COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 57, No. 1 2008

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

On Supersingular Cyclic Quotients of Fermat Curves

by

Noboru AOKI

(Received April 30, 2008)

1. Introduction

Let C be a projective smooth curve of genus g defined over $\mathbb{F}_q$, the finite field of q elements, where $q = p^f$ is a power of a prime number p. A. Weil proved that the zeta function of $C/\mathbb{F}_q$ has the form

$$Z(C/\mathbb{F}_q, t) = \frac{P(t)}{(1-t)(1-qt)},$$

where $P(t)$ is a polynomial with integral coefficients of degree $2g$ such that the constant term is 1 and the leading coefficient is q^g. Moreover he showed that if $\alpha_1, \ldots, \alpha_{2g}$ are the roots of $P(t)$ then $|\alpha_i| = q^{-1/2}$ (thus $|\alpha_i/\sqrt{q}| = 1$) for $i = 1, \ldots, 2g$. We say that C is *supersingular* if all the $\alpha_i/\sqrt{q}$ are roots of unity. This holds if and only if the zeta function of $C/\mathbb{F}_{q^n}$ over a suitable finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ has the form

$$Z(C/\mathbb{F}_{q^n}, t) = \frac{(1+q^{n/2}t)^{2g}}{(1-t)(1-q^n t)}.$$

Although it is usually hard to obtain the explicit form of the zeta function, there is a special class of curves whose zeta functions have been deeply studied. Let $m > 1$ be an integer not divisible by p and consider the Fermat curve of degree m

$$F_m : x^m + y^m + z^m = 0$$

defined over $\mathbb{F}_q$. It follows from the Davenport and Hasse relation ([12]) that the zeta function of F_m can be expressed using Jacobi sums. As a result, one can easily see that F_m is supersingular if and only if the following condition holds:

$$p^i \equiv -1 \pmod{m} \quad \text{for some } i \tag{1}$$

For each triple of integers $\alpha = (a, b, c)$ such that $0 < a, b, c < m$ and $a + b + c = m$, let F_α denote the projective model of the curve defined over $\mathbb{F}_p$ by the equation

$$v^m = (-1)^c u^a (1-u)^b.$$

As is well known, these curves are dominated by the Fermat curve F_m. Therefore, if F_m is supersingular, then so is F_α. However, the converse is not always true. Namely, even if (1) fails to hold, F_α can be supersingular.

Given m and α, it is not hard to determine whether F_α is supersingular or not because a combinatorial criteion for F_α to be supersingular is known (see Proposition 3.3). As an example, we begin with a sufficient condition for F_α to be supersingular. To state it, for an integer a, we denote by $\langle a\rangle_m$ the integer such that $0 \le \langle a\rangle_m < m$ and $\langle a\rangle_m \equiv a \pmod{m}$. For two triples $\alpha = (a, b, c)$ and $\alpha = (a', b', c')$, we write $\alpha \approx \alpha'$ if there is an integer such that $(m, t) = 1$ and $\{a', b', c'\} = \{\langle ta\rangle_m, \langle tb\rangle_m, \langle tc\rangle_m\}$.

THEOREM 1.1. *Suppose that f is even and one of the following conditions holds*:

(i) $4|m$, $p^{f/2} \equiv m/2+1 \pmod{m}$, *and* $\alpha \approx (1, \langle p^i\rangle_m, \langle -2p^j\rangle_m)$ *for some integers* i, j.

(ii) *There exist a divisor d of m and positive integers i, j such that*

$$p^i \equiv 1 \pmod{d}, \qquad p^j \equiv -1 \pmod{d},$$

and $\alpha \approx (1, \langle -p^j\rangle_m, \langle p^j - 1\rangle_m)$.

Then F_α is supersingular.

However, it is not so easy to determine the set of the pairs (m, α) for which F_α is supersingular. If $(a, b, c, m) = 1$, we say that α is *primitive*. In this paper we shall exhibit some examples of primitive elements α for which F_α is supersingular when condition (1) does not hold. Our results mainly concern the following two cases:

(i) m is a power of a prime number.

(ii) $m = 3l$ or $4l$, where l is a prime number greater than 3.

First, we consider the case where m is a power of a prime number l. If l is an odd prime number, then it is known that f must be even. Since $(\mathbb{Z}/m\mathbb{Z})^\times$ is a cyclic group, this implies that $p^{f/2} \equiv -1 \pmod{m}$. Therefore (1) holds. Thus the following theorem holds.

THEOREM 1.2. *Suppose that either $m = 4$ or $m = l^e$, where l is an odd prime number. Then F_α is supersingular if and only if condition* (1) *holds.*

In the case of $l = 2$ and $e > 2$, the situation is slightly complicated since in this case $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic.

THEOREM 1.3. *Let $m = 2^e$ $(e > 2)$ be a power of* 2. *Assume that $p^i \not\equiv -1$* $\pmod{m}$ *for any integer i and α is primitive. Then F_α is supersingular if and only if α is one of the following types.*

(i) $p^{f/2} \equiv m/2 + 1$ *and* $\alpha = (1, \langle p^i\rangle_m, \langle -2p^j\rangle_m)$ *for some integers* $i, j \ge 0$ *such that* $1 + p^i \equiv 2p^j \pmod{m}$.

(ii) $\alpha \approx (1, \langle -p^i\rangle_m, \langle p^i - 1\rangle_m)$ *for some integer* $i > 0$ *such that* $p^i \equiv 1 \pmod{f}$.

In the case of $m = 3l$ or $4l$ with $l > 3$ being a prime, we can determine when F_α is supersingular. To state the results, let

$$V_1(m) = \{x \in (\mathbb{Z}/m\mathbb{Z})^\times \mid x^2 = 1\}$$

be the 2-torsion group of $(\mathbb{Z}/m\mathbb{Z})^\times$. Then

$$V_1(m) = \begin{cases} \{\pm 1, \pm u\} & (m = 4l)\,, \\ \{\pm 1, \pm v\} & (m = 3l)\,, \end{cases}$$

where $u = m/2 - 1 = 2l - 1$ and v denotes the element of $(\mathbb{Z}/3l\mathbb{Z})^\times$ such that

$$v = \begin{cases} 1 & \pmod 3\,, \\ -1 & \pmod l\,. \end{cases}$$

Let H be the subgroup of $(\mathbb{Z}/l\mathbb{Z})^\times$ generated by the class of p, and let $\tilde{H}$ be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by the classes of -1 and p.

THEOREM 1.4. *Let $m = 3l$. Let $\alpha = (a, b, c)$ be a primitive element. Assume that $p^i \not\equiv -1 \pmod m$ for any integer i. Then F_α is supersingular if and only if one of the following conditions holds*:

(i) *If $p^{f/2} \equiv v \pmod m$, then one of the following assertions holds.*
   (1) *$p \equiv 1 \pmod 3$ and either $f = l - 1$ or $f = (l-1)/3$. Moreover, if $f = (l-1)/3$, then $a \equiv b \equiv c \pmod 3$ and $\{a, b, c\}$ is a complete set of representatives of $(\mathbb{Z}/l\mathbb{Z})^\times/H$.*
   (2) *$\alpha \approx (1, \langle -p^i\rangle_m, \langle p^i - 1\rangle_m)$, where i is an integer such that $p^i \equiv 1 \pmod 3$.*

(ii) *If $p^{f/2} \equiv v \pmod m$, then one of the following assertions holds.*
   (1) *$a \equiv b \equiv c \pmod 3$ and either*
      (a) *$3 \in H$ or*
      (b) *$\{a, b, c\}H$ is the subgroup of $(\mathbb{Z}/l\mathbb{Z})^\times$ of order $3f$ and $3 \in \langle a, H\rangle$.*
   (2) *$\alpha \approx (1, \langle v\rangle_m, \langle -v - 1\rangle_m)$.*

THEOREM 1.5. *Let $m = 4l$. Let $\alpha = (a, b, c)$ be a primitive element. Assume that $p^i \not\equiv -1 \pmod m$ for any integer i. Then F_α is supersingular if and only if one of the following conditions holds*:

(i) *If $p^{f/2} \equiv m/2 - 1 \pmod m$, then $p \equiv 1 \pmod 4$, $a \equiv b \pmod 4$ and one of the following assertions holds*:
   (1) *$f = l - 1$.*
   (2) *$f = (l-1)/2$, $l \equiv 1 \pmod 4$ and $\{a, b\}$ is a complete set of representatives of $(\mathbb{Z}/m\mathbb{Z})^\times/\tilde{H}$.*
   (3) *$\alpha \approx (1, \langle p^i\rangle_m, \langle -2p^i\rangle_m)$ for some integer i.*

(ii) *If $p^{f/2} \equiv m/2 + 1 \pmod m$, then either $2 \in H$ or $\alpha \approx (1, m/2 - 1, m/2)$.*

(iii) *Either $\alpha \approx (1, 3l - 1, l)$ or $(1, l - 1, 3l)$, and the following assertions hold*:
   (1) *If $2 \| a$, then $2 \in H$.*
   (2) *If $4 | a$, then $-2 \in H$.*

2. Cyclic quotients of F_m

In this section we recall some basic facts on the cyclic quotients of the Fermat curve F_m over a finite field. Let μ_m be the group of m-th roots of unity in the algebraic closure of $\mathbb{F}_p$, and put

$$G_m = (\mu_m \times \mu_m \times \mu_m)/\Delta\,,$$

where $\Delta = \{(\zeta, \zeta, \zeta) \mid \zeta \in \mu\}$ denotes the diagonal subgroup of $\mu_m \times \mu_m \times \mu_m$. We let G_m act on F_m by the following manner.

$$(x : y : z) \longmapsto (\zeta x : \eta y : \xi z) \qquad ((\zeta, \eta, \xi) \in G_m,\ (x : y : z) \in F_m)\,.$$

Then the group

$$\mathcal{Z}_m := \{(a, b, c) \in (\mathbb{Z}/m\mathbb{Z})^3 \mid a + b + c = 0\}$$

can be naturally regarded as the character group of G_m by putting

$$\alpha(g) = \zeta^a \eta^b \xi^c \in \mu_m \qquad (\alpha = (a, b, c) \in \mathcal{Z}_m,\ g = (\zeta, \eta, \xi) \in G_m)\,.$$

If α is primitive, then the homomorphism $\alpha : G_m \to \mu_m$ is surjective and $\mathrm{Ker}(\alpha)$ is a cyclic group of order m.

