqslant q_0-1} \overline{\psi_{2\ell}}(m)\psi_{2\ell}(n) = \begin{cases} q_0 & n = m, -m, \\ 0 & \textit{otherwise}. \end{cases}$$

Using this lemma and (3), we can express $F_{q,d}(x)$ as follows

$$\begin{aligned} F_{q,d}(x) &= (-2/(q_0\pi)) \sum_{1\leqslant m\leqslant q_0} (\cos(2\pi md/q) - 1) \\ &\quad \times \left(\sum_{n=1}^{\infty} \left(\sum_{0\leqslant \ell\leqslant q_0-1} \overline{\psi_{2\ell}}(m)\psi_{2\ell}(n)(\sin nx)/n\right)\right). \end{aligned} \tag{4}$$

For any positive integer n, let $G(n,\chi) = \sum_{1\leqslant j\leqslant p-1} \chi(j)\zeta_p^{nj}$, so that $G(\chi) = G(1,\chi)$. Since χ is odd, we have

$$\begin{aligned} G(n,\chi) &= \sum_{1\leqslant j\leqslant p_0} \chi(j)\zeta_p^{nj} - \sum_{1\leqslant j\leqslant p_0} \chi(j)\zeta_p^{-nj} \\ &= \sum_{1\leqslant j\leqslant p_0} \chi(j)\cdot 2\sqrt{-1}\,\sin(2\pi nj/p) \\ &= \sqrt{-1} \sum_{1\leqslant j\leqslant p-1} \chi(j)\,\sin(2\pi nj/p). \end{aligned} \tag{5}$$

Using (4) and (5), we compute as follows

$$\begin{aligned}
&(-2/(q_0\pi)) \sum_{1\leqslant m\leqslant q_0} (\cos(2\pi md/q) - 1) \sum_{0\leqslant \ell\leqslant q_0-1} \overline{\psi_{2\ell}}(m)\psi_{2\ell}(n)G(n,\chi)/n \\
&= (-2\sqrt{-1}/(q_0\pi)) \\
&\quad \times \sum_{1\leqslant m\leqslant q_0} (\cos(2\pi md/q) - 1) \sum_{n=1}^{\infty} \sum_{0\leqslant \ell\leqslant q_0-1} \overline{\psi_{2\ell}}(m)\psi_{2\ell}(n) \\
&\quad \times \left(\sum_{1\leqslant j\leqslant p-1} \chi(j)\ \sin n(2\pi j/p) \right) /n \qquad \text{(by (5))} \\
&= \sqrt{-1} \sum_{1\leqslant j\leqslant p-1} \chi(j) F_{q,d}(2\pi j/p) \qquad \text{(by (4))} \\
&= \sqrt{-1} \left(\sum_{1\leqslant j< pd/q} \chi(j) - \sum_{p-(pd/q)<j\leqslant p-1} \chi(j) \right) \\
&\quad \text{(by the definition of the function } F_{q,d}(x)\text{)} \\
&= 2\sqrt{-1}T_{q,d}(\chi). \qquad (6)
\end{aligned}$$

(The last equality follows from the definition of $T_{q,d}(\chi)$). Substituting the equality $G(n,\chi) = \bar{\chi}(n)G(\chi)$ in the most left side of (6), we obtain

$$\begin{aligned}
&2\sqrt{-1}T_{q,d}(\chi) \\
= [6pt] \quad &= (-2/(q_0\pi)) \sum_{1\leqslant m\leqslant q_0} (\cos(2\pi md/q) - 1) \\
&\quad \times \sum_{n=1}^{\infty} \sum_{0\leqslant \ell\leqslant q_0-1} \overline{\psi_{2\ell}}(m)\psi_{2\ell}(n)\bar{\chi}(n)G(\chi)/n \\
&= (-2G(\chi)/(q_0\pi)) \sum_{1\leqslant \ell\leqslant q_0-1} \\
&\quad \left\{ \sum_{1\leqslant m\leqslant q_0} \overline{\psi_{2\ell}}(m)(\cos(2\pi md/q) - 1)L(1,\bar{\chi}\psi_{2\ell}) \right\}. \qquad (7)
\end{aligned}$$

To compute the sum $\Sigma_{1\leqslant d\leqslant q_0}\psi_{2k}(d)T_{q,d}(\chi)$, which appears in (2), we need the following

