Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 119–135

Some Observations on Jacobi Sums

Tetsuji Shioda

Dedicated to Professor S. Iyanaga for his 80th birthday

In this paper, we shall be interested in the properties of the rational numbers $N(1-j(\alpha)q^{-n/2})$ which are the norm of the difference of 1 and $j(\alpha)q^{-n/2}$ (algebraic numbers of absolute value 1 in a cyclotomic field) where $j(\alpha)$ are the Jacobi sums defined below by (1.3), α being suitable $(n+2)$-tuples of integers modulo m. Typically, a formula of the form

$$N(1-j(\alpha)q^{-n/2})=(\text{square})(m\text{-power})/(q\text{-power})$$

seems to hold for m prime and n even, and we want to understand such a phenomenon in connection with arithmetic geometry of the Fermat varieties. The main result is Theorem 7.1 in Section 7 for the case $n=2$. The plan of the paper will be found at the end of Section 1.

Notation. Throughout the paper, the following notation will be used.
m: a fixed positive integer >2
$K=\boldsymbol{Q}(\zeta_m)$: the m-th cyclotomic field ($\zeta_m=e^{2\pi i/m}$)
n: a non-negative integer
$\mathfrak{A}_m^n$: the set of $(n+2)$-tuples $\alpha=(a_0, \cdots, a_{n+1})$ such that

$$a_i \in \boldsymbol{Z}/m, \quad a_i\neq 0, \quad \sum_{i=0}^{n+1} a_i=0$$

$\|\alpha\|=\sum_{i=0}^{n+1}\langle a_i/m\rangle-1$. ($\langle x\rangle$ is the fractional part of $x \in \boldsymbol{Q}/\boldsymbol{Z}$).
p: a prime number, $p\nmid m$.
$q=p^\nu$: a power of p such that $q\equiv 1 \pmod m$
$j(\alpha)$: the Jacobi sum (see § 1, (1.3))
$X_m^n(q)$: the Fermat variety $\sum_{i=0}^{n+1} x_i^m=0$ in $\boldsymbol{P}^{n+1}$ defined over $\boldsymbol{F}_q$.
$G_m^n=(\mu_m)^{n+1}/(\text{diagonal})$ regarded as a subgroup of $\mathrm{Aut}(X_m^n(q))$
$\hat{G}_m^n=$ the character group of G_m^n
$\quad=\{(a_0, \cdots, a_{n+1}) \mid a_i \in \boldsymbol{Z}/m, \sum_{i=0}^{n+1} a_i=0\}$
$0(\hat{G}_m^n)$: the set of $(\boldsymbol{Z}/m)^\times$-orbits in $\hat{G}_m^n$
$0(\mathfrak{A}_m^n)$: 〃 $\mathfrak{A}_m^n$

Received April 11, 1986.

$\mathfrak{B}^n_{m,q}$, $\mathfrak{B}^n_m(p)$, $\mathfrak{T}^n_{m,q}$, $\mathfrak{T}^n_m(p)$, $0(\mathfrak{T}^n_m(p))$, etc: see Section 5.
p_α, p_A: see Section 4

§ 1. The Jacobi sums

Fix a positive integer $m>2$ and let $K=\boldsymbol{Q}(\zeta_m)$ be the m-th cyclotomic field ($\zeta_m=e^{2\pi i/m}$). For any integer $n\geqq 0$, let

$$(1.1)\qquad \mathfrak{A}^n_m=\{(a_0,\cdots,a_{n+1})\,|\,a_i\in \boldsymbol{Z}/m,\ a_i\neq 0,\ \textstyle\sum_{i=0}^{n+1}a_i=0\}.$$

Take a finite field $\boldsymbol{F}_q$ with q elements such that

$$(1.2)\qquad q\equiv 1 \pmod m,$$

and choose a character $\chi\colon \boldsymbol{F}_q^\times\to K^\times\subset \boldsymbol{C}^\times$ of exact order m. For any $\alpha=(a_0,\cdots,a_{n+1})\in\mathfrak{A}^n_m$, the *Jacobi sum* $j(\alpha)$ (relative to $\boldsymbol{F}_q$ with chosen χ) is defined by

$$(1.3)\qquad j(\alpha)=(-1)^n\sum \chi(v_1)^{a_1}\cdots\chi(v_{n+1})^{a_{n+1}}$$

where the summation is taken over all $(n+1)$-tuples $(v_1,\cdots,v_{n+1})(v_i\in\boldsymbol{F}_q^\times)$ subject to the relation $v_1+\cdots+v_{n+1}=-1$.

This definition is the same as that of Weil [W1] except for the sign, and we refer to that paper for the basic properties of Jacobi sums. In particular, each $j(\alpha)$ is an algebraic integer in K of absolute value $q^{n/2}$:

$$(1.4)\qquad |j(\alpha)|=q^{n/2}$$

which depends symmetrically on $a_0, a_1,\cdots,a_{n+1}$ and which has the property that

$$(1.5)\qquad j(\alpha)^{\sigma_t}=j(t\cdot\alpha)\qquad (t\in(\boldsymbol{Z}/m)^\times).$$

Here σ_t is the automorphism of K over $\boldsymbol{Q}$ such that $\zeta^{\sigma_t}=\zeta^t$ and $t\cdot\alpha$ denotes $(ta_0,\cdots,ta_{n+1})\in\mathfrak{A}^n_m$. The latter determines an action of the group $(\boldsymbol{Z}/m)^\times$ on the set $\mathfrak{A}^n_m$. Let us write $A=[\alpha]$ for the $(\boldsymbol{Z}/m)^\times$-orbits of α, and $0(\mathfrak{A}^n_m)$ for the set of $(\boldsymbol{Z}/m)^\times$-orbits. If $\alpha=(a_i)$ and d is the g.c.d. of m and a_i's, then let $K_A=\boldsymbol{Q}(\zeta^d_m)$. For any $\alpha\in A$, $j(\alpha)$ belongs to K_A.