Now for each $\alpha \in \mathcal{Z}_m$, we define F_α to be the quotient curve $F_m/\mathrm{Ker}(\alpha)$. If $\alpha = (a, b, c) \in \mathcal{Z}_m$, $(a, b, c, m) = d$ and $a + b + c = m$, then F_α is the projective curve in $\mathbb{P}^3$ defined by

$$T^{m'} = X^{a'} Y^{b'} Z^{c'}, \quad X + Y + Z = 0\,,$$

where $m' = m/d$, $a' = a/d$, $b' = b/d$, $c' = c/d$, and the natural surjection $F_m \to F_\alpha$ is given by

$$(x, y, z) \longmapsto (X, Y, Z, T) = (x^{m'}, y^{m'}, z^{m'}, x^{a'} y^{b'} z^{c'})\,.$$

If we put $\alpha' = (a', b', c') \in \mathcal{Z}_{m'}$, then F_α is isomorphic to $F_{\alpha'}$. Therefore, we have only to focus on primitive elements. Moreover, if two elements α, α' of $\mathcal{Z}_m$ are identical after a permutation of the components, we write $\alpha \approx \alpha'$. It is then clear from the definition that F_α is isomorphic to $F_{\alpha'}$ whenever $\alpha \approx \alpha'$.

Let $\alpha \in \mathcal{Z}_m$ be a primitive element. Considering the affine plane $Z \neq 0$ in $\mathbb{P}^2$ and letting $u = -X/Z$, $v = -Y/Z$, we find that F_α is birational to the affine curve defined by

$$v^m = (-1)^c u^a (1 - u)^b\,.$$

Applying the Riemann-Hurwitz formula for the covering $F_\alpha \to \mathbb{P}^1$ associated to the rational function u on F_α, one can easily calculate the genus of F_α:

$$g(F_\alpha) = \frac{m - (m, a) - (m, b) - (m, c)}{2} + 1\,.$$

One of easy consequences of this formula is the following.

PROPOSITION 2.1. *The genus $g(F_\alpha)$ is positive if and only if none of a, b, c is zero.*

This naturally leads us to consider the subset of $\mathcal{Z}_m$ defined by

$$\mathfrak{A}_m := \{(a, b, c) \in \mathcal{Z}_m \mid a, b, c \neq 0\}\,.$$

In order to calculate the zeta function of F_m or F_α, we recall the definition of Jacobi sums. Fix a multiplicative complex valued character $\chi : \mathbb{F}_q^\times \to \mu_m(\mathbb{C})$ of order m. For $\alpha = (a, b, c) \in \mathcal{Z}_m$, we define the Jacobi sum J_α by

$$J_\alpha = J_\alpha(\chi) = \frac{1}{q - 1} \sum_{x+y+z=0} \chi(x)^a \chi(y)^b \chi(z)^c$$

where the sum is over the triples $(x, y, z) \in (\mathbb{F}_q^\times)^3$ satisfying $x+y+z=0$. It is clear from the definition that if $\alpha \approx \alpha'$, then $J_\alpha = J_{\alpha'}$.

We define an action of $\mathbb{Z}/m\mathbb{Z}$ on $\mathcal{Z}_m$: For $u \in \mathbb{Z}/m\mathbb{Z}$ and $\alpha = (a, b, c) \in \mathcal{Z}_m$, put

$$u \cdot \alpha = (ta, tb, tc) .$$

Clearly for $\alpha = (a, b, c) \in \mathfrak{A}_m$ we have $u \cdot \alpha \in \mathfrak{A}_m$ if and only if $ua, ub, uc \not\equiv 0 \pmod{m}$. Let

$$[\alpha] = \{u \cdot \alpha \mid u \in \mathbb{Z}/m\mathbb{Z},\ u \cdot \alpha \in \mathfrak{A}_m\} .$$

Then the cardinality of $[\alpha]$ is $m - (m, a) - (m, b) - (m, c) + 2$. Note that $\#[\alpha]$ equals $2g(F_\alpha)$.

THEOREM 2.2. *The zeta functions of $F_m/\mathbb{F}_q$ and $F_\alpha/\mathbb{F}_q$ are calculated as follows:*

(i) *Let $P(t) = Z(F_m/\mathbb{F}_q, t)(1-t)(1-qt)$. Then $P(t)$ is a polynomial given by*

$$P(t) = \prod_{\alpha \in \mathfrak{A}_m} (1 + J_\alpha t) .$$

(ii) *For $\alpha \in \mathfrak{A}_m$ with $a+b+c=m$, let $P_\alpha(t) = Z(F_\alpha/\mathbb{F}_q, t)(1-t)(1-qt)$. Then $P_\alpha(t)$ is a polynomial given by*

$$P_\alpha(t) = \prod_{\beta \in [\alpha]} (1 + J_\beta t) .$$

Jacobi sums satisfy the following properties.

PROPOSITION 2.3. *If $\alpha \in \mathfrak{A}_m$, then $|J_\alpha| = \sqrt{q}$.*

Proof. See [16]. □

We say that J_α is pure if J_α^k is real for some positive integer k. In other words, J_α is pure if and only if $J_\alpha = \varepsilon\sqrt{q}$ for some root of unity ε. Theorem 2.2 then shows that F_α is supersingular if and only if J_α is pure and that F_m is supersingular if and only if J_α is pure for all $\alpha \in \mathfrak{A}_m$.

PROPOSITION 2.4. *If $p^i \equiv -1 \pmod{m}$, then $J_\alpha = \pm\sqrt{q}$ and in particular it is pure.*

Proof. For $t \in (\mathbb{Z}/m\mathbb{Z})^\times$, we denote by σ_t the element of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ such that $\zeta_m^{\sigma_t} = \zeta_m^t$. Then $J_\alpha^{\sigma_t} = J_{t\cdot\alpha}$ for any $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $J_\alpha^{\sigma_p} = J_\alpha$. It follows that J_α belongs to $\mathbb{Q}(\zeta_m)^{\langle\sigma_p\rangle}$, the fixed subfield of the subgroup $\langle\sigma_p\rangle$ generated by σ_p. Therefore, if $p^i \equiv -1 \pmod{m}$, then $J_\alpha^{\sigma_{-1}} = J_\alpha$. Since σ_{-1} is the complex conjugate, this shows that J_α is real. But, since $|J_\alpha|^2 = q$, it follows that $J_\alpha = \pm\sqrt{q}$. □

Conversely, it is known that if J_α is pure for any $\alpha \in \mathfrak{A}_m$ then $p^i \equiv -1 \pmod{m}$ for some integer i. Therefore we obtain the following

COROLLARY 2.5. *F_m is supersingular if and only if Condition* (1) *holds.*

3. Preliminaries

In this section we define a commutative ring R_m and submodules A_m, B_m, D_m of R_m.

First, we define R_m to be the free abelian group over $\mathbb{Z}/m\mathbb{Z}\setminus\{0\}$. We write an element of R_m as

$$\alpha = \sum_{a\in\mathbb{Z}/m\mathbb{Z}\setminus\{0\}} c_a(a) \qquad (c_a \in \mathbb{Z})\,.$$

For simplicity we write $(a_1, \cdots, a_r)$ for $\sum_{i=1}^{r}(a_i)$. Next, for $a, b \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$, define the product of (a), $(b) \in R_m$ by the rule

$$(a)(b) = \begin{cases} (ab) & \text{if } ab \neq 0\,, \\ 0 & \text{if } ab = 0\,. \end{cases}$$

Extending linearly this product, we define the ring structure on R_m. Let

$$A_m = \left\{ \sum_a c_a(a) \in R_m \;\middle|\; \sum_a c_a a = 0 \right\}.$$

For any $a \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$, let $\langle\frac{a}{m}\rangle$ denote the rational number such that $0 < \left\langle\frac{a}{m}\right\rangle < 1$ and $m\left\langle\frac{a}{m}\right\rangle \equiv a \pmod m$. Let B_m be the submodule of R_m generated by elements $(a_1, \cdots, a_r) \in R_m$ such that

$$\sum_{i=1}^{r}\left\langle\frac{ta_i}{m}\right\rangle = \frac{r}{2} \quad (\forall t \in (\mathbb{Z}/m\mathbb{Z})^{\times})\,.$$

We define D_m to be the $\mathbb{Z}/m\mathbb{Z}$-submodule of R_m generated by $(1, -1)$. Thus, D_m consists of elements of R_m of the form

$$(a_1, -a_1, \cdots, a_r, -a_r) \qquad (r \in \mathbb{N})\,.$$

It is then easy to see that D_m is contained in B_m. Indeed this follows from the relation

$$\left\langle\frac{a}{m}\right\rangle + \left\langle\frac{-a}{m}\right\rangle = 1 \quad (a \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\})\,.$$

Let $\nu_p = (1, p, \cdots, p^{f-1}) \in R_m$. The following two subsets of R_m will be fundamental in the study of purity problem of Jacobi sums.

$$B_m(p) = \{\alpha \in R_m \mid \nu_p\alpha \in B_m\}\,.$$

Thus an element $(a_1, \cdots, a_r)$ of R_m belongs to $B_m(p)$ if and only if

$$\sum_{i=1}^{r}\sum_{j=0}^{f-1}\left\langle\frac{tp^j a_i}{m}\right\rangle = \frac{rf}{2} \quad (\forall t \in (\mathbb{Z}/m\mathbb{Z})^{\times})\,. \tag{2}$$

In order to investigate the structure we define a map $\tau_d : R_m \to R_{m/d}$ for each divisor $d|m$.

$$\tau_d(a) = \begin{cases} \dfrac{\varphi(m)}{\varphi(m')} \left(\displaystyle\prod_{\substack{l|d/(m,a) \\ p\nmid m/d}} (1, -l^{-1}) \right) (a') & (\text{if } (m,a)|d)\,, \\ 0 & (\text{if } (m,a) \nmid d)\,, \end{cases}$$

where $m' = m/(m,a),\ a' = a/(m,a)$.

Let $C(m)$ be the character group of $(\mathbb{Z}/m\mathbb{Z})\times$ and let $C^-(m)$ be the set of $\chi \in C(m)$ such that $\chi(-1) = -1$. Then the following proposition characterize the set B_m in terms of characters in $C^-(m)$. If $\chi \in C(m)$ and $\alpha = \sum c_a(a) \in R_m$, we put

$$\chi(\alpha) = \sum c_a \chi(a)\,.$$

Let $PC^-(m)$ be the set of primitive odd characters of $(\mathbb{Z}/\mathbb{Z})^\times$.