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

LEMMA 4.3.2. *Fix an integer* k *with* $1 \leqslant k \leqslant q_0 - 1$. *Then for any* ℓ *with* $0 \leqslant \ell \leqslant q_o - 1$,

$$\sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) \sum_{1\leqslant m\leqslant q_0} \overline{\psi_{2\ell}}(m)(\cos(2\pi md/q) - 1)$$

$$= \begin{cases} q_0 G(\psi_{2\ell})/2 & \textit{if } \ell = q_0 - k, \\ 0 & \textit{otherwise}. \end{cases} \tag{8}$$

Proof of Lemma 4.3.2. The left-hand side of (8) is computed as follows

$$\sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) \sum_{1\leqslant m\leqslant q_0} \overline{\psi_{2\ell}}(m)(\cos(2\pi md/q) - 1)$$

$$= \sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) \sum_{1\leqslant m\leqslant q_0} \overline{\psi_{2\ell}}(m)(\zeta_q^{md} + \zeta_q^{-md})/2$$

$$- \sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) \sum_{1\leqslant m\leqslant q_0} \overline{\psi_{2\ell}}(m)$$

$$= 1/2 \sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) \sum_{1\leqslant m\leqslant q-1} \overline{\psi_{2\ell}}(m)\zeta_q^{md}$$

(since $\overline{\psi_{2\ell}}$ is even and $\sum_{1\leqslant d\leqslant q_0} \psi_{2\ell}(d) = 0$)

$$= 1/2 \sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) G(d, \overline{\psi_{2\ell}})$$

$$= G(\overline{\psi_{2\ell}})/2 \sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d)\psi_{2\ell}(d)$$

$$= \begin{cases} q_0 G(\psi_{2k})/2 & \textit{if } \ell = q_0 - k, \\ 0 & \text{otherwise}, \end{cases}$$

(by Lemma 4.3.1 and by the fact $\psi_{2(q_0-\ell)} = \overline{\psi_{2\ell}}$).

It follows from this lemma and (7) that

$$\sqrt{-1} \sum_{1\leqslant d\leqslant q_0} \psi_{2k}(d) T_{q,d}(\chi)$$

$$= (-G(\chi)/(q_0\pi)) \sum_{0\leqslant \ell\leqslant q_0-1}$$

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

$$\left(\sum_{1\leqslant d\leqslant q_0}\psi_{2k}(d)\sum_{1\leqslant m\leqslant q_0}\overline{\psi_{2\ell}}(m)(\cos(2\pi md/q)-1)\right)L(1,\bar{\chi}\psi_{2\ell})$$

$$= (-G(\chi)/(a_0\pi))(q_0G(\psi_{2k})/2)L(1,\overline{\chi\psi_{2k}})$$

$$= (-1/(2\pi))G(\chi)G(\psi_{2k})L(1,\overline{\chi\psi_{2k}}). \quad (9)$$

Hence, by Proposition 4.2, we have

$$\begin{aligned}\sum_{s\in S}\chi\psi(s) &= 2\chi(q)\psi(-p)\sum_{1\leqslant d\leqslant q_0}\psi(d)T_{q,d}(\chi)\\ &= 2\chi(q)\psi(-p)\cdot(\sqrt{-1}/(2\pi))\\ &\quad\times G(\chi)G(\psi)L(1,\overline{\chi\psi}) \qquad \text{(by (9))},\\ &= (\sqrt{-1}/\pi)\chi(q)\psi(-p)G(\chi)G(\psi)L(1,\overline{\chi\psi}).\end{aligned}$$

Since $G(\chi\psi) = \chi(q)\psi(p)G(\chi)G(\psi)$ as is easily checked, we have

$$\sum_{s\in S}\chi\psi(s) = (\sqrt{-1}/\pi)G(\chi\psi)L(1,\overline{\chi\psi}),$$

which is nonzero. This completes the proof of Proposition 4.3.