In this paper, we shall study the properties of the rational numbers

$$(1.6)\qquad N_{K_A/\boldsymbol{Q}}\left(1-\frac{j(\alpha)}{q^{n/2}}\right)=\prod_{\alpha\in A}\left(1-\frac{j(\alpha)}{q^{n/2}}\right)\qquad (A\in 0(\mathfrak{A}^n_m))$$

for n even, especially for $n=2$. To have some idea, let us write down the value of (1.6) for a few explicit examples in the case where

(1.7) $\qquad n=2, \quad m=\text{prime}>3, \quad q=p=\text{prime}\equiv 1 \pmod m$.

Example 1.1.

(a) $m=5$, $\alpha=(1112)$

$N(1-j(\alpha)/p)=m^3/p \qquad$ for $p=11, 31, 41$

(b) $m=7$, $\alpha=(1114)$, $\beta=(1123)$

$N(1-j(\alpha)/p)=m^3/p^2 \qquad$ for $p=29, 43, 71$

$N(1-j(\beta)/p)=m^3/p \qquad$ ″

(c) $m=11$.

α	$p=23$	$p=67$	$p=89$
(1118)	m^3/p^3	$23^2m^3/p^3$	$67^2m^3/p^3$
(1136)	$43^2m^3/p^3$	m^3/p^3	m^3/p^3
(1145)	m^3/p^2	m^3/p^2	m^3/p^2
(1127)	m^3/p^2	m^3/p^2	$23^2m^3/p^2$
(1235)	m^3/p	m^3/p	m^3/p

We are naturally led to the following

Question 1.2. *Under the condition* (1.7), *is it true that*

(1.8) $$N_{K/Q}(1-j(\alpha)/p)=(\textit{square})\cdot m^3/p^{w(\alpha)} \qquad (\alpha\in\mathfrak{A}_m^2)$$

for some $w(\alpha)$ depending only on α and independent of p with $p\equiv 1 \pmod m$? What is the meaning of such a formula, especially of the square factor? More generally, what can one say about the quantity (1.6) *without assuming the condition* (1.7)?

In the next two sections (§ 2, § 3) we deduce from the known properties of Jacobi sums the results concerning the "p-part" (for any m) and the "m-part" (for m prime) in a formula like (1.8). The remaining "square(?) part" will be considered in Section 6 after we recall some facts on Fermat varieties in Section 4 and Section 5. A partial answer to Question 1.2 will be given by Theorem 7.1 in Section 7.

§ 2. The denominator of $N(1-j(\alpha)q^{-n/2})$

Fix $m>2$, n even and p a prime number not dividing m. Let $H=\langle p \bmod m\rangle$ be the subgroup of $(Z/m)^\times$ generated by $p \bmod m$, and let f be the order of H. Write $q_0=p^f$.

Propoition 2.1. *For $\alpha\in\mathfrak{A}_m^n$, $A=[\alpha]$ and $q=q_0^r$, the Jacobi* sum $j(\alpha)$ *relative to F_q,* (1.3), *has the property that*

$$(2.1) \qquad N_{K_A/Q}\left(u-\frac{j(\alpha)}{q^{n/2}}\right) \in \frac{1}{q^w} Z \qquad (u \in Z)$$

where $w=w(A;p)$ *is a non-negative integer, defined below by* (2.8), *which depends only on* A *and* p.

Proof. We may assume that the coefficients a_i of α and m are relatively prime and so $K_A=K$. (If d is the g.c.d. of m and a_i's, then replace α by $\alpha'=(a_i/d)$ and m by $m'=m/d$.)

The proof is based on the Stickelberger's theorem on the prime decomposition of $j(\alpha)$ in $\mathfrak{o}=Z[\zeta_m]$, which we now recall (cf. Weil [W2]).

First we consider the case $q=q_0$. Take a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ over p and identify $\mathfrak{o}/\mathfrak{p}$ with F_q. Then, for a standard choice of the character χ in the definition of $j(\alpha)$ in (1.3), we have

$$(2.2) \qquad (j(\alpha))=\mathfrak{p}^{\omega(\alpha)}$$

for an element $\omega(\alpha)$ of the group ring $Z[\mathrm{Gal}(K/Q)]$:

$$(2.3) \qquad \omega(\alpha)=\sum_{t\in(Z/m)^\times} \|t\cdot\alpha\|\sigma_{-t}^{-1}$$

where, for any $\alpha=(a_i)\in\mathfrak{A}_m^n$, we set

$$(2.4) \qquad \|\alpha\|=\sum_{i=0}^{n+1}\left\langle\frac{a_i}{m}\right\rangle-1.$$

Taking a set of coset representatives $\{t_1, \cdots, t_g\}(g=\varphi(m)/f)$ of H in $(Z/m)^\times$, we set $\mathfrak{p}_\nu=\mathfrak{p}^{\tau_\nu}$ with $\tau_\nu=\sigma_{-t_\nu}^{-1}$. Then $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ are the primes in $\mathfrak{o}$ over p, and we have

$$(2.5) \qquad (p)=\mathfrak{p}_1\cdots\mathfrak{p}_g.$$

Further (2.2) can be rewritten as

$$(2.6) \qquad (j(\alpha))=\mathfrak{p}_1^{c_1}\cdots\mathfrak{p}_g^{c_g}, \qquad c_\nu=\sum_{h\in H}\|t_\nu h\alpha\|.$$

Thus $(j(\alpha)-uq^{n/2})$ $(u\in Z)$ is divisible by $\prod_\nu \mathfrak{p}_\nu^{\min(c_\nu,nf/2)}$, and hence $N_{K/Q}(j(\alpha)-uq^{n/2}))$ is divisible by $q^{\sum_\nu \min(c_\nu,nf/2)}$, i.e.

$$(2.7) \qquad q^{(n/2)\varphi(m)-\sum_\nu \min(c_\nu,nf/2)}N_{K/Q}\left(u-\frac{j(\alpha)}{q^{n/2}}\right)\in Z.$$

Define

(2.8)
$$w(A;p)=\frac{n}{2}\varphi(m)-\sum_{\nu=1}^{g}\min(c_\nu, nf/2)$$
$$=\sum_{\nu=1}^{g}\max(nf/2-c_\nu, 0)\geqq 0.$$

Then (2.1) holds with this definition of $w=w(A;p)$.