PROPOSITION 3.1. *For $\alpha \in R_m$, we have $\alpha \in B_m$ if and only if $\chi(\tau_d(\alpha)) = 0$ for any $\chi \in PC^-(m/d)$ and for any $d|m$.*

If l is a prime divisor of m and $la \not\equiv 0 \pmod m$, we define the standard element element $\sigma_{l,a}$ by

$$\sigma_{l,a} = \begin{cases} \left(a,\ a + \dfrac{m}{d},\ a + \dfrac{2m}{d},\ \ldots,\ a + \dfrac{(l-1)m}{l}, -la\right) & (l > 2)\,, \\ \left(a,\ a + \dfrac{m}{2},\ -2a,\ \dfrac{m}{2}\right) & (l = 2)\,. \end{cases}$$

If $4a \not\equiv 0 \pmod m$, we put

$$\sigma'_{2,a} = \left(a,\ a + \frac{m}{2}\,,\ 2a + \frac{m}{2}\,,\ -4a\right).$$

Moreover, for $\mathbf{x} = (x_1, \ldots, x_r) \in R_m$, we put

$$\sigma_{l,\mathbf{x}} = \sum_{i=1}^{r} \sigma_{l,x_i}\,, \qquad \sigma'_{2,\mathbf{x}} = \sum_{i=1}^{r} \sigma'_{2,x_i}\,.$$

PROPOSITION 3.2. *If $la \not\equiv 0 \pmod m$, then $\sigma_{l,a} \in B_m$. Moreover, if $4a \not\equiv 0 \pmod m$, then $\sigma'_{2,a} \in B_m$.*

Proof. See [2]. □

PROPOSITION 3.3. *Let $\alpha = (a,b,c)$ be a primitive element. Then the Jacobi sum J_α is pure if and only if $\alpha \in B_m(p)$, that is, $\nu_p\alpha \in B_m$.*

Proof. See [16]. □

Let

$$U(m) = \{t \in (\mathbb{Z}/m\mathbb{Z})^\times \mid \chi(t) = 1\ (\forall \chi \in PC^-(m))\}\,.$$

If $4|m$, we put $u = m/2 - 1$ and if $\mathrm{ord}_3(m) = 1$, we denote by v the element of $(\mathbb{Z}/m\mathbb{Z})^\times$ such that

$$v \equiv \begin{cases} 1 \pmod 3 \\ -1 \pmod{m/3}\,. \end{cases}$$

Then for an integer m with $\mathrm{ord}_2(m) \neq 1$ we have

$$U(m) = \begin{cases} \{1\} & \text{if } 4 \nmid m \text{ and } \mathrm{ord}_3(m) \neq 1\,, \\ \{1, u\} & \text{if } 4|m \text{ and } \mathrm{ord}_3(m) \neq 1\,, \\ \{1, v\} & \text{if } 4 \nmid m \text{ and } \mathrm{ord}_3(m) = 1\,, \\ \{1, uv\} & \text{if } 4|m \text{ and } \mathrm{ord}_3(m) = 1\,. \end{cases}$$

From the relation (2) one can easily see that if J_α is pure then f must be even. As for the simplest case $f = 2$, the following theorem is proved in [5, Theorem 3.5].

THEOREM 3.4. *Suppose* $f = 2$, $p \not\equiv -1 \pmod m$ *and*

$$m \notin \{12, 15, 20, 21, 24, 30, 39, 40, 42, 48, 60, 66, 78, 84, 120\}\,.$$

For a primitive element α, *the Jacobi sum* J_α *is pure if and only if one of the following conditions holds*:

(i) $\alpha \sim (1, w, -(1+w))$ *and* $p \equiv -w \pmod m$, *where* $w^2 \equiv 1, w \not\equiv \pm 1 \pmod m$ *and*, *in addition*, $w \not\equiv \frac{m}{2} + 1 \pmod m$ *if* $8|m$.

(ii) $4|m$ *and* $\alpha \sim (1, 1, -2)$ *and* $p \equiv \frac{m}{2} + 1 \pmod m$.

(iii) $16|m$ *and* $\alpha \sim (1, \frac{m}{2} + 1, \frac{m}{2} - 2)$ *and* $p \equiv \frac{m}{2} - 1 \pmod m$.

(iii′) $8\|m$ *and* $\alpha \sim (1, \frac{m}{2} + 1, \frac{m}{2} - 2)$ *and* $p \equiv \frac{m}{4} + 1, \frac{m}{2} - 1, \frac{3m}{4} + 1 \pmod m$.

In these four cases, *we have*

$$J_\alpha = \begin{cases} \pm p & \textit{in the case of } \text{(i) \textit{and} (iii)}\,, \\ \pm \chi(2)^{-a} p & \textit{in the case of } \text{(ii)}\,, \\ \pm \chi(2)^{\frac{m}{4} - 2a} p & \textit{in the case of } \text{(iii')}\,. \end{cases}$$

4. Proofs of Theorem 1.1 and Theorem 1.3

In this section we prove Theorem 1.1 and Theorem 1.3.

THEOREM 4.1. *Suppose that* f *is even and one of the following conditions holds*:

(i) $4|m$, $p^{f/2} \equiv m/2 + 1 \pmod m$, *and* $\alpha = (1, p^i, -2p^j)$ *for some integers* i, j.

(ii) *There exist a divisor* d *of* m *and positive integers* i, j *such that*

$$p^i \equiv 1 \pmod d, \qquad p^j \equiv -1 \pmod{m/d},$$

and $\alpha = (1, -p^j, p^j - 1)$.

Then F_α *is supersingular.*

Proof. (i) In this case, we have

$$\nu_p \alpha = \nu_p(1, 1, -2)\,.$$

Since $p^{f/2} \equiv m/2+1 \pmod{m}$, it follows that

$$\begin{aligned}(1,1,-2)\nu_p &= (1, m/2+1, m/2-2)\nu_p \\ &= (1, m/2+1, m/2-2)(1, m/2+1)\nu'_p \\ &= 2(1, m/2+1, -2, m/2)\nu'_p - 2(m/2, m/2)\nu'_p \in B_m\,.\end{aligned}$$

Therefore $\alpha \in B_m(p)$.

(ii) In this case, we have

$$(1, -p^i, p^i - 1)\nu_p = (1, -1)\nu_p + (p^i - 1)\nu_p\,.$$

Since $p^i - 1 \equiv 0 \pmod{d}$ and $p^j \equiv -1 \pmod{m/d}$, we see that $(p^i - 1)\nu_p \in D_m$. Therefore $\alpha \in D_m(p)$. This completes the proof. □

THEOREM 4.2. *Let $m = 2^e$ $(e > 1)$ be a power of 2 and suppose that α is primitive. Then F_α is supersingular if and only if α is one of the following types.*

(i) $\alpha = (1, p^i, -2p^j)$ *for some integers $i, j \geq 0$ such that* $1 + p^i \equiv 2p^j \pmod{m}$.

(ii) $\alpha = (1, -p^i, p^i - 1)$ *for some integer $i > 0$ such that* $p^i \equiv 1 \pmod{f}$.

Proof. Since the assertion is true for $m = 4$, we assume that $m > 4$. For simplicity suppose that $\alpha = (1, a, b)$ with $(m, a) = 1$ and $(m, b) > 1$. Note that f is even and $p^{f/2} \not\equiv -1 \pmod{m}$. Hence $p^{f/2} \equiv m/2 + 1$ or $m/2 - 1 \pmod{m}$.

Case 1. First, suppose that $p^{f/2} \equiv m/2 - 1 \pmod{m}$. Then $p^{f/2} \equiv -1 \pmod{4}$. If $f > 2$, then $f/2$ is even and $p^{f/2} \equiv 1 \pmod{4}$, which is a contradiction. Thus $f = 2$ and so $p \equiv -1 \pmod{4}$. In this case, we have $\chi(p) = 1$ for any $\chi \in PC^-(m)$. Since $\nu_p\alpha \in B_m$, it follows that $1 + \chi(a) = 0$ for any $\chi \in PC^-(m)$. Therefore $a \equiv m/2 + 1 \pmod{m}$, and $\alpha = (1, m/2+1, m/2-2)$.

Case 2. Next, suppose that $p^{f/2} \equiv m/2 + 1 \pmod{m}$.

Case 2-1. If $p \equiv 1 \pmod{4}$, then $p \equiv m/f + 1 \pmod{2m/f}$ and we have

$$\langle p \rangle = \{t \in (\mathbb{Z}/m\mathbb{Z})^\times \mid t \equiv 1 \pmod{m/f}\}\,.$$

It follows that $\chi(\nu_p) = 0$ for any $\chi \in C(m)$ such that $\mathrm{cond}(\chi) > m/f$, where $\mathrm{cond}(\chi)$ denotes the conductor of χ. Let $d = (m, b)$ and $b' = b/d$. Then

$$\tau_f(\nu_p\alpha) = \begin{cases} f\{(1,a) + d(b')\} & (\text{if } d \leq f)\,, \\ f(1,a) & (\text{if } d > f)\,. \end{cases}$$

In the first case, we have $1 + \chi(a) + d\chi(b') = 0$ for any $\chi \in PC^-(m/f)$. This holds only when $d = 2$, $a \equiv 1$, $b' \equiv -1 \pmod{m/f}$. It follows that $a \in \langle p \rangle$ and $b \in -2\langle p \rangle$. Hence α is of type (i).

In the second case, we have $1 + \chi(a) = 0$ for any $\chi \in PC^-(m/f)$. Therefore $a \equiv -1$ or $m/2f + 1 \pmod{m/f}$. But if $a \equiv m/2f + 1 \pmod{m/f}$, then

$$b \equiv -1 - a \equiv m/2f - 2 \pmod{m/f}\,,$$

and so $d = 2$, which is a contradiction. Therefore $a \equiv -1 \pmod{m/f}$. It follows that $a \in -\langle p \rangle$, say $a \equiv -p^i \pmod{m}$, then $b \equiv p^i - 1 \pmod{m}$. Hence α is of type (ii).

Case 2-2. On the other hand, if $p \equiv -1 \pmod 4$, then $p \equiv m/f - 1 \pmod{2m/f}$ since $m/f \geq 4$, and we have

$$\langle p^2 \rangle = \{t \in (\mathbb{Z}/m\mathbb{Z})^\times \mid t \equiv 1 \pmod{2m/f}\}.$$

Note that

$$\nu_p = (1, p)(1, p^2, \ldots, p^{f-2}).$$

It follows that $\chi(\nu_p) = 0$ for any $\chi \in C(m)$ such that $\mathrm{cond}(\chi) > 2m/f$. We have

$$\tau_f(\nu_p \alpha) = \begin{cases} \dfrac{f}{2}(1, m/f - 1)\{(1, a) + d(b')\} & (\text{if } d < f), \\ f(1, a) & (\text{if } d \geq f). \end{cases}$$

In the first case, since $m/f - 1 \in U(2m/f)$, we have $1 + \chi(a) + d\chi(b') = 0$ for any $\chi \in PC^-(2m/f)$. This holds only when $d = 2$, $a \equiv 1$, $b' \equiv -1 \pmod{2m/f}$. It follows that $a \in \langle p \rangle$ and $b \in -2\langle p \rangle$. Hence α is of type (i).