(*Case* 1.2). $\psi = \psi_0$, the trivial character of conductor q.
We prove the following

PROPOSITION 4.4. *Notation being as above,*

$$\sum_{s\in S}(\chi\psi_0)(s) = (\sqrt{-1}/\pi)\chi(q)(\chi(q)-q)G(\chi)l_0(1,\bar{\chi}\psi_0).$$

Proof. In this case, we need the following lemma instead of Lemma 4.3.2

LEMMA 4.4.1. *For any* ℓ *with* $0\leqslant\ell\leqslant q_0-1$,

$$\sum_{1\leqslant d\leqslant q_0}\sum_{1\leqslant m\leqslant q_0}\overline{\psi_{2\ell}}(m)(\cos(2\pi md/q)-1)$$

$$= \begin{cases} -q_0(q_0+\frac{1}{2}) & \textit{if } \ell = 0,\\ 0 & \textit{otherwise}.\end{cases}$$

Proof of Lemma 4.4.1. Note that

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

$$\sum_{1\leqslant d\leqslant q_0}\sum_{1\leqslant m\leqslant q_0}\overline{\psi_{2\ell}}(m) = q_0 \sum_{1\leqslant m\leqslant q_0}\overline{\psi_{2\ell}}(m)$$
$$= \begin{cases} q_0^2 & \textit{if } \ell = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Since $G(\psi_0) = -1$, the assertion follows from this and a similar computation to that in the proof of Lemma 4.3.2.

Therefore, by (7), we have

$$\sqrt{-1}\sum_{1\leqslant d\leqslant q_0} T_{q,d}(\chi)$$
$$= (-G(\chi)/(q_0\pi)) \sum_{0\leqslant \ell\leqslant q_0-1}$$
$$\left\{\sum_{1\leqslant d\leqslant q_0}\sum_{1\leqslant m\leqslant q_0}\overline{\psi_{2\ell}}(m)(\cos(2\pi md/q)-1)\right\} L(1,\bar\chi\psi_{2\ell})$$
$$= (-G(\chi)/(q_0\pi))(-q_0(q_0+\tfrac{1}{2}))L(1,\bar\chi\psi_0)$$
(by Lemma 4.4.1)
$$= (qG(\chi)/(2\pi))L(1,\bar\chi\psi_0). \tag{10}$$

Hence we can compute the character sum as follows:

$$\sum_{s\in S}(\chi\psi_0)(s) = 2\chi(q)\sum_{1\leqslant d\leqslant q_0} T_{q,d}(\chi) \qquad \text{(by Proposition 4.2)}$$
$$= (-\sqrt{-1}/\pi)q\chi(q)G(\chi)L(1,\bar\chi\psi_0) \qquad \text{(by (10))}$$
$$= (\sqrt{-1}/\pi)\chi(q)(\chi(q)-q)G(\chi)L_0(1,\bar\chi\psi_0).$$

(The last equality follows from (1)). This completes the proof of Proposition 4.4.

(*Case* 2). χ is even and ψ is odd
This case is reduced to (*Case* 1) because of the symmetry. More precisely, the Catalan curve $y^q = x^p - 1$ is isomorphic to the curve $C_{p,q}\colon x^p + y^q = 1$ over **Q**. Further, the transposition $(x, y) \to (y, x)$ of the coordinates gives an isomorphism of $C_{p,q}$ to $C_{q,p}$, and it transforms (*Case* 2) for $C_{p,q}$ to (*Case* 1) for $C_{q,p}$. Therefore we obtain the following

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

PROPOSITION 4.5. *Notation being as above, if χ is nontrivial, then*

$$\sum_{s\in S}(\chi\psi)(s) = (\sqrt{-1}/\pi)G(\chi\psi)L(1,\overline{\chi\psi}).$$

If $\chi = \chi_0$, the trivial character of conductor p, then

$$\sum_{s\in S}(\chi_0\psi)(s) = (\sqrt{-1}/\pi)\psi(p)(\psi(p) - p)G(\psi)L_0(1,\chi_0\bar{\psi}).$$

Therefore in both cases the character sums are nonzero.

Thus we complete the proof of Main Theorem.

REMARK. Without appealing to the symmetry, we can give another proof for (*Case* 2), by using an *even* step function instead of $F_{q,d}(x)$.