In the general case $q=q_0^r$, we have by the theorem of Davenport-Hasse (see [W1])

$$j(\alpha)-uq^{n/2}=j(\alpha)_0^r-uq_0^{rn/2},$$

where $j(\alpha)_0$ is the Jacobi sum relative to $\boldsymbol{F}_{q_0}$. Hence the same argument as above applies with the same $w=w(A;p)$. q.e.d.

The following special case is worth mentioning.

Corollary 2.2. *Assume p is a prime number satisfying $p\equiv 1 \pmod m$, and let $q=p^\nu$. Then, for any $\alpha\in\mathfrak{A}_m^n$, we have*

(2.9)
$$N_{K_A/Q}\left(1-\frac{j(\alpha)}{q^{n/2}}\right)\in\frac{1}{q^w}\boldsymbol{Z}\qquad(\alpha\in A)$$

where

(2.10)
$$w=w(A)=\sum_{\alpha\in A}\max\left(\frac{n}{2}-\|\alpha\|, 0\right).$$

In particular, in case $n=2$, we have

(2.11)
$$w(A)=\#\{\alpha\in A \mid \|\alpha\|=0\}.$$

The reader may check that, in Example 1.1, the power of p in the denominator of $N(1-j(\alpha)/p)$ is exactly the value of w given by (2.11).

§ 3. The m-part

Proposition 3.1. *Assume m is a prime number, $m>3$. For any prime power q such that $q\equiv 1 \pmod m$ and for $\alpha\in\mathfrak{A}_m^n$ (n=even), the Jacobi* sum *$j(\alpha)$ relative to $\boldsymbol{F}_q$ satisfies the congruence:*

(3.1)
$$N_{K/Q}(j(\alpha)-q^{n/2})\equiv 0 \qquad (\mathrm{mod}\ m^3).$$

Proof. This is an immediate consequence of a theorem of Iwasawa (see [Iw]), according to which one has

(3.2)
$$j(\alpha)\equiv 1 \qquad (\mathrm{mod}\ (1-\zeta_m)^3)$$

for any $\alpha \in \mathfrak{A}_m^n$, any n, provided that m is a prime number >3. q.e.d.

By making use of a recent result of Ihara generalizing Iwasawa's theorem ([Ih, II, § 6]), we also have

Proposition 3.2. *Suppose that m is a prime power such that $m=m_0^r$ with m_0 odd prime and $r>1$ if $m_0=3$. Then, for any $q\equiv 1 \pmod m$ and $\alpha \in \mathfrak{A}_m^n$ (n=even), we have*

$$N_{K/Q}(j(\alpha)-q^{n/2})\equiv 0 \pmod{m_0^3}. \tag{3.3}$$

Combining Proposition 3.1 with Corollary 2.2, we obtain a preliminary result about Question 1.2:

Corollary 3.3. *Assume m is a prime >3, $K=\boldsymbol{Q}(\zeta_m)$ the m-th cyclotomic field and n=even. Then for any $\alpha \in \mathfrak{A}_m^n$, there is a non-negative integer B such that*

$$N_{K/Q}\left(1-\frac{j(\alpha)}{q^{n/2}}\right)=\frac{Bm^3}{q^w} \tag{3.4}$$

where $q\equiv 1 \pmod m$ and w is defined by (2.8).

Thus Question 1.2 now becomes:

Question 3.4. *In the above situation, is the integer B a square for those $\alpha \in \mathfrak{A}_m^n$ with $j(\alpha)\neq q^{n/2}$?*

Example 3.5. Assume the condition (1.7): $n=2$, m=prime>3, $p\equiv 1 \pmod m$. Let $j(\alpha)$ be the Jacobi sum relative to $\boldsymbol{F}_p$. For any $\alpha \in \mathfrak{A}_m^2$ such that $j(\alpha)\neq p$ (cf. Theorem 7.1), we can write by (3.4)

$$N_{K/Q}\left(1-\frac{j(\alpha)}{p}\right)=\frac{Bm^3}{p^w}, \qquad N_{K/Q}\left(1+\frac{j(\alpha)}{p}\right)=\frac{C}{p^w} \tag{3.5}$$

for some positive integers B and C (the latter comes from the case $q=p^2$). D. Zagier has verified by computor that B, C are always *squares* for all such α in the case where

$$m<20 \quad \text{and} \quad p<500, \quad p\equiv 1 \pmod m.$$

To understand Question 3.4, at least in the case $n=2$, we turn to the geometric objects behind the Jacobi sums—the Fermat varieties.

§ 4. The Fermat motives

Given $m\geq 1$ and $n\geq 0$, let

$$X_m^n\colon x_0^m+x_1^m+\cdots+x_{n+1}^m=0 \tag{4.1}$$

be the Fermat variety of degree m and of dimension n in characteristic $p \geqq 0$. It is always assumed that $p \nmid m$. Letting μ_m be the group of m-th roots of unity, the group

$$G_m^n = (\mu_m)^{n+2}/(\text{diagonal}) \tag{4.2}$$

acts naturally on X_m^n. The character group $\hat{G}_m^n$ of G_m^n is identified with the set of $(n+2)$-tuples $(a_0, \cdots, a_{n+1})$ such that $a_i \in \boldsymbol{Z}/m$ and $\sum a_i = 0$. Hence the set $\mathfrak{A}_m^n$ (defined in § 1) is a subset of $\hat{G}_m^n$.