In the second case, we have $1 + \chi(a) = 0$ for any $\chi \in PC^-(2m/f)$. Therefore $a \equiv -1$ or $m/f + 1 \pmod{2m/f}$. But if $a \equiv m/f + 1 \pmod{2m/f}$, then

$$b \equiv -1 - a \equiv m/f - 2 \pmod{2m/f},$$

and so $d = 2$, which is a contradiction. Therefore $a \equiv -1 \pmod{2m/f}$. It follows that $a \in -\langle p \rangle$, say $a \equiv -p^i \pmod m$, then $b \equiv p^i - 1 \pmod m$. Hence α is of type (ii). This completes the proof. □

5. Evaluation of some character sums

For a power $l^e (> 2)$ of a prime number l, we define two subgroups $V_1(l^e)$, $V_2(l^e)$ of $(\mathbb{Z}/l^e\mathbb{Z})^\times$ as follows. If l is an odd prime number, let

$$V_1(l^e) = \{x \in (\mathbb{Z}/l^e\mathbb{Z})^\times \mid x^2 \equiv 1 \pmod{l^e}\},$$
$$V_2(l^e) = \{x \in (\mathbb{Z}/l^e\mathbb{Z})^\times \mid x^{n(l^e)} \equiv \pm 1 \pmod{l^e}\},$$

where

$$n(l^e) = \begin{cases} (l-1)/2 & (e = 1), \\ l & (e > 1). \end{cases} \tag{3}$$

If $l = 2$, let

$$V_1(2^e) = V_2(2^e) = \{\pm 1, 2^{e-1} \pm 1\}.$$

Let $m = m_0 m_1 \cdots m_r$ be the prime power factorization of m, where $m_0 = 1, 3, 4$ or 12, and for $i = 1, \ldots, r$ $m_i = l_i^{e_i} > 4$ is a power of a prime number such that $(m_i, m_j) = 1$ $(i \neq j)$. Let

$$V_1(m_0) = V_2(m_0) = (\mathbb{Z}/m_0\mathbb{Z})^\times$$

and define the subgroups $V_1(m)$, $V_2(m)$ of $(\mathbb{Z}/m\mathbb{Z})^\times$ by

$$V_1(m) = V_1(m_0) \times V_1(m_1) \times \cdots \times V_1(l_r^{e_r}),$$
$$V_2(m) = V_2(m_0) \times V_2(l_1^{e_1}) \times \cdots \times V_2(l_r^{e_r}).$$

Let

$$E(m) = \begin{cases} \{(\varepsilon_1, \ldots, \varepsilon_r) \mid \varepsilon_i = \pm 1 \ (i = 1, \ldots, r)\} & (\text{if } m_0 = 1)\,, \\ \{(-1, \varepsilon_1, \ldots, \varepsilon_r) \mid \varepsilon_i = \pm 1 \ (i = 1, \ldots, r)\} & (\text{if } m_0 = 3 \text{ or } 4)\,, \\ \{(1, \varepsilon_1, \ldots, \varepsilon_r) \mid \varepsilon_i = \pm 1 \ (i = 1, \ldots, r)\} & (\text{if } m_0 = 12) \end{cases}$$

and

$$E^+(m) = \{(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r) \mid \varepsilon_0\varepsilon_1 \cdots \varepsilon_r = 1\}\,,$$
$$E^-(m) = \{(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r) \mid \varepsilon_0\varepsilon_1 \cdots \varepsilon_r = -1\}\,.$$

It is clear from the definition that $\#E(m) = 2^r$. If $r > 0$, then

$$\#E^+(m) = \#E^-(m) = 2^{r-1}\,.$$

If $r = 0$, then

$$E(m_0) = E^-(m_0) = \{-1\}$$

for $m_0 = 3$ or 4, and $E(12) = E^+(12) = \{1\}$. For example, if $l > 4$ is a prime number and $m_0 = 3$ or 4, then $E(m_0 l) = \{(-1, 1)\}$.

For each $\mathbf{e} = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r) \in E(m)$ we define

$$PC^{\mathbf{e}}(m) = PC^{\varepsilon_0}(m_0) \times PC^{\varepsilon_1}(m_1) \times \cdots \times PC^{\varepsilon_r}(m_r)\,,$$

where $PC^{\varepsilon_i}(m_i)$ denotes $PC^+(m_i)$ or $PC^-(m_i)$ according as $\varepsilon_i = 1$ or -1. Then $PC^-(m) \neq \emptyset$ if and only if $m \neq 12$.

In the following, we assume that $m \neq m_0$. For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, let

$$\xi(a) = \frac{1}{\#E^-(m)} \sum_{\mathbf{e} \in E^-(m)} \frac{1}{\#PC^{\mathbf{e}}(m)} \sum_{\chi \in PC^{\mathbf{e}}(m)} \chi(a)\,.$$

To give an explicit formula for $\xi(a)$, we define some notations. Let

$$I_1 = \{i \in \{1, \ldots, r\} \mid e_i = 1\}\,,$$
$$I_2 = \{i \in \{1, \ldots, r\} \mid e_i > 1\}\,.$$

For $a \in V_2(m)$, define subsets $I(a) \subset I,\ I_2(a) \subset J$ by

$$I_1(a) = \{i \in I \mid a \notin V_1(l_i)\}\,,$$
$$I_2(a) = \{i \in J \mid a \in V_2(l_i^{e_i}) \setminus V_1(l_i^{e_i})\}\,.$$

Furthermore, let $\tilde{a}$ denote the unique element of $V_1(m)$ such that

$$\tilde{a} \equiv \begin{cases} a & (\text{mod } m_i) \quad (i \notin I_1(a) \cup I_2(a)) \\ a^{n_i} & (\text{mod } m_i) \quad (i \in I_1(a) \cup I_2(a))\,, \end{cases}$$

where $n_i = n(m_i)$ is the integer defined in (3). Put

$$\delta(a) = \prod_{i \in I_1(a)} l_i\,.$$

Let $c(a) = 1$ or 2 according as $m/\delta(a) \neq m_0$ or $m/\delta(a) = m_0$.

THEOREM 5.1. *For any $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, we have*

$$\xi(a) = \begin{cases} c(a)\chi_0(\tilde{a}) \displaystyle\prod_{i\in I_1(a)} \frac{-1}{l_i - 3} \prod_{i \in I_2(a)} \frac{-1}{l_i - 1} & (\textit{if } a \in V_2(m) \textit{ and } \tilde{a} \in \pm U(m/\delta(a))) \\ 0 & (\textit{otherwise}), \end{cases}$$

where χ_0 is an arbitrary character in $PC^+(\delta(a)) \times PC^-(m/\delta(a))$.

As for the special case $r = 1$, we have the following

COROLLARY 5.2. *Let $m = m_0 l$, where $m_0 = 3$ or 4 and $l > 3$ is a prime number. Let $\kappa = \pm 1$ and assume that $a \equiv \kappa \pmod{m_0}$. Then*

$$\xi(a) = \begin{cases} \kappa & (\textit{if } a \equiv \pm 1 \pmod{l}), \\ -\dfrac{2\kappa}{l-3} & (\textit{if } a \not\equiv \pm 1 \pmod{l}). \end{cases}$$

Proof. In this case, we have

$$\delta(a) = \begin{cases} 1 & (\text{if } a \equiv \pm 1 \pmod{l}), \\ l & (\text{if } a \not\equiv \pm 1 \pmod{l}). \end{cases}$$

In the first case, we have $c(a) = 1$, $a \in \pm U(m)$, and $\chi_0(a) = \kappa$ for any $\chi_0 \in PC^-(m)$. Hence $\xi(a) = \kappa$. In the second case, we have $c(a) = 2$, $\tilde{a} \in \pm U(m)$, and $\chi_0(\tilde{a}) = \kappa$ for any $\chi_0 \in PC^-(m)$. Hence $\xi(a) = -\frac{2\kappa}{l-3}$. This proves the corollary. □

Before proving the theorem, we prove two lemmas.

LEMMA 5.3. *Let l^e be a power of an odd prime number l or $l^e = 4$, and $\varepsilon = \pm$. Then the following assertions hold for any $a \in (\mathbb{Z}/l^e\mathbb{Z})^\times$.*

(i) *If $e = 1$, then*

$$\frac{1}{\#PC^\varepsilon(l)} \sum_{\chi \in PC^\varepsilon(l)} \chi(a) = \begin{cases} \chi_0(a) & (\textit{if } a \in V_1(l)), \\ -\dfrac{2}{l-3} & (\textit{if } a \notin V_1(l) \textit{ and } \varepsilon = +), \\ 0 & (\textit{if } a \notin V_1(l) \textit{ and } \varepsilon = -), \end{cases}$$

where χ_0 is an arbitrary element of $PC^\varepsilon(l)$.

(ii) *If $e > 1$, then*

$$\frac{1}{\#PC^\varepsilon(l^e)} \sum_{\chi \in PC^\varepsilon(l^e)} \chi(a) = \begin{cases} \chi_0(a) & (\textit{if } a \in V_1(l^e)), \\ -\dfrac{\chi_0(a^l)}{l-1} & (\textit{if } a \in V_2(l^e) \setminus V_1(l^e)), \\ 0 & (\textit{if } a \notin V_2(l^e)), \end{cases}$$

where χ_0 is an arbitrary element of $PC^\varepsilon(l^e)$.

Proof. The assertion is trivially true if $l^e = 3$ or 4 since $PC^-(3)$ and $PC^-(4)$ consists of one element. In the following, we assume that $l^e > 4$. The character group $C(l^e)$ is a cyclic group. Fix a generator χ_1 of $C(l^e)$. Then

$$PC^-(l^e) = \{\chi_1^k \mid 0 < k < \varphi(l^e),\ (k, 2l) = 1\},$$
$$PC^+(l^e) = \{\chi_1^{2k} \mid 0 < k < \varphi(l^e)/2,\ (k, l) = 1\}.$$

Put $\zeta = \chi_1(a)$.

First, suppose that $e = 1$. Then $\#PC^-(l) = (l-1)/2$ and

$$\begin{aligned}
\frac{1}{\#PC^-(l)} \sum_{\chi \in PC^-(l)} \chi(a) &= \frac{2}{l-1} \sum_{\substack{0<k<l-1 \\ (k,2)=1}} \zeta^k \\
&= \frac{2}{l-1} \left(\sum_{0<k\leq l-1} \zeta^k - \sum_{0<i\leq \varphi(l)/2} \zeta^{2k} \right) \\
&= \begin{cases} \zeta & (\text{if } \zeta = \pm 1), \\ 0 & (\text{if } \zeta \neq \pm 1). \end{cases}
\end{aligned}$$

If $l = 3$, then $PC^+(3) = \emptyset$. If $l > 3$, then $\#PC^+(l) = (l-3)/2$ and

$$\begin{aligned}
\frac{1}{\#PC^+(l)} \sum_{\chi \in PC^+(l)} \chi(a) &= \frac{2}{l-3} \sum_{0<k<(l-1)/2} \zeta^{2k} \\
&= \frac{2}{l-3} \left(\sum_{0<k\leq (l-1)/2} \zeta^{2k} - 1 \right) \\
&= \begin{cases} 1 & (\text{if } \zeta = \pm 1), \\ -\dfrac{2}{l-3} & (\text{if } \zeta \neq \pm 1). \end{cases}
\end{aligned}$$

This proves (i).