5. Class number of $\mathbf{Q}(\zeta_{pq})$

As an application of the results in the previous Section, we construct a (0,1) square matrix, whose determinant gives the relative class number of $\mathbf{Q}(\zeta_{pq})$. Throughout this Section we assume that $p > q$. Let us put

$$T = \{(c,d); 1 \leqslant d \leqslant q-1, 1 \leqslant c < pd/q\},$$

which is regarded as a subset of $G = (\mathbf{Z}/p\mathbf{Z})^* \times (\mathbf{Z}/q\mathbf{Z})^*$. Then the CM-type S of $J(C)$ is equal to $(q,-p)\cdot T$, hence T is also a CM-type of a certain abelian variety isomorphic to $J(C)$. Let $G' = (\mathbf{Z}/pq\mathbf{Z})^*$ and let $T' = \alpha^{-1}(T) \subset G'$ be the inverse image of T, under the natural isomorphism $\alpha\colon G' \to G$.

DEFINITION 5.1. *We denote by $H = (H_{a,b})_{a,b\in T'}$ the $g\times g$ matrix defined by the following*

$$H_{a,b} = \begin{cases} 1 & \text{if } ab \in T', \\ 0 & \text{if } ab \notin T'. \end{cases}$$

Our purpose is to prove the following

THEOREM 5.2. *For arbitrary distinct odd prime numbers p, q, let $f(p;q)$ denote the order of p in $\mathbf{F}_q^*$ and let $e(p;q) = (q-1)/f(p;q)$. Let us put*

$$A(p;q) = \begin{cases} (p^{f(p;q)/2}+1)^{e(p;q)} & \text{if } f(p;q) \text{ is even}, \\ (p^{f(p;q)}-1)^{e(p;q)/2} & \text{if } f(p;q) \text{ is odd}. \end{cases}$$

Let h^- denote the relative class number of $\mathbf{Q}(\zeta_{pq})$. Then

$$h^- = 2pq|\det H|/(A(p;q)A(q;p)).$$

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

Proof. First we need some elementary lemmas.

LEMMA 5.2.1. *Let* $M = (M_{a,b})_{a,b\in T'}$ *denote the* $g \times g$ *matrix defined by*

$$M_{a,b} = \begin{cases} 1 & \textit{if } ab \in T', \\ -1 & \textit{if } ab \notin T'. \end{cases}$$

Then $\det M = 2^{g-1} \det H$.

Proof of Lemma 5.2.1. First note that $1 \in T'$ under our assumption that $p > q$. Therefore the '1'-th column of M is equal to ${}^t(1, \ldots, 1)$. For each $b \in T' - \{1\}$, adding the '1'-th column of M to its 'b'-th column, we see that $\det M = 2^{g-1} \det H$.

LEMMA 5.2.2. *Let* S' *denote the subset* $\alpha^{-1}(S)$ *of* G' *corresponding to* S. *Let* $N = (N_{a,b})_{a,b\in S'}$ *denote the* $g \times g$ *matrix defined by*

$$N_{a,b} = \begin{cases} 1 & \textit{if } ab \in S', \\ -1 & \textit{if } ab \notin S'. \end{cases}$$

Then $|\det N| = |\det M|$.

Proof of Lemma 5.2.2. Let $\bar{M} = (\bar{M}_{a,b})_{a\in T', b\in G'}$ denote the $g \times 2g$ matrix defined by

$$\bar{M}_{a,b} = \begin{cases} 1 & \text{if } ab \in T', \\ -1 & \text{if } ab \notin T'. \end{cases}$$

For any $b \in G'$, let $\bar{M}_b$ denote the b-th column of the matrix $\bar{M}$. Then we have

$$\bar{M}_{-b} = (-1) \cdot \bar{M}_b. \tag{11}$$

Let $r = \alpha^{-1}(q, -p)$. Then it follows from the equality $S = (q, -p) \cdot T$ that $S' = r \cdot T'$. Let $c, d \in S$. Then there exist $a, b \in T'$ such that $c = ra, d = rb$, and we have

$$N_{c,d} = \bar{M}_{a,rb}, \tag{12}$$

for, by the definition of the matrix N,

$$N_{c,d} = \begin{cases} 1 & \text{if } rab \in T', \\ -1 & \text{if } rab \notin T'. \end{cases}$$

Since both T' and $r \cdot T'$ are CM-types, if we put $T' = \{t_1, \ldots, t_g\}$, then we have $r \cdot T' = \{\varepsilon_1 t_1, \ldots, \varepsilon_g t_g\}$, for some $\varepsilon_i \in \{\pm 1\} (1 \leqslant i \leqslant g)$. Hence it follows from (11) that

$$\det(\bar{M}_{a,rb})_{a,b\in T'} = \pm \det(\bar{M}_{a,b})_{a,b\in T'}. \tag{13}$$

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

By (12) and (13), we obtain the assertion of Lemma 5.2.2.