For any $\alpha \in \hat{G}_m^n$, let $A = [\alpha]$ be the $(\boldsymbol{Z}/m)^\times$-orbit of α and let $K_\alpha = K_A$ be defined as in Section 1. We define the following elements in the group ring $K[G_m^n]$ or $\boldsymbol{Z}[1/m][G_m^n]$:

$$p_\alpha = \frac{1}{m^{n+1}} \sum_{g \in G_m^n} \alpha(g)^{-1} g \tag{4.3}$$

$$p_A = \sum_{\alpha \in A} p_\alpha = \frac{1}{m^{n+1}} \sum_{g \in G_m^n} \mathrm{tr}_{K_\alpha/K}(\alpha(g)^{-1}) g. \tag{4.4}$$

It is easy to check that they satisfy

$$p_\alpha \cdot p_\beta = \begin{cases} p_\alpha & (\alpha = \beta) \\ 0 & (\alpha \neq \beta) \end{cases}, \quad \sum_{\alpha \in \hat{G}} p_\alpha = 1 \tag{4.5}$$

$$p_A \cdot p_B = \begin{cases} p_A & (A = B) \\ 0 & (A \neq B) \end{cases}, \quad \sum_{A \in 0(\hat{G})} p_A = 1. \tag{4.6}$$

Here $0(\hat{G})$ denotes the set of $(\boldsymbol{Z}/m)^\times$-orbits in $\hat{G} = \hat{G}_m^n$. By identifying each automorphism g of X_m^n with its graph, we can view p_A as an algebraic n-cycle on $X_m^n \times X_m^n$ with coefficients in $\boldsymbol{Z}[1/m]$. Since p_A is idempotent as a correspondence by (4.6), the pair

$$M_A = (X_m^n, p_A) \qquad (A \in 0(\hat{G}_m^n)) \tag{4.7}$$

defines a motive (cf. [D, II. § 6]), which may be called a *Fermat submotive* of X_m^n corresponding to the $(\boldsymbol{Z}/m)^\times$-orbit A in $\hat{G}_m^n$.

From now on, assume $p > 0$, and take a prime number l such that $l \nmid pm$. Letting $H^n(\bar{X}, \boldsymbol{Z}_l)$ be the l-adic cohomology group of $\bar{X} = X_m^n \otimes_{\boldsymbol{F}_p} \bar{\boldsymbol{F}}_p$, we define

$$H^n(M_A, \boldsymbol{Z}_l) = H^n(\bar{X}, \boldsymbol{Z}_l)^{p_A} \tag{4.8}$$

as the image of p_A (equivalently, the kernel of $p_A - 1$) acting on $H^n(\bar{X}, \boldsymbol{Z}_l)$; note that this makes sense since m is invertible in $\boldsymbol{Z}_l$. Then we have

$$H^n(\bar{X}, Z_l) = \bigoplus_{A \in O(\mathfrak{A}_m^n)} H^n(M_A, Z_l), \tag{4.9}$$

where $O(\mathfrak{A}_m^n)'$ is the set $O(\mathfrak{A}_m^n)$ of $(Z/m)^\times$-orbits in $\mathfrak{A}_m^n$ (n: odd) or the set $O(\mathfrak{A}_m^n \cup \{0\})$ (n: even). This follows from a similar decomposition of the Hodge structure of $H^n(X_m^n \otimes C, Q)$ into G_m^n-stable sub-Hodge structures (cf. [S2] or [S4]) via the comparison theorem of etale and classical cohomologies.

For any p-power q, let us write

$$X_m^n(q) = X_m^n \underset{F_p}{\otimes} F_q. \tag{4.10}$$

By Weil [W1], the zeta function of $X_m^n(q)$ is expressed in terms of the Jacobi sums (1.3). Assuming $q \equiv 1 \pmod m$, we have

$$\begin{cases} Z(X_m^n(q), T) = 1/\prod_{i=0}^{n} (1-q^i T) P(T)^{(-1)^n} \\ P(T) = \prod_{\alpha \in \mathfrak{A}_m^n} (1-j(\alpha)T). \end{cases} \tag{4.11}$$

If φ is the Frobenius endomorphism of $X_m^n(q)$, then the characteristic polynomial of the induced map φ^* on $H^n(\bar{X}, Q_l)$ is equal to $P(T)$ or $P(T) \times (1-q^{n/2}T)$ according to the parity of n. Now the action of φ^* is compatible with (4.9), tensored by Q_l, because φ commutes with each $g \in G_m^n$ (note that we are assuming $q \equiv 1 \pmod m$) so that we have

$$\varphi^* \cdot p_A = p_A \cdot \varphi^*. \tag{4.12}$$

If we set

$$R_A(T) = \det(1 - T\varphi^* \mid H^n(M_A, Q_l)) \qquad (A \in O(\mathfrak{A}_m^n)) \tag{4.13}$$

then

$$R_A(T) = \prod_{\alpha \in A} (1-j(\alpha)T) \tag{4.14}$$

(cf. [D, I. § 7]). The rational number (1.6) is nothing but the value of $R_A(T)$ at $T = q^{-n/2}$:

$$R_A(q^{-n/2}) = N_{K_A/Q}(1-j(\alpha)q^{-n/2}) \qquad (A \in O(\mathfrak{A}_m^n)). \tag{4.15}$$

§ 5. The Artin-Tate formula for Fermat surfaces

We keep the notation of the previous sections. For n even, we define the following subsets of $\mathfrak{A}_m^n$:

$$(5.1)\qquad \begin{cases} \mathfrak{B}^n_{m,q}=\{\alpha\in\mathfrak{A}^n_m \mid j(\alpha)=q^{n/2}\} \\ \mathfrak{B}^n_m(p)=\{\alpha\in\mathfrak{A}^n_m \mid j(\alpha)q^{-n/2} \text{ is a root of unity}\} \\ \mathfrak{T}^n_{m,q}=\mathfrak{A}^n_m-\mathfrak{B}^n_{m,q} \\ \mathfrak{T}^n_m(p)=\mathfrak{A}^n_m-\mathfrak{B}^n_m(p). \end{cases}$$

By (4.11), we see that

$$(5.2)\qquad 1+\#\mathfrak{B}^n_{m,q}=\text{the order of pole of } Z(X^n_m(q), T) \text{ at } T=q^{-n/2}.$$

The set $\mathfrak{B}^n_{m,q}$ is a subset of $\mathfrak{B}^n_m(p)$ which depends only on p but not on each p-power q. In fact, by Stickelberger's theorem (2.6), we have (with the notation there)

$$(5.3)\qquad \mathfrak{B}^n_m(p)=\{\alpha\in\mathfrak{A}^n_m \mid \sum_{h\in H}\|th\alpha\|=nf/2,\ \forall t\in(\boldsymbol{Z}/m)^\times\}.$$

For suitable choice of q, $\mathfrak{B}^n_{m,q}$ is equal to $\mathfrak{B}^n_m(p)$; this is always the case if q is replaced by q^{2m}.