Next, suppose that $e > 1$. Then $\#PC^-(l^e) = \varphi(l^e)/2$ and

$$\begin{aligned}
&\frac{1}{\#PC^-(l^e)} \sum_{\chi \in PC^-(l^e)} \chi(a) = \frac{2}{\varphi(l^e)} \sum_{\substack{0<i<\varphi(l^e) \\ (k,2l)=1}} \zeta^k \\
&= \frac{2}{l^{e-1}(l-1)} \left(\sum_{0<k\leq\varphi(l^e)} \zeta^k - \sum_{0<k\leq\varphi(l^e)/2} \zeta^{2k} - \sum_{0<k\leq\varphi(l^e)/l} \zeta^{lk} + \sum_{0<i\leq\varphi(l^e)/2l} \zeta^{2lk} \right) \\
&= \begin{cases} \zeta & (\text{if } \zeta = \pm 1), \\ -\dfrac{\zeta^l}{l-1} & (\text{if } \zeta^l = \pm 1,\ \zeta \neq \pm 1), \\ 0 & (\text{if } \zeta^l \neq \pm 1). \end{cases}
\end{aligned}$$

On the other hand, we have $\#PC^+(l^e) = l^{e-2}(l-1)^2/2$ and

$$\begin{aligned}\frac{1}{\#PC^+(l^e)}\sum_{\chi\in PC^+(l^e)}\chi(a) &= \frac{2}{l^{e-2}(l-1)^2}\sum_{\substack{0<k<\varphi(l^e)/2\\(k,l)=1}}\zeta^{2k}\\ &= \frac{2}{l^{e-2}(l-1)^2}\left(\sum_{0<k\le\varphi(l^e)/2}\zeta^{2k}-\sum_{0<k\le\varphi(l^e)/2l}\zeta^{2lk}\right)\\ &= \begin{cases}1 & (\text{if } \zeta=\pm1)\,,\\ -\dfrac{1}{l-1} & (\text{if } \zeta^l=\pm1,\ \zeta\ne\pm1)\,,\\ 0 & (\text{if } \zeta^l\ne\pm1)\,.\end{cases}\end{aligned}$$

This proves (ii). □

LEMMA 5.4. *Let $e>2$. Then the following assertion holds for any $a\in(\mathbb{Z}/2^e\mathbb{Z})^\times$.*

$$\frac{1}{\#PC^\varepsilon(2^e)}\sum_{\chi\in PC^\varepsilon(2^e)}\chi(a)=\begin{cases}\chi_0(a) & (\textit{if } a\in V_1(2^e))\,,\\ 0 & (\textit{if } a\notin V_1(2^e))\,,\end{cases}$$

where χ_0 is an arbitrary element of $PC^\varepsilon(2^e)$.

Proof. Since $(\mathbb{Z}/2^e\mathbb{Z})^\times\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{e-2}\mathbb{Z}$, there exist two characters $\chi_1\in C^-(2^e)$, $\chi_2\in C^+(2^e)$ of order 2 and 2^{e-2}, respectively. Then $C(2^e)$ is generated by χ_1 and χ_2, and

$$\begin{aligned}PC^-(2^e)&=\{\chi_1\chi_2^k\mid 0<k<2^{e-2},\ (k,2)=1\}\,,\\ PC^+(2^e)&=\{\chi_1^k\mid 0<k<2^{e-2},\ (k,2)=1\}\,.\end{aligned}$$

Hence $\#PC^-(2^e)=\#PC^+(2^e)=2^{e-3}$. Put $\chi_1(a)=\eta$ and $\zeta=\chi_2(a)$. Then

$$\begin{aligned}\frac{1}{\#PC^-(2^e)}\sum_{\chi\in PC^-(2^e)}\chi(a)&=\frac{1}{2^{e-3}}\sum_{\substack{0<k<2^{e-2}\\(k,2)=1}}\eta\zeta^k\\ &=\frac{1}{2^{e-3}}\left(\sum_{0<k\le2^{e-2}}\eta\zeta^k-\sum_{0<k\le2^{e-3}}\eta\zeta^{2k}\right)\\ &=\begin{cases}\eta\zeta & (\text{if } \zeta=\pm1)\,,\\ 0 & (\text{if } \zeta\ne\pm1)\,.\end{cases}\end{aligned}$$

On the other hand, as for $PC^+(2^e)$ we have

$$\begin{aligned}\frac{1}{\#PC^+(2^e)}\sum_{\chi\in PC^+(2^e)}\chi(a)&=\frac{1}{2^{e-3}}\sum_{\substack{0<k<2^{e-2}\\(k,2)=1}}\zeta^k\\ &=\frac{1}{2^{e-3}}\left(\sum_{0<i\le2^{e-2}}\zeta^k-\sum_{0<i\le2^{e-3}}\zeta^{2k}\right)\\ &=\begin{cases}\zeta & (\text{if } \zeta=\pm1)\,,\\ 0 & (\text{if } \zeta\ne\pm1)\,.\end{cases}\end{aligned}$$

Note that $\zeta = \pm 1$ if and only if $a \in V_1(2^e)$, and that if $a \in V_1(2^e)$, then $\chi(a) = \eta\zeta$ for any $\chi \in PC^-(2^e)$ and $\chi(a) = \zeta$ for any $\chi \in PC^+(2^e)$. Therefore the lemma holds. □

Proof of Theorem 5.1. For each $\mathbf{e} \in E(m)$, define

$$\xi^{\mathbf{e}}(a) = \frac{1}{\# PC^{\mathbf{e}}(m)} \sum_{\chi \in PC^{\mathbf{e}}(m)} \chi(a) .$$

Then $\xi(a)$ is the average of $\xi^{\mathbf{e}}(a)$ ($\mathbf{e} \in E^-(m,a)$), that is,

$$\xi(a) = \frac{1}{\# E^-(m)} \sum_{\mathbf{e} \in E^-(m)} \xi^{\mathbf{e}}(a) .$$

In order to calculate $\xi^{\mathbf{e}}(a)$, let

$$E^*(m,a) = \{(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r) \in E^*(m) \mid \varepsilon_i = +1 \ \text{ for any } i \in I_1(a)\} ,$$

where $*$ denotes $+$ or $-$. If $m_0 = 3$ or 4, then $E^-(m,a) \neq \emptyset$ for any a, and if $m_0 = 1$ or 12, then $E^-(m,a) = \emptyset$ if and only if $\delta(a) = m'$.

Let

$$\chi^{\mathbf{e}} = \prod_{i=1}^{r} \chi_{m_i}^{k_i} \ \in PC^{\mathbf{e}}(m) ,$$

where χ_{m_i} is a generator of $C(m_i)$ and $k = 1$ if $\varepsilon_i = -1$ and $k_i = 2$ if $\varepsilon_i = +1$. Then from Lemma 5.3 and Lemma 5.4 it follows that

$$\xi^{\mathbf{e}}(a) = \begin{cases} \chi^{\mathbf{e}}(\tilde{a}) \displaystyle\prod_{i \in I_1(a)} \frac{-2}{l_i - 3} \prod_{i \in I_2(a)} \frac{-1}{l_i - 1} & (\text{if } \ a \in V_2(m) \text{ and } \varepsilon \in E^-(m,a)) , \\ 0 & (\text{otherwise}) . \end{cases}$$

Therefore,

$$\xi(a) = \frac{1}{\# E^-(m)} \left(\sum_{\mathbf{e} \in E^-(m,a)} \chi_0^{\mathbf{e}}(\tilde{a}) \right) \prod_{i \in I_1(a)} \frac{-2}{l_i - 3} \prod_{i \in I_2(a)} \frac{-1}{l_i - 1} .$$

Now, suppose $E^-(m,a) \neq \emptyset$ and fix an element $\mathbf{e}_0 \in E^-(m,a)$. Then

$$E^-(m,a) = \mathbf{e}_0 E^+(m,a) .$$

If $\# E^-(m,a) = 1$, then $E^+(m,a) = \{\mathbf{1}\}$, where $\mathbf{1} = (1, \dots, 1)$. But this is equivalent to the condition $\delta(a) = m'$. On the other hand, if $\# E^-(m,a) > 1$, then write $\mathbf{e} = \mathbf{e}_0 \mathbf{e}'$ with $\mathbf{e}' \in E^+(m,a)$. Then

$$\chi^{\mathbf{e}} = \chi^{\mathbf{e}_0} \chi^{\mathbf{e}'} .$$

Hence

$$\begin{aligned} \frac{1}{\# E^-(m,a)} \sum_{\mathbf{e} \in E^-(m,a)} \chi^{\mathbf{e}}(\tilde{a}) &= \frac{\chi^{\mathbf{e}_0}(\tilde{a})}{\# E^-(m,a)} \sum_{\mathbf{e}' \in E^+(m,a)} \chi^{\mathbf{e}'}(\tilde{a}) \\ &= \begin{cases} \chi^{\mathbf{e}_0}(\tilde{a}) & (\text{if } \ \tilde{a} \equiv \pm 1 \pmod{m'/\delta(a)}) , \\ 0 & (\text{if } \ \tilde{a} \not\equiv \pm 1 \pmod{m'/\delta(a)}) . \end{cases} \end{aligned}$$

Note that

$$\tilde{a} \equiv \pm 1 \pmod{m'/\delta(a)} \iff \tilde{a} \in \pm U(m/\delta(a)) .$$

Moreover, if $E^-(m,a) \neq \emptyset$, then

$$\#E^-(m,a) = \begin{cases} \#E^-(m)/2^{\#I_1(a)} & (\text{if } m/\delta(a) \neq m_0) , \\ \#E^-(m)/2^{\#I_1(a)-1} & (\text{if } m/\delta(a) = m_0) . \end{cases}$$

Therefore,

$$\#E^-(m,a) = c(a) \cdot \frac{\#E^-(m)}{2^{\#I_1(a)}} ,$$

and consequently

$$\begin{aligned} \xi(a) &= \frac{c(a)\chi_0(\tilde{a})}{2^{\#I_1(a)}} \prod_{i \in I_1(a)} \frac{-2}{l_i - 3} \prod_{i \in I_2(a)} \frac{-1}{l_i - 1} \\ &= c(a)\chi_0(\tilde{a}) \prod_{i \in I_1(a)} \frac{-1}{l_i - 3} \prod_{i \in I_2(a)} \frac{-1}{l_i - 1} . \end{aligned}$$

This completes the proof. □

6. A useful lemma in the case of $m = m_0 l$

In the following we consider the case of $m = 3l$ or $m = 4l$ with l being a prime number > 3. We will always assume that $p^i \not\equiv -1 \pmod{m}$ for any integer i. Let H be the subgroup of $(\mathbb{Z}/l\mathbb{Z})^\times$ generated by the class of p, and let $\tilde{H}$ be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by the classes of -1 and p.

The lemma below will be useful in the following sections.

LEMMA 6.1. *Let $m = m_0 l$, where $m_0 = 3$ or 4, and $l > 3$ is a prime number. Suppose that f is even and $p^{f/2} \not\equiv -1 \pmod{m}$. Let $a_1, \ldots, a_r$ be r elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ such that*

(a) $a_i \tilde{H} \not\equiv a_j \tilde{H}$ $(i \neq j)$, *and*

(b) $\chi(\nu_p(a_1, \ldots, a_r)) = 0$ *for any* $\chi \in PC^-(m)$.

Assume that $p^{f/2} \in U(m)$. Then the following assertions hold.

(i) $f = \frac{l-1}{r}$.

(ii) $p \equiv 1 \pmod{m_0}$ *and* $a_1 \equiv \cdots \equiv a_r \pmod{m_0}$.

(iii) $\nu_p(a_1, \ldots, a_r) = \sigma_{l,1}^{(1)}$,

where $\sigma_{l,1}^{(1)}$ denotes the primitive part of $\sigma_{l,1}$.

Proof. Without loss of generality we may assume that $a_1 = 1$. Note that the assumption (a) implies that

$$r \geq ((\mathbb{Z}/m\mathbb{Z})^\times : \tilde{H}) .$$

Since $V_1(m) = \{\pm 1, \pm u\}$ and $p^{f/2} \in V_1(m)$, we have $|\tilde{H}| = 2f$, and hence

$$((\mathbb{Z}/m\mathbb{Z})^\times : \tilde{H}) = \frac{2(l-1)}{2f} .$$

Therefore, $f \leq \frac{l-1}{r}$.

Let w denote u or v according as $m = 4l$ or $3l$, respectively. Since $p^{f/2} \not\equiv \pm 1 \pmod{m}$, we have $p^{f/2} \equiv \pm w \pmod{m}$.

Since $p^{f/2} \equiv w \pmod{m}$, we have $\nu_p = (1, w)\nu'_p$, where

$$\nu'_p = (1, p, \dots, p^{f/2-1}) .$$

It follows that $\chi(\nu_p \alpha) = 2\chi(\nu'_p \alpha)$ for any $\chi \in PC^-(m)$. Put

$$\nu''_p = (p, p^2, \dots, p^{f/2-1}) , \qquad \alpha' = (a_2, \dots, a_r) .$$

Then

$$\nu_p \alpha = (1, w)((1) + \nu''_p + \nu'_p \alpha') .$$

It follows that

$$2\{1 + \xi(\nu''_p) + \xi(\nu'_p \alpha')\} = 0 . \tag{4}$$

Since every component of ν''_p and $\nu'_p \alpha'$ is in $(\mathbb{Z}/m\mathbb{Z})^\times \setminus V_1(m)$, it follows from Theorem 5.1 that

$$|\xi(\nu''_p) + \xi(\nu'_p \alpha')| \leq \frac{2}{l-3} \cdot \left\{ \frac{f}{2} - 1 + \frac{f}{2}(r-1) \right\} = \frac{fr-2}{l-3} . \tag{5}$$

But $\xi(\nu''_p) + \xi(\nu'_p \alpha') = -1$ by (4). Therefore, $\frac{fr-2}{l-3} \geq 1$ and so $f \geq \frac{l-1}{r}$. Hence $f = \frac{l-1}{r}$. But this holds if and only if the equality holds in (5). Therefore, Theorem 5.1 again implies that $p \equiv a_1 \equiv \cdots \equiv a_r \equiv 1 \pmod{m_0}$. This completes the proof. □

For each divisor n of $l-1$, let χ_l be a generator of $C(l)$ and put

$$\eta(a) = \frac{2n}{l-1} \sum_{\substack{0<k<(l-1)/n \\ k:\text{odd}}} \chi_l^k(a) .$$

LEMMA 6.2. *Notation being as above, we have*

$$\eta(a) = \begin{cases} 1 & (a^n \equiv 1 \pmod{l}) , \\ -1 & (a^n \equiv -1 \pmod{l}) , \\ 0 & (a^n \not\equiv \pm 1 \pmod{l}) . \end{cases}$$

In particular, if at least one of $\eta(a)$ and $\eta(b)$ is non-zero, then

$$\eta(ab) = \eta(a)\eta(b) .$$

Proof. Let χ be a generator of $C(l)$ and put $\chi(a) = \zeta$. Then

$$\eta(a) = \frac{2n}{l-1} \left(\sum_{0<k\leq(l-1)/n} \zeta^k - \sum_{0<k\leq(l-1)/2n} \zeta^{2k} \right) .$$

Here note that the first sum equals $(l-1)/n$ or 0 according as $\zeta = 1$ or not, and the second sum equals $(l-1)/2n$ or 0 according as $\zeta^2 = 1$ or not. Therefore we have

$$\eta(a) = \begin{cases} 1 & (\zeta = 1) \\ -1 & (\zeta = -1) \\ 0 & (\zeta \neq \pm 1) . \end{cases}$$

Since $\zeta = 1$ (resp. -1) if and only if $a^n \equiv 1$ (resp. -1) $\pmod{l}$, this proves the lemma. □

7. The case $N(\alpha) = 3$

For a primitive element $\alpha = (a_1, a_2, a_3) \in \mathfrak{A}_m$, let

$$N(\alpha) = \#\{i \mid (m, a_i) = 1\}\,.$$

If $m = m_0 l$ with $m_0 = 3$ or 4, then $N(\alpha) = 1, 2$ or 3. In addition, if $N(\alpha) = 3$, then m must be odd, so $m = 3l$ and

$$a_1 \equiv a_2 \equiv a_3 \equiv 1 \pmod{3}\,.$$

Recall that H is the subgroup of $(\mathbb{Z}/l\mathbb{Z})^\times$ generated by the class of p, and $\tilde{H}$ is the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by the classes of -1 and p.

THEOREM 7.1. *Let $m = 3l$ and assume that $p^i \not\equiv -1 \pmod{m}$ for any integer i. Let $\alpha = (1, a, b) \in \mathfrak{A}_m$ be such that $(ab, m) = 1$. Assume that $\nu_p\alpha \in B_m$. Then the following statements hold.*

(i) *If $p^{f/2} \equiv v \pmod{m}$, then $l \equiv 1 \pmod{3}$, and either $f = l - 1$ or $f = (l-1)/3$. Moreover, $\{1, a, b\}$ is a complete set of representative of $(\mathbb{Z}/m\mathbb{Z})^\times/\tilde{H}$ if $f = (l-1)/3$. In this case, we have*

$$\nu_p\alpha = \begin{cases} \sigma_{l,\alpha} - (l, -l)\alpha & (\text{if } f = l - 1)\,, \\ \sigma_{l,1} - (l, -l) & (\text{if } f = (l-1)/3)\,. \end{cases}$$

(ii) *If $p^{f/2} \equiv -v \pmod{m}$, then either*

(1) *$3 \in \langle p \pmod{l}\rangle$ or*

(2) *$\{1, a, b\}H = \langle a, p \pmod{l}\rangle$ is the subgroup of $(\mathbb{Z}/l\mathbb{Z})^\times$ of order $3f/2$ and $3 \in \langle a, p \pmod{l}\rangle$.*

In this case, we have

$$\nu_p\alpha = \sigma_{3,\nu'_p\alpha} - (3, -3)\nu'_p\alpha\,.$$

Proof. Case 1. Suppose $p^{f/2} \equiv v \pmod{m}$. Then

$$\nu_p = (1, v)\nu'_p\,,$$

where $\nu'_p = (1, p, \ldots, p^{f/2-1})$.

Case 1-1. If $\{1, a, b\}$ is a complete set of representative of $(\mathbb{Z}/m\mathbb{Z})^\times/\tilde{H}$, then Lemma 6.1 implies that $l \equiv 1 \pmod{3}$, $f = (l-1)/3$ and

$$\nu_p\alpha = \sigma_{l,1} - (l, -l) \in B_m\,.$$

Case 1-2. Suppose $\{1, a, b\}$ is not a complete set of representative of $(\mathbb{Z}/m\mathbb{Z})^\times/\tilde{H}$. Then there are only two essentially distinct cases:

(i) $a \in \tilde{H}, b \notin \tilde{H}$.

(ii) $a, b \in \tilde{H}$.

In the case of (i), $a \in \langle p\rangle$ or $a \in -\langle p\rangle$. In the first case, we have

$$\nu_p\alpha = \nu_p(1, 1, b)\,.$$

But since $\chi((1, 1, b)) \neq 0$ for any $\chi \in PC^-(m)$, this implies that $\nu_p \in B_m$. In the second case, we have

$$\nu_p\alpha = \nu_p(1, -1, b)\,.$$

This also implies that $\nu_p \in B_m$. Consequently we have $\nu_p \in B_m$ in the both cases.

Now, write ν_p as

$$\nu'_p = (1) + \nu''_p\,,$$

where $\nu''_p = (p, p^2, \dots, p^{f/2-1})$. Then

$$0 = \xi(\nu_p) = 1 + \xi(\nu''_p)\,.$$

Since $p^i \notin V_1(m)$ for any $i = 1, \dots, f/2 - 1$, it follows that

$$1 = |\xi(\nu''_p)| \leq \frac{2}{l-3}(f/2-1) = \frac{f-2}{l-3} \leq 1\,.$$

Therefore $f = l - 1$ and $p \equiv 1 \pmod 3$. This implies that $\nu_p = \sigma^{(1)}_{l,1}$. If $l \equiv 1 \pmod 3$, then it follows that $\nu_p = \sigma_{l,1} - (l, -l)$ and so

$$\nu_p\alpha = \sigma_{l,\alpha} - (l, -l)\alpha\,.$$

On the other hand, if $l \equiv -1 \pmod 3$, then

$$\nu_p\alpha = \sigma_{l,\alpha} - 2(-l)\alpha\,.$$

But since $(-l)\alpha = (-l, -l, -l) \notin B_m$, this case does not occur.

Case 2. Suppose $p^{f/2} \equiv -v \pmod m$. Then $f/2$ is odd and $p \equiv -1 \pmod 3$. We have

$$\nu_p = (1, -v)\nu'_p\,.$$

Since $-v \equiv -1 \pmod 3$, we have

$$\tau_l(\nu_p\alpha) = 3(1, -l^{-1})(1, -1)\nu'_p \in D_3\,.$$

On the other hand, we have

$$\tau_3(\nu_p\alpha) = 2(1, -3^{-1})\nu'_p\alpha\,.$$

If $3 \in H$, then $(1, -3^{-1})\nu'_p \in D_l$, and so $(1, -3^{-1})\nu'_p\alpha \in D_l$. On the contrary, if $3 \notin H$, then

$$(1 - \chi(3)^{-1})\chi(\alpha) = 0$$

for the character $\chi = \chi_l^{f/2} \in PC^-(l)$, where χ_l is a generator of $C(l)$. Since $3 \notin H$, we have $\chi(3) \neq 1$, hence $\chi(\alpha) = 0$. Then the order of a in $(\mathbb{Z}/l\mathbb{Z})^\times/H$ is 3, and

$$b \equiv a^2 p^i \pmod l$$

for some i. Taking $\chi = \chi^3 = \chi_l^{3f/2} \in PC^-(l)$, we have

$$0 = \chi'(\tau_3(\nu_p\alpha)) = 3f(1 - \chi'(3)^{-1})\,.$$

Hence $\chi'(3) = 1$. This implies that $3 \in \langle a, p \,(\mathrm{mod}\ l)\rangle$.

In order to get an explicit form of $\nu_p\alpha$, first suppose $l \equiv 1 \pmod 3$. Then $v = 2l - 1$ and

$$(1, -v) = \sigma_{3,1} - (2l + 1, -3) .$$

Since $3 \in \{1, a, b\}H = \langle a, p \,(\mathrm{mod}\, l)\rangle$, we have $(2l + 1, -3)\nu'_p\alpha = (3, -3)\nu'_p\alpha \in D_m$. Therefore

$$\nu_p\alpha = \sigma_{3,\nu'_p\alpha} - (3, -3)\nu'_p\alpha \in B_m .$$

Next suppose $l \equiv 2 \pmod 3$. Then $v = l - 1$ and

$$(1, -v) = \sigma_{3,1} - (l + 1, -3) .$$

Since $3 \in \langle a, p \,(\mathrm{mod}\, l)\rangle$, we have $(l + 1, -3)\nu'_p\alpha = (3, -3)\nu'_p\alpha \in D_m$. Therefore

$$\nu_p\alpha = \sigma_{3,\nu'_p\alpha} - (3, -3)\nu'_p\alpha \in B_m$$

This completes the proof. □

8. The case $N(\alpha) = 2$

In this section we consider the case where $N(\alpha) = 2$. For this we begin with the following

PROPOSITION 8.1. *Let x be an element of $(\mathbb{Z}/m\mathbb{Z})^\times$ of order 2. If $p^{f/2} \equiv x \pmod m$, then $(1, -x, x - 1)$ belongs to $B_m(p)$.*

Proof. Let $\nu'_p = (1, p, \ldots, p^{f/2-1})$. Then $\nu_p = (1, x)\nu'_p$. It follows that

$$\begin{aligned}\nu_p\alpha &= (1, x)\nu'_p(1, -x) + (1, x)\nu'_p(x - 1)\\ &= (1, x)(1, -x)\nu'_p + (x - 1, 1 - x)\nu'_p\\ &= (1, -1)(1, -x)\nu'_p + (1, -1)(x - 1)\nu'_p\\ &= (1, -1)(1, -x, x - 1)\nu'_p\\ &= (1, -1)\alpha\nu'_p \in D_m .\end{aligned}$$

Therefore $\alpha \in B_m(p)$. □

THEOREM 8.2. *Let $m = 3l$, where l is a prime number greater than 3. Let $\alpha = (1, a, b)$ be an element of $\in B_m(p)$ such that $(m, a) = 1$ and $(m, b) > 1$. Assume that $p^i \not\equiv -1 \pmod m$ for any integer i. Then one of the following statements holds.*

(i) *If $p^{f/2} \equiv v \pmod m$, then $\alpha = (1, -p^i, p^i - 1)$, where i is an integer such that $0 < i < f$ and $p^i \equiv 1 \pmod 3$.*

(ii) *If $p^{f/2} \equiv -v \pmod m$, then $\alpha = (1, v, -v - 1)$.*

In the both cases, we have

$$\nu_p\alpha = (1, -1)\alpha\nu'_p \in D_m .$$

Proof. Case 1. First consider the case $p^{f/2} \equiv v \pmod m$.

Case 1-1. Suppose $a \notin \tilde{H}$. Then Lemma 6.1 implies that $f = (l-1)/2$, $a \equiv 1 \pmod 3$ and $\{1, a\}$ is a complete set of representative of $(\mathbb{Z}/l\mathbb{Z})^\times/H$. In this case we have

$$\nu_p(1, a) = \sigma_{l,1}^{(1)} .$$

Since $a \not\equiv -1 \pmod 3$, $b \not\equiv 0 \pmod 3$ and so $l|b$. But in this case it follows that $a \equiv -1 \pmod l$, which implies that $a \in \tilde{H}$. This gives a contradiction. Hence this case cannot occur.

Case 1-2. Suppose $a \in \tilde{H}$. Then $a \in H$ or $a \in -H$.

If $a \in H$, then

$$\nu_p \alpha = \nu_p(1, 1, b) .$$

It follows that $\chi(\nu_p) = 0$ for any $\chi \in PC^-(m)$. Then by Lemma 6.1 we have

$$f = l - 1 , \qquad p \equiv 1 \pmod 3 , \qquad \nu_p = \sigma_{l,1}^{(1)} .$$

In this case, we have $a \equiv 1 \pmod 3$ and so $b \not\equiv 0 \pmod 3$. Consequently $l|b$. But in this case, we have $a \equiv -1 \pmod l$, which implies that $a = v$ and $b = -v - 1$. Therefore

$$\tau_l(\nu_p \alpha) = f\{2(1, -l^{-1}) + (l-1)(-l^{-1})\} .$$

It follows that

$$2(1, -l^{-1}) + (l-1)(-l^{-1}) \in D_3 .$$

But this is impossible.

If $a \in -\langle p \pmod l \rangle$, then

$$\nu_p \alpha = \nu_p(1, -1, b) .$$

It follows that $(b)\nu_p \in B_m$.

If $3|b$, then $(b)\nu_p \in D_m$ and

$$\alpha = (1, -p^i, p^i - 1)$$

for some i such that $p^i \equiv 1 \pmod 3$.

If $l|m$, then $a \equiv -1 \pmod l$. But since $a \equiv -p^i \pmod m$ for some i with $0 < i < f$, we have $p^i \equiv 1 \pmod l$, which is a contradiction.

Case 2. Next consider the case $p^{f/2} \equiv -v \pmod m$. Then $f/2$ is odd and $p \equiv -1 \pmod 3$. In this case, we have

$$\nu_p = (1, -v)\nu'_p .$$

Suppose $l|b$. Then $a \equiv -1 \pmod{-1}$. It follows that $a = v$ and

$$\nu_p(1, a) = (1, -v)(1, v)\nu'_p = (1, -1)(1, v)\nu'_p \in D_m .$$

Since $p \equiv -1 \pmod 3$, we have $(b)\nu_p \in D_m$, and consequently $\nu_p \alpha \in B_m$.

If $3|b$, then $a \equiv -1 \pmod 3$. In this case, we have

$$\tau_3(\nu_p \alpha) = 2\nu'_p\{(1, -3^{-1})(1, a) + 2(b')\} .$$

But one can show that the right hand side cannot belong to D_l, which is a contradiction. This completes the proof. □

THEOREM 8.3. *Let $m = 4l$, where l is a prime number greater than 3. Let $\alpha = (1, a, b)$ be an element of $B_m(p)$ such that $(m, a) = 1$ and $(m, b) > 1$. Assume that $p^i \not\equiv -1 \pmod m$ for any integer i.*

(i) *If $p^{f/2} \equiv u \pmod m$, then $p \equiv a \equiv 1 \pmod 4$ and $f = l - 1$ or $(l-1)/2$.*

(1) *If $f = l - 1$, then $l \equiv 1 \pmod 4$ and*

$$\nu_p \alpha = \sigma_{l,\alpha} - (l, -l)\alpha .$$

(2) *If $f = (l-1)/2$, then $l \equiv 1 \pmod 4$, $\{1, a\}$ is a complete set of representatives of $(\mathbb{Z}/m\mathbb{Z})^\times/\tilde{H}$ and*

$$\nu_p \alpha = \sigma_{l,(1,b)} - (l, -l) - (lb, -lb) .$$

(ii) *If $p^{f/2} \equiv -u \pmod m$, then one of the following statements holds.*

(1) *$\alpha = (1, m/2 - 1, m/2)$ and*

$$\nu_p \alpha = (1, -1)\nu'_p \alpha .$$

(2) *$a \equiv 1 \pmod 4$, $2 \in H$, and*

$$\nu_p \alpha = \sigma'_{2,\nu'_p\alpha} - (4, -4)\nu'_p \alpha .$$

Proof. Case 1. Suppose $p^{f/2} \equiv u \pmod m$.

If $l | b$, then $\alpha = (1, m/2 - 1, m/2)$. By Lemma 6.1 one can easily see that $\alpha \in B_m(p)$ if and only if $f = l - 1$ and $l \equiv 1 \pmod 4$. Thus we may assume that $l \nmid b$.

Case 1-1. Suppose $a \notin \tilde{H}$. Then $a \not\equiv \pm 1 \pmod l$. In particular, $1 + a \not\equiv 0 \pmod l$. Therefore $b \not\equiv 0 \pmod l$.

By Lemma 6.1, we have $f = (l-1)/2$ and $p \equiv a \equiv 1 \pmod 4$. Hence

$$\tau_l(\nu_p \alpha) = (1, -l^{-1})\nu_p(1, a) = 2f(1, -l^{-1}) \in D_4 .$$

This is possible only when $l \equiv 1 \pmod 4$. Moreover we have

$$\tau_4(\nu_p \alpha) = (1, -2^{-1})\nu_p\{(1, a) + 2(b')\} ,$$

which belongs to D_l since $p^{f/2} \equiv -1 \pmod l$. Hence

$$\nu_p \alpha = \sigma_{l,1} - (l, -l) + \nu_p(b) .$$

Here we note that $\nu_p(b) = (b, -b)\nu'_p \in D_m$.

Case 1-2. Suppose $a \in H$. Then $a \in \pm\langle p \rangle$.

If $a \equiv p^i \pmod m$ for some i, then we have $\nu_p(1, a) = 2\nu_p$. Therefore, $\chi(\nu_p) = 0$ for any $\chi \in PC^-(m)$. Then Lemma 6.1 again shows that $f = l - 1$ and $p \equiv 1 \pmod 4$. Hence $a \equiv 1 \pmod 4$ and $2 \| b$. Therefore

$$\tau_4(\nu_p \alpha) = (1, -2^{-1})\nu_p\{(1, a) + 2(b')\} .$$

This implies that $b \equiv 2p^i \pmod m$.

On the other hand, if $a \equiv -p^i \pmod m$ for some i, then one can easily see that α is of type (ii) of Theorem 1.1.

Case 2. Suppose that $p^{f/2} \equiv -u \pmod m$.

If $l|b$, then $\alpha = (1, m/2-1, m/2)$. In this case, we see that

$$\nu_p\alpha = (1,-1)\nu'_p\alpha \in D_m\,.$$

Assume that $l \nmid b$.

Case 2-1. Suppose $a \notin \tilde{H}$. In this case, since $p^{f/2} \equiv -1 \pmod 4$, we have

$$\tau_l(\nu_p\alpha) = (1, -l^{-1})\nu_p(1,a) \in D_4\,.$$

Moreover

$$\tau_4(\nu_p\alpha) = \begin{cases} (1,-2^{-1})\nu_p\{(1,a)+2(b')\} & (\text{if } 2||b)\,, \\ \nu_p\{(1,-2^{-1})(1,a)+2(b')\} & (\text{if } 4|b)\,. \end{cases}$$

Since a similar argument as above shows that the case $4|b$ cannot occur, we suppose that $2||b$. In this case, we have $a \equiv 1 \pmod 4$ since $1+a \equiv 2 \pmod 4$. Letting $\chi = \chi^{f/2}$, we have

$$(1-\chi(2^{-1}))(1+\chi(a)+2\chi(b')) = 0\,.$$

If $1+\chi(a)+2\chi(b') = 0$, then $\chi(a) = 1$ and $\chi(b') = -1$. But this implies that $a \in H$, which is a contradiction. Therefore, $\chi(2) = 1$, which implies that $2^n \equiv 1 \pmod l$, or equivalently $2 \in \langle p \pmod l\rangle$. Then the assertion follows since

$$\nu_p\alpha = \sigma'_{2,\nu'_p\alpha} - (4,-4)\nu'_p\alpha\,.$$

Case 2-2. Suppose $a \in H$. Then $a \in \pm \pmod{\langle p\rangle}$.

If $a \equiv p^i \pmod m$, then $\nu_p(1,a) = 2\nu_p$ and

$$\nu_p\alpha = \sigma_{2,(1,a)\nu'_p} - \sigma_{2,(-2)(1,a)\nu'_p} + 2\sigma_{2,(b)\nu'_p} + (m/2-2,4)\nu'_p - 2(m/2+b,-2b)\nu'_p\,.$$

Therefore $\nu_p \in B_m$ if and only if

$$(m/2-2,4)\nu'_p - 2(m/2+b,-2b)\nu'_p \in D_m\,,$$

and this holds if and only if $2 \in \langle p \pmod l\rangle$.

On the other hand, if $a \equiv -p^i \pmod m$ for some i, then

$$\nu_p\alpha = (1,-1)\nu_p \in D_m\,.$$

Therefore, $\nu_p\alpha \in B_m$ if and only if $(b)\nu_p \in B_m$. This holds if and only if α is the element of type (ii) of Theorem 1.1. This completes the proof. □

9. The case $N(\alpha) = 1$

In this section we prove the following

THEOREM 9.1. *Let $m = 4l$ and assume that $p^i \not\equiv -1 \pmod m$ for any integer i. Let $\alpha = (1,a,b)$ be an element of $B_m(p)$ such that $2|a$, $l|b$. Then $\alpha = (1,3l-1,l)$ or $(1,l-1,3l)$, and the following assertions hold*:

(i) *If $2\|a$, then $2 \in H$.*

(ii) *If $4|a$, then $-2 \in H$.*

Moreover, we have

$$\nu_p\alpha = \begin{cases} \sigma'_{2,(1,a)\nu'_p} - (4,-4)(1,a)\nu'_p + (b,-b)\nu'_p & (\text{if } 2\|a), \\ \sigma'_{2,\nu'_p} + (4,-4)\nu'_p - (m/2+2, m/2-2)\nu'_p - (l,-l)\nu'_p & (\text{if } 4|a). \end{cases}$$

Before proving this we remark that in the case of $N(\alpha) = 1$ it suffices to consider the case $m = 4l$.

LEMMA 9.2. *If $m = 3l$ and $N(\alpha) = 1$. Then α cannot belong to $B_m(p)$.*

Proof. Suppose $\alpha \in B_m(p)$. We may assume that $\alpha = (1, a, b)$ with $3|a$ and $l|b$. Then $a \equiv -1 \pmod{l}$.

First, suppose $p^{f/2} \equiv v \pmod{m}$. Then by Lemma 6.1, we have $f = l - 1$ and $\nu_p = \sigma^{(1)}_{l,1}$. Hence

$$\tau_l(\nu_p\alpha) = f\{(1, -l^{-1}) + (l-1)(b')\}.$$

It follows that $\chi(\tau_l(\nu_p\alpha)) \neq 0$ for any $\chi \in PC^-(3)$ since $l-1 > 2$. This is a contradiction.

Next, suppose $p^{f/2} \equiv -v \pmod{m}$. Then

$$\tau_3(\nu_p\alpha) = 2\nu'_p\{(1, -3^{-1}) + 2(a')\}.$$

Therefore

$$1 - \eta(3) + 2\eta(a') = 0,$$

which implies that $\eta(3) = \eta(a') = -1$. This implies that $\eta(a) = \eta(3a') = 1$. But this is a contradiction since $a \equiv -1 \pmod{l}$. □

Proof of Theorem 9.1. First note that $a \equiv -1 \pmod{l}$ since $1 + a + b \equiv 0 \pmod{m}$ and $l|b$. Hence either $a = 3l - 1$ or $a = l - 1$, and

$$\alpha = (1, 3l-1, l) \quad \text{or} \quad (1, l-1, 3l).$$

Moreover, we $\chi(\nu_p) = 0$ for any $\chi \in PC^-(m)$.

Case 1. Suppose $p^{f/2} \equiv u \pmod{m}$. Then by Lemma $f = l - 1$, $p \equiv 1 \pmod{4}$. In this case, we have

$$\tau_l(\nu_p\alpha) = f\{(1, -l^{-1}) + (l-1)(b')\}.$$

But, since $l - 1 \geq 4$, we have $\chi(\tau_l(\nu_p\alpha)) \neq 0$ for the character $\chi \in PC^-(4)$, which is a contradiction.

Case 2. Next, suppose $p^{f/2} \equiv -u \pmod{m}$. Then $f/2$ is odd and $p \equiv -1 \pmod{4}$. Therefore $\tau_l(\nu_p\alpha) \in D_l$. On the other hand, since $p^{f/2} \equiv 1 \pmod{l}$ and $f/2$ is odd, we have $p^i \not\equiv -1 \pmod{l}$ for any i.

Case 2-1. If $2\|a$, then

$$\tau_4(\nu_p\alpha) = 2\nu'_p(1, -2^{-1})(1, a', a').$$

Since $\chi((1, a', a')) = 1 + 2\chi(a') \neq 0$ for any $\chi \in PC^-(l)$, we have $\eta(2) = 1$. It follows that $2 \in H$. Then $(m/2 - 2, 4)\nu'_p \in D_m$. On the other hand, we have

$$\begin{aligned} \nu_p &= (1, m/2 + 1)\nu'_p \\ &= (1, m/2 + 1, m/2 + 2, -4)\nu'_p - (m/2 + 2, -4)\nu'_p \\ &= \sigma'_{2,\nu'_p} - (m/2 - 2, 4)\nu'_p. \end{aligned}$$

Moreover $\nu_p(b) = f(l, -l) \in D_m$. Therefore

$$\nu_p\alpha = \sigma'_{2,\nu'_p}(1, a) - (m/2 - 2, 4)\nu'_p(1, a) + \nu_p(b) \in B_m .$$

Case 2-2. If $4|a$, then

$$\tau_4(\nu_p\alpha) = 2\nu'_p\{(1, -2^{-1}) + 2(a')\} .$$

In this case, we have

$$1 - \eta(2) + 2\eta(a') = 0 .$$

This holds in the following two cases:

(i) $\eta(2) = -1$ and $\eta(a') = 0$.

(ii) $\eta(2) = \eta(a') = -1$.

Case (i) cannot occur. Indeed, in that case we have

$$\eta(a) = \eta(4a') = 0 ,$$

which is a contradiction since $a \equiv -1 \pmod{l}$.

In the case of (ii), we have $-2 \in H$ and $\eta(4a') = -1$. Hence $\eta(a) = -1$, and so $(1, a)\nu_p = (1, -4)\nu_p$. Therefore

$$\begin{aligned} \nu_p(1, a) &= (1, m/2 + 1)(1, -4)\nu'_p \\ &= (1, m/2 + 1, -4, -4)\nu'_p \\ &= (1, m/2 + 1, m/2 + 2, -4)\nu'_p + (-4, m/2 - 2)\nu'_p - (m/2 + 2, m/2 - 2)\nu'_p \\ &\in B_m \end{aligned}$$

Consequently

$$\nu_p\alpha = \sigma'_{2,\nu'_p} + (4, -4)\nu'_p - (m/2 + 2, m/2 - 2)\nu'_p - (l, -l)\nu'_p .$$

This completes the proof. □

References

[1] Akiyama, S., On the pure Jacobi sums, Acta Arith., **LXXV.2** (1996), 97–104.

[2] Aoki, N., On some arithmetic problems related to the Hodge cycles on the Fermat varieties, Math. Ann., **266** (1983), 23–54. (Erratum: Math. Ann. **267** (1984), p. 572.)

[3] Aoki, N., Simple factors of the jacobian of a Fermat curve and the Picard number of a product of Fermat curves, Amer. J. Math., **113** (1991), 779–833.

[4] Aoki, N., Abelian fields generated by a Jacobi sum, Comm. Math. Univ. Sancti Pauli, **45** (1996), 1–21.

[5] Aoki, N., On the purity problem of Gauss sums and Jacobi sums over finite fields, Comm. Math. Univ. Sancti Pauli, **46** (1997), 223–233.

[6] Aoki, N., Some remarks on the Hodge conjecture for abelian varieties of Fermat type, Comm. Math. Univ. Sancti Pauli, **49** (2000), 177–194.

[7] Aoki, N., A finiteness theorem for pure Gauss sums, Comm. Math. Univ. Sancti Pauli, **53** (2004), 145–168.

[8] Aoki, N., On the solvability of a certain linear Diophantine equation with a parity condition, Comm. Math. Univ. Sancti Pauli, **56** (2007), 71–96.

[9] Berndt, B. C., Evans, R. J. and Williams, K. S., Gauss and Jacobi Sums, Wiley-Interscience, N.Y., 1998.

[10] Chowla. S., On Gaussian sums, Narske Vid. Selsk. Forh. (Trendheim), **35** (1962), 66–67.

[11] Chowla. S., On Gaussian sums, Proc. Nat. Acad. Sci., **48** (1962), 1127–1128.

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

[13] Coleman, R. F., Torsion points on abelian étale covering of $\mathbb{P}^1 - \{0, 1, \infty\}$, Trans. Amer. Math. Soc., **311** (1989), 185–208.

[14] Evans, R. J., Pure Gauss sums over finite fields, Mathmatika, **28** (1981), 239–248.

[15] Gouvêa, F. Q. and Yui, N., *Arithmetic of Diagonal Hypersurfaces over Finite Fields*, LMS Lect. Note Series **209** 1995.

[16] Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag 1993.

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

[18] Joly, J. R., Nombre de solutions de certaines équations diagonales sur un corps fini, C. R. Acad. Sci. Paris, Ser. A-B, **272** (1971), 1549–1552.

[19] Kubert, D. S. and Lang, S., Independence of modular units, Math. Ann., **240** (1979), 191–201.

[20] Lidl, R. and Niederreiter, H., Finite fields, Encyclopedia of Mathematics and Its Applications, **20**, Addison-Wesley, 1983.

[21] Mordell, L. J., On a cyclotomic resolvent, Arch. Math., **13** (1962), 486–487.

[22] Schmidt, W. M., Equations over finite fields, Lecture Notes in Mathematics, **536**, Springer