LEMMA 5.2.3. *Let* $\tilde{H} = (\tilde{H}_{a,b})_{a,b\in S'}$ *denote the* $g \times g$ *matrix defined by*

$$\tilde{H}_{a,b} = \begin{cases} 1 & ab^{-1} \in S', \\ -1 & ab^{-1} \notin S'. \end{cases}$$

Then $|\det \tilde{H}| = |\det N|$.

Proof of Lemma 5.2.3. A proof similar to that for Lemma 5.2.2 can be constructed, because $(S')^{-1}(= \{a^{-1}; a \in S'\})$ is also a CM-type.

LEMMA 5.2.4. $|\det \tilde{H}| = 2^{g-1}|\det H|$.

Proof of Lemma 5.2.4. Combine (5.2.1), (5.2.2), and (5.2.3).

LEMMA 5.2.5. *For any character* φ, *let* $\varphi(S)$ *denote the character sum* $\Sigma_{s\in S}\varphi(s)$. *Then* $\det \tilde{H} = \Pi_{\varphi:\text{odd}}\varphi(S)$, *where* φ *moves through the set of odd characters of the group* G.

Proof of Lemma 5.2.5. We prove this by generalizing the proof of [5, Chap. 3, Theorem 6.1]. Let F be the space of *odd functions* on G. Namely, we put

$$F = \{f; f \text{ is a } \mathbf{C}\text{-valued function on } G, \text{ and } f(-x) = -f(x) \text{ for any } x \in G\}.$$

It is a g-dimensional vector space, and has two natural bases

$$\{\varphi; \varphi \text{ is an odd character on } G\}, \text{ and } \{\delta_s; s \in S\},$$

where we put, for any $b \in G$,

$$\delta_b(x) = \begin{cases} 1 & \text{if } x = b, \\ -1 & \text{if } x = -b, \\ 0 & \text{otherwise.} \end{cases}$$

For each $a \in G$ let $T_a f$ be the function such that $T_a f(x) = f(ax)$. Then every odd character φ is an eigenvector of T_a with eigenvalue $\varphi(a)$. Let $T = \Sigma_{s\in S}T_s$. Then T is a linear map on F, and we have

$$T_\varphi = \varphi(S)\varphi.$$

Therefore φ is an eigenvector of T, and the determinant of T is the product of the character sums occurring on the right hand side of the equality in our lemma. On the other hand, we have

$$T\delta_b = \sum_{a\in S} T_a\delta_b = \sum_{a\in S} \delta_{a^{-1}b} = \sum_{c\in bS^{-1}} \delta_c,$$

hence, if we let $H' = (H'_{a,b})_{a,b\in S}$ denote the matrix of T w.r.t. the basis $\{\delta_s; s \in S\}$, then

$$H'_{a,b} = \begin{cases} 1 & \text{if } a \in bS^{-1}, \\ -1 & \text{if } a \notin bS^{-1}. \end{cases}$$

Noting that the condition $a \in bS^{-1}$ is equivalent to the condition $a^{-1}b \in S$, we see that H' is the transpose of $\tilde{H}$. This completes the proof of Lemma 5.2.5.

For any character φ of G', let denote B_φ denote the sum $\Sigma_{1\leqslant d\leqslant f_\varphi - 1}\varphi_f(d)d/f_\varphi$.

LEMMA 5.2.6 ([5, Chap. 3]). *For any odd character of* G',

$$L_0(1, \varphi) = (\sqrt{-1}\,\pi G(\varphi_f)/f_\varphi)B_{\bar{\varphi}}.$$

By this and the well-known fact that

$$|G(\varphi_f)| = \sqrt{f_\varphi}, \tag{14}$$

we have

$$|L_0(1, \varphi)| = (\pi/\sqrt{f_\varphi})|B_\varphi|. \tag{15}$$

It follows from (4.3), (4.4), and (4.5), that

$$\begin{aligned} \prod_{s\in S}\varphi(S) \;=\; & \prod_{\chi\psi\in\Phi,\text{nontrivial}} (\sqrt{-1}/\pi)G(\chi\psi)L(1, \overline{\chi}\psi) \\ & \times \prod_{\chi:\text{odd}} (\sqrt{-1}/\pi)\chi(q)(\chi(q) - q)G(\chi)L_0(1, \bar{\chi}\psi_0) \\ & \times \prod_{\psi:\text{odd}} (\sqrt{-1}/\pi)\psi(p)(\psi(p) - p)G(\psi)L_0(1, \chi_0\bar{\psi}). \end{aligned}$$