The order of pole (5.2) is not smaller than the middle Picard number of $X^n_m(q)$ (i.e. the rank of cohomology classes of $\boldsymbol{F}_q$-rational algebraic cycles of middle dimension on X^n_m), and the two numbers will be equal if the Tate conjecture is true, which is known to hold for certain m, n, q (cf. [S1]).

From now on, we consider the case $n=2$. First we note:

Proposition 5.1. *The Tate conjecture holds for the Fermat surface $X^2_m(q)$ over $\boldsymbol{F}_q$, and the Picard number $\rho(X^2_m(q))$ (i.e. the rank of the Neron-Severi group $NS(X^2_m(q))$ is given by*

$$(5.4)\qquad \rho(X^2_m(q))=1+\#\mathfrak{B}^2_{m,q}.$$

Proof. By Tate [T2], the Tate conjecture holds for a product of curves over a finite field, and hence, in particular, for the product $Y=X^1_m\times X^1_m$ of the Fermat curve X^1_m over $\boldsymbol{F}_q$. On the other hand, there is a dominant rational map of Y to X^2_m as a special case of the inductive structure (cf. [K-S]). Hence the Tate conjecture holds for $X^2_m(q)$, and (5.4) follows from (5.2).

Now the zeta function (4.11) for $X=X^2_m(q)$ takes the form

$$1/(1-T)(1-qT)^\rho(1-q^2T)R(T)\qquad (\rho=\rho(X^2_m(q))$$

where

$$(5.5)\qquad R(T)=\prod_{\alpha\in\mathfrak{T}^2_{m,q}}(1-j(\alpha)T),\qquad R(q^{-1})\neq 0.$$

By the Artin-Tate formula (Tate [T1], Milne [Mi1]), the rational number $R(q^{-1})$ is related to other arithmetic or geometric invariants such as the Brauer group $\mathrm{Br}(X)$ and the Néron-Severi group $\mathrm{NS}(X)$. In the present case, we have

Proposition 5.2. *The notation being as above, the Artin-Tate formula for the Fermat surface $X=X_m^2(q)$ over $\boldsymbol{F}_q$ reads as follows:*

$$\prod_{\alpha\in\mathfrak{X}_{m,q}^2}\left(1-\frac{j(\alpha)}{q}\right)=\frac{|\mathrm{Br}(X)|\cdot|\det \mathrm{NS}(X)|}{q^{p_g(X)}} \tag{5.6}$$

where

$$p_g(X)=(m-1)(m-2)(m-3)/6. \tag{5.7}$$

Proof. Note that for X a nonsingular surface in $\boldsymbol{P}^3$ (i) the Néron-Severi group $\mathrm{NS}(X)$ is torsion-free, (ii) the Picard variety is trivial and (iii) the geometric genus is given by (5.7). Then we have only to apply the results of [T1] and [Mi1] in view of Proposition 5.1. q.e.d.

By (4.14) and (4.15), we have

Corollary 5.3. *For $X=X_m^2(q)$, the following formula holds.*

$$|\mathrm{Br}(X)|\cdot|\det \mathrm{NS}(X)|=q^{p_g(X)}\prod_{A\in O(\mathfrak{X}_{m,q}^2)}R_A(q^{-1}), \tag{5.8}$$

with

$$R_A(q^{-1})=N_{K_A/Q}\left(1-\frac{j(\alpha)}{q}\right) \qquad (\alpha\in A). \tag{5.9}$$

For any prime number $l\neq p$ and any rational number a $(a\neq 0)$, let $|a|_l$ denote the l-part of a, i.e. the power of l such that $a/|a|_l$ is an l-adic unit. From (5.8), we deduce

$$|\mathrm{Br}(X)|_l\cdot|\det \mathrm{NS}(X)|_l=\prod_{A\in O(\mathfrak{X}_{m,q}^2)}|R_A(q^{-1})|_l \qquad (l\neq p). \tag{5.10}$$

In the next section, we shall obtain a refined version of this formula which reflects the "motivic decomposition" of X and which will lead to a partial answer to the question 3.4 in case $n=2$.

Example 5.4. Under the condition (1.7), we have $\mathfrak{X}_{m,p}^2=\mathfrak{X}_m^2(p)$, and the α in Example 1.1 are the representatives of the set $O(\mathfrak{X}_m^2(p))$ up to permutation, for m, p given there. If we call V the value of the right hand side of (5.8) for $X=X_m^2(p)$, then $|\mathrm{Br}(X)|\cdot|\det \mathrm{NS}(X)|=V$ is computed by using Example 1.1:

(a) $m=5, p_g=4.\quad V=p^4(m^3/p)^4=m^{12}\quad$ for $p=11, 31, 41$

(b) $m=7, p_g=20.\quad V=p^{20}(m^3/p^2)^4(m^3/p)^{12}=m^{48}\quad$ for $p=29, 43, 71$

(c) $m=11, p_g=120.$

$V=p^{120}(m^3/p^3)^4(43^2m^3/p^3)^{12}(m^3/p^2)^{12}(m^3/p^2)^{12}(m^3/p)^{24}=43^{24}m^{192}\quad$ for $p=23$

$V=23^8m^{192}\quad$ for $p=67$

$V=67^8 23^{24}m^{192}\quad$ for $p=89$.

§ 6. The refined Artin-Tate formula

As before, let $X=X_m^2(q)$ be the Fermat surface of degree m over $\boldsymbol{F}_q$, $q\equiv 1 \pmod m$. Take a prime number l such that $l\nmid pm$. Let $\mathrm{Br}(X)(l)$ denote the l-primary part of $\mathrm{Br}(X)$, and let

$$\mathrm{Br}(M_A)(l)=\mathrm{Br}(X)(l)^{p_A} \tag{6.1}$$

be the image of p_A (equivalently the kernel of p_A-1), where p_A is the idempotent (4.4) corresponding to $A\in \mathrm{O}(\hat{G}_m^2)$. By (4.6), we have

$$\mathrm{Br}(X)(l)=\bigoplus_{A\in \mathrm{O}(\hat{G}_m^2)}\mathrm{Br}(M_A)(l). \tag{6.2}$$

Proposition 6.1. *The notation being as above, we have*:

$$|\mathrm{Br}(M_A)(l)|=|R_A(q^{-1})|_l \qquad \textit{if } A\in \mathrm{O}(\mathfrak{X}_m^2(p)) \tag{6.3}$$

$$|\mathrm{Br}(M_A)(l)|=1 \qquad \textit{if } A\in \mathrm{O}(\hat{G}_m^2-\mathfrak{X}_m^2(p)) \tag{6.4}$$

provided that $l\nmid pm$.

Proof. The idea is to modify the proof of the Artin-Tate formula in [T1] or [Mi1]. From the Kummer sequence on $\bar{X}$, we have the exact sequence

$$0\longrightarrow \mathrm{NS}(\bar{X})/l^\nu\mathrm{NS}(\bar{X})\longrightarrow H^2(\bar{X},\mu_{l^\nu})\longrightarrow \mathrm{Br}(\bar{X})_{l^\nu}\longrightarrow 0. \tag{6.5}$$

Taking the direct limit for $\nu\to\infty$, we get

$$0\longrightarrow \mathrm{NS}(\bar{X})\otimes\boldsymbol{Q}_l/\boldsymbol{Z}_l\longrightarrow H^2(\bar{X},\mu_{l^\infty})\longrightarrow \mathrm{Br}(\bar{X})(l)\longrightarrow 0.$$

For any $(\boldsymbol{Z}/m)^\times$-orbit A in $\hat{G}_m^2$, this gives the exact sequence

$$0\longrightarrow (\mathrm{NS}(\bar{X})\otimes\boldsymbol{Q}_l/\boldsymbol{Z}_l)^{p_A}\longrightarrow H^2(\bar{X},\mu_{l^\infty})^{p_A}\longrightarrow \mathrm{Br}(\bar{X})(l)^{p_A}\longrightarrow 0.$$

Further, if A is in $\mathfrak{T}^2_m(p)$, then the first term vanishes since p_A kills $\mathrm{NS}(\bar{X}) \otimes \boldsymbol{Q}_l$ so that we have

$$H^2(\bar{X}, \mu_{l^\infty})^{p_A} \simeq \mathrm{Br}(\bar{X})(l)^{p_A}.$$

Let $\Gamma = \mathrm{Gal}(\bar{\boldsymbol{F}}_q/\boldsymbol{F}_q)$, and take the Γ-invariants of both sides:

$$(6.6) \qquad (H^2(\bar{X}, \mu_{l^\infty})^{p_A})^\Gamma \simeq (\mathrm{Br}(\bar{X})(l)^{p_A})^\Gamma \qquad (A \in 0(\mathfrak{T}^2_m(p)).$$

Now observe that the actions of Γ and p_A commute. For if σ denotes the standard generator of Γ, σ commutes with the projectors p_A (any A) because σ is the inverse of the geometric Frobenius element φ^* (cf. [Mi2, p. 292]), and one has (4.12). Hence (6.6) can be rewritten as

$$(6.7) \qquad (H^2(\bar{X}, \mu_{l^\infty})^\Gamma)^{p_A} \simeq (\mathrm{Br}(\bar{X})(l)^\Gamma)^{p_A} \qquad (A \in 0(\mathfrak{T}^2_m(p))).$$

On the other hand, there is a commutative diagram (see [T1, (5.1)] or [Mi1, (3.2)]):

$$(6.8) \qquad \begin{array}{ccc} H^2(X, \mu_{l^\infty}) & \twoheadrightarrow & H^2(\bar{X}, \mu_{l^\infty})^\Gamma \\ \downarrow & & \downarrow \\ \mathrm{Br}(X)(l) & \longrightarrow & \mathrm{Br}(\bar{X})(l)^\Gamma \end{array}$$

with the arrow $\twoheadrightarrow$ being surjective. Considering the images under p_A of (6.8) and using (6.7), we deduce that

$$(6.9) \qquad \mathrm{Br}(X)(l)^{p_A} \twoheadrightarrow (\mathrm{Br}(\bar{X})(l)^{p_A})^\Gamma \qquad (A \in 0(\mathfrak{T}^2_m(p)).$$

Now we claim that

$$(6.10) \qquad |(\mathrm{Br}(\bar{X})(l)^{p_A})^\Gamma| = |R_A(q^{-1})|_l \qquad (A \in 0(\mathfrak{T}^2_m(p))).$$

To see this, we note first that $\mathrm{Br}(\bar{X})(l)$ is a divisible group, as follows from [G, (8.2)] in view of the fact that $\mathrm{NS}(\bar{X})$ is torsion-free. Thus its direct factor $\mathrm{Br}(\bar{X})(l)^{p_A}$ is also divisible and isomorphic to $(\boldsymbol{Q}_l/\boldsymbol{Z}_l)^r$ for some r. Then it is easy to see that the order of the kernel of $\sigma-1$ on $\mathrm{Br}(\bar{X})(l)^{p_A}$ is equal to the order of the cokernel of the map induced by $\sigma-1$ on the Tate module $T_l\,\mathrm{Br}(\bar{X})(l)^{p_A}$, which is isomorphic to $H^2(\bar{X}, \boldsymbol{Z}_l(1))^{p_A}$ for $A \in \mathfrak{T}^2_m(p)$ (use the projective limit of (6.5)). By the method of [T1, § 5], the order of the cokernel in question is equal to

$$|\det(\sigma-1 : H^2(\bar{X}, \boldsymbol{Z}_l(1))^{p_A})|_l = |R_A(q^{-1})|_l,$$

which proves (6.10).

It follows from (6.9) and (6.10) that the order of $\mathrm{Br}(X)(l)^{p_A}$ is divisible by $|R_A(q^{-1})|_l$. Now we rewrite the formula (5.10) using (6.2) as follows;

$$(6.11)\qquad \prod_{A\in 0(\mathfrak{T}_m^2(p))} \frac{|\mathrm{Br}(M_A)(l)|}{|R_A(q^{-1})|_l}\cdot \prod_{A\notin 0(\mathfrak{T}_m^2(p))} |\mathrm{Br}(M_A)(l)|\cdot|\det \mathrm{NS}(X)|_l = \prod_{A\in 0(\mathfrak{T}_{m,q}^2-\mathfrak{T}_m^2(p))} |R_A(q^{-1})|_l.$$

But the right side is 1, because, for $A\in 0(\mathfrak{T}_{m,q}^2-\mathfrak{T}_m^2(p))$, $j(\alpha)/q$ is a root of unity ($\neq 1$) in $K=\boldsymbol{Q}(\zeta_m)$ and we are assuming $l\nmid pm$. Therefore we conclude that

$$\begin{aligned} &|\mathrm{Br}(M_A)(l)|=|R_A(q^{-1})|_l && \text{if } A\in 0(\mathfrak{T}_m^2(p))\\ &|\mathrm{Br}(M_A)(l)|=1 && \text{if } A\in 0(\hat{G}_m^2-\mathfrak{T}_m^2(p))\\ &|\det \mathrm{NS}(X)|_l=1 \end{aligned}$$

which proves (6.3), (6.4) and also Corollary 6.3 below. q.e.d.

Proposition 6.2. *For any $\alpha\in\mathfrak{T}_m^2(p)$, a prime factor l of the numerator of $N_{K_A/\boldsymbol{Q}}(1-j(\alpha)/q)$ appears with an even power provided that $l\nmid 2pm$.*

Proof. By [T1], there is a nondegenerate skewsymmetric pairing on $\mathrm{Br}(X)(l)$ for X a surface over a finite field satisfying the Tate conjecture. In our case, it induces a nondegenerate pairing on the direct factor $\mathrm{Br}(M_A)(l)$ for each $A\in 0(\mathfrak{T}_m^2(p))$, and so the order of $\mathrm{Br}(M_A)(l)$ is a square if $l\neq 2$. It follows from Proposition 6.1 that $|R_A(q^{-1})|_l$ is a square if $l\neq 2$ and $l\nmid mp$. In view of (4.15) this proves the assertion.

Corollary 6.3. *The discriminant of the Néron-Severi group* $\mathrm{NS}(X)$ *of the Fermat surface of degree m over $\boldsymbol{F}_q$ ($q=p^\nu\equiv 1 \pmod m$) divides a power of pm.*

Remark 6.4. It is likely that if p is "ordinary" in the sense that $p\equiv 1 \pmod m$ then the discriminant of $\mathrm{NS}(\bar{X})$ divides a power of m. This is true if g.c.d. $(m, 2\cdot 3)=1$, which can be shown by using the results of [S3, §7]. On the other hand, if p is "supersingular" in the sense that $p^\nu\equiv -1 \pmod m$ for some ν, then the discriminant of $\mathrm{NS}(\bar{X})$ is a power of p; this follows from (5.15).

§ 7. Conclusion and open questions

Concerning our original question 1.2 (or 3.4), we can state our results in the following way.

Theorem 7.1. *Assume m is a prime number* >3, *and let* $K=\boldsymbol{Q}(\zeta_m)$ *be the m-th cyclotomic field. Let p be a prime number* >3 *such that* $p\equiv 1 \pmod m$ *and fix a p-power* $q=p^\nu$. *For any* $\alpha=(a_0, a_1, a_2, a_3)\in\mathfrak{A}_m^2$ (*i.e.* $a_i\in \boldsymbol{Z}/m$, $a_i\neq 0$, $a_0+\cdots+a_3=0$), *let* $j(\alpha)$ *be the Jacobi sum* (1.3) *relative to* $\boldsymbol{F}_q$. *Then the following three conditions are equivalent to each other*:

$$N_{K/Q}\left(1-\frac{j(\alpha)}{q}\right)\neq 0 \tag{7.1}$$

$$w(\alpha)=\#\left\{t\in(\boldsymbol{Z}/m)^\times \,\middle|\, \sum_{i=0}^{3}\left\langle\frac{ta_i}{m}\right\rangle=1\right\}>0 \tag{7.2}$$

$$a_i+a_j\neq 0 \qquad \textit{for } i\neq j. \tag{7.3}$$

When these conditions are satisfied, then

$$N_{K/Q}\left(1-\frac{j(\alpha)}{q}\right)=\frac{B\cdot m^3}{q^{w(\alpha)}} \tag{7.4}$$

with a positive integer B which is a square, possibly multiplied by a divisor of $2mp$.

Proof. Granting the first half, the second assertion follows from Corollary 2.2, Corollary 3.3 and Proposition 6.2.

The first part is a consequence of the known results as follows:

a) By definition (5.1) and Proposition 5.1, the condition (7.1) holds precisely when α belongs to $\mathfrak{T}_{m,q}^2$.

b) When $p\equiv 1(m)$, the set $\mathfrak{B}_m^n(p)$ defined by (5.1) equals the set $\mathfrak{B}_m^n$ of [S2] related to Hodge cycles on the complex Fermat variety $X_m^n(\boldsymbol{C})$ (n: even).

c) Suppose $n=2$ and g.c.d. $(m, 2\cdot 3)=1$. Then $\mathfrak{B}_m^2$ coincides with the set $\mathfrak{D}_m^2$ consisting of $\alpha=(a_i)$ with $a_i+a_j=0$ for some $i\neq j$ (see [S3, Th. 6]).

d) If $p\equiv 1(m)$ and g.c.d. $(m, 2.3)=1$, then the Néron-Severi group of $\bar{X}=X_m^2(p)\otimes\bar{\boldsymbol{F}}_p$ has generators of $\boldsymbol{F}_p$-rational cycles, because the lines defined over $\boldsymbol{F}_p$ span NS $(\bar{X})\otimes\boldsymbol{Q}$ (cf. [S3, Th. 7] where the complex case is treated; the proof is the same in this situation). Hence $\mathfrak{B}_{m,q}^2=\mathfrak{B}_m^2(p)$ for any p-power q.

Now (7.1), (7.2) or (7.3) respectively says that (1′) $\alpha\in\mathfrak{T}_{m,q}^2$, (2′) $\alpha\notin\mathfrak{B}_m^2$ or (3′) $\alpha\notin\mathfrak{D}_m^2$. Hence these conditions are equivalent in the case under consideration. q.e.d.

Letting $A=[\alpha]$ be the $(\boldsymbol{Z}/m)^\times$-orbit of α, and writing $B=B(A)$ and $w(\alpha)=w(A)$ in (7.4), we can rewrite the Artin-Tate formula (5.8) for $X=X_m^2(q)$ as follows:

(7.5) $$|\mathrm{Br}(X)|\cdot|\det \mathrm{NS}(X)|=\{\prod_{A\in O(\mathfrak{T}_m^2)} B(A)\}\, m^{3(m-3)^2}.$$

where $\mathfrak{T}_m^2=\mathfrak{A}_m^2-\mathfrak{B}_m^2$. It should be noted here that we have

(7.6) $$\sum_{A\in O(\mathfrak{T}_m^2)} w(A)=p_g(X) \qquad (\text{any } m)$$

by (2.11), and for m odd prime, we also have (cf. [S3])

(7.7) $$\begin{aligned}\#O(\mathfrak{T}_m^2)&=(\#\mathfrak{A}_m^2-\#\mathfrak{D}_m^2)/(m-1)\\&=(m-3)^2.\end{aligned}$$

On the other hand, we know that $\det \mathrm{NS}(X)$ is a power of m in our case, as mentioned in Remark 6.4. Hence it seems natural to ask the following

Question 7.2. *For the Fermat surface $X=X_m^2$ of prime degree m in characteristic $p\equiv 1$ (mod m), does one have*

(7.8) $$|\det \mathrm{NS}(X)|=m^{3(m-3)^2}\,?$$

or equivalently, with the notation of (7.4) *and* (7.5),

(7.9) $$|\mathrm{Br}(X)|=\prod_{A\in O(\mathfrak{T}_m^2)} B(A)\,?$$

In this paper, we have mainly considered the case $n=2$ of Question 1.2 about $N(1-j(\alpha)/q^{n/2})$ ($\alpha\in\mathfrak{A}_m^n$), but it seems likely that similar phenomena occur for higher n. Then, reversing the above argument, we may ask

Question 7.3. *Will this suggest the existence of some finite group with non-degenerate pairing for a higher dimensional variety (here X_m^n) which might play the role of the Brauer group for surfaces in a possible generalization of the Artin-Tate formula?*

Finally, it was in trying to compute the Néron-Severi groups of the *complex* Fermat surfaces that we came to notice the properties of Jacobi sums discussed in this paper. Concerning this, we formulate some related questions:

Question 7.4. *Are the following statements* (7.10), $\cdots$, (7.13) *true?*
(i) *For the complex Fermat surface X_m^2 of prime degree m ($m>2$):*

(7.10) $$|\det \mathrm{NS}(X_m^2)|=m^{3(m-3)^2}$$

(7.11) $\mathrm{NS}(X_m^2)$ *is spanned by the classes of lines on X_m^2.*

(ii) *Similarly, for the product* $X_m^1 \times X_m^1$ *of the complex Fermat curve with itself, with m prime* >3:

$$|\det \mathrm{NS}\,(X_m^1 \times X_m^1)| = m^{3r} \tag{7.12}$$

where $r = m^3 - 5m^2 + 2m + 17$.

(7.13) $\mathrm{NS}\,(X_m^1 \times X_m^1)$ *is spanned by the classes of the graphes* Γ_g *of the automorphisms* $g \in G_m^1$ (*see* (4.2)).

We know that (7.11) and (7.13) are true over $\boldsymbol{Q}$, and so the question is whether it is true over $\boldsymbol{Z}$ or not.

Acknowledgement. We would like to thank D. Zagier who showed interest in our observation and sent us the numerical data mentioned in Example 3.5 (March 1983) and T. Watanabe who supplied us further evidence for higher n. Also we thank K. Kato for helpful conversations on the subjects of Section 6.

Added in proof. (1) The first statement of the Remark 6.4 can be proven for any m, by making use of a result of P. Berthelot and A. Ogus "F-Isocrystals and De Rham Cohomology, I", Invent. Math. 72 (1983). Also the corresponding fact for the complex Fermat surfaces is true. Namely the discriminant of the Néron-Severi group of the complex Fermat surface of degree m divides a power of m for arbitrary m.

(2) The results of Section 6 have since been extended to the case $l=p$ by N. Suwa and N. Yui (in preparation).

References

[D] Deligne, P. et al, Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Math., **900**, Springer, Berlin-Heidelberg-New York (1982).

[G] Grothendieck, A., Le groupe de Brauer III, In: Dix Exposés sur la cohomologie des Schemas, North-Holland, Amsterdam, 88–188 (1968).

[Ih] Ihara, Y., Profinite braid groups, Galois representations and complex multiplications, Ann. of Math., **123** (1986), 43–106.

[Iw] Iwasawa, K., A note on Jacobi sums, Symposia Matematica, **15** (1975), 447–459.

[K-S] Katsura, T., Shioda, T., On Fermat varieties, Tohoku Math. J., **31** (1979), 97–115.

[Mi1] Milne, J. S., On a conjecture of Artin and Tate, Ann. of Math., **102** (1975), 517–533.

[Mi2] ——, Êtale Cohomology, Princeton Univ. Press, Princeton (1980).

[S1] Shioda, T., The Hodge conjecture and the Tate conjecture for Fermat varieties, Proc. Japan Academy, **55** (1979), 111–114.

[S2] ——, The Hodge conjecture for Fermat varieties, Math. Ann., **245** (1979), 175–184.

[S3] ——, On the Picard number of a Fermat surface, J. Fac. Sci. Univ. Tokyo, Sec. IA, **28** (1982), 725–734.

[S4] ——, Lectures on Fermat varieties, (in preparation).

[T1] Tate, J., On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Sém Bourbaki 1965/66, n° 306; In: Dix Exposés sur la Cohomologie des Schémas, North Holland, Amsterdam, 189–214 (1968).

[T2] ——, Endomorphisms of abelian varieties over finite fields, Invent. Math. **2** (1966), 134–144.

[W1] Weil, A., Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. **55** (1949), 497–508.

[W2] ——, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc. **73** (1952), 487–495.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo, Japan

Present Address:
Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo 171, Japan