Therefore, by (14) and (15), we have

$$\left|\prod_{\varphi:\text{odd}}\varphi(S)\right| = \left|\prod_{\varphi:\text{odd}} B_\varphi\right| \cdot \left|\prod_{\chi:\text{odd}} (\chi(q) - q)\right| \cdot \left|\prod_{\psi:\text{odd}} (\psi(p) - p)\right|. \tag{16}$$

As for the products $\Pi_{\chi:\text{odd}}(\chi(q) - q)$ and $\Pi_{\psi:\text{odd}}(\psi(p) - p)$, we have the following

LEMMA 5.2.7. *Notation being as in Theorem* 5.2,

$$\prod_{\chi:\text{odd}} (\chi(q) - q) = A(q; p), \quad \textit{and} \quad \prod_{\psi:\text{odd}} (\psi(p) - p) = A(p; q).$$

https://doi.org/10.1023/A:1000106427229 Published online by Cambridge University Press

Proof of Lemma 5.2.7. A proof similar to that in [3] can be constructed.

Further, as for the product $\Pi_{\varphi:\text{odd}} B_\varphi$, we have the following

PROPOSITION 5.2.8 ([5, Chap. 3, Theorem 3.2]). *Let K denote an arbitrary abelian number field with $[K:\mathbf{Q}] = 2g$. Let Q denote the unit index, w the number of roots of unity in K, h^- the relative class number of K. Then*

$$\prod_{\varphi:\text{odd}} B_\varphi = (-2)^g h^-/(Qw).$$

When $K = \mathbf{Q}(\zeta_{pq})$, we have $Q = 2$ (see [loc. cit., Chap. 3, Theorem 4.1]) and $w = 2pq$. Hence we have

$$\prod_{\varphi:\text{odd}} B_\varphi = (-2)^g h^-/(4pq). \tag{17}$$

Combining (16), (17), and $(5.2.6)$, we have

$$\left|\prod_{\varphi:\text{odd}} \varphi(S)\right| = (2^g h^-/(4pq))A(p;q)A(q;p).$$

By $(5.2.4)$ and $(5.2.5)$, this implies that

$$h^- = 2pq|\det H|/(A(p;q)A(q;p)).$$

This completes the proof of Theorem 5.2.

References

1. Berndt, B. C.: Classical theorems on quadratic residues. *Enseignement Math.* 22 (1976) 261–304.
2. Hazama, F.: Algebraic cycles on certain abelian varieties and powers of special surfaces. *J. Fac. Sci. Univ. Tokyo* 31 (1985) 487–520.
3. Hazama, F.: Demjanenko matrix, class number, and Hodge group. *J. Number Theory* 34 (1990) 174–177.
4. Kubota, T.: On the field extension by complex multiplication. *Trans. AMS* 118 (1965) 113–122.
5. Lang, S.: 'Cyclotomic Fields', *Graduate Texts in Math.* 59, Springer-Verlag, New York, Heidelberg, Berlin, 1978.
6. Ribet, K.: Division fields of abelian varieties with complex multiplication. *Soc. Math. France Mémoire* 2 (1980) 75–94.
7. Schwarz, W.: Demjanenko matrix and 2-divisibility of class numbers. *Arch. Math.* 60 (1993) 154–156.
8. Shioda, T.: The Hodge Conjecture for Fermat varieties. *Math. Ann.* 245 (1979) 175–184.
9. Skula, L.: The Stickelberger ideal and the Demjanenko matrix. In: Hazama, F. (ed.) *Algebraic Cycles and Related Topics*, World Scientific, (1995) Singapore, pp. 69–76.
10. Skula, L.: On a special ideal contained in the Stickelberger ideal. *J. Number Theory* 58 (1996) 173–195.
11. Weil, A.: Jacobi sums as 'Grössencharaktere.' *Trans. Amer. Math. Soc.* 73 (1952) 487–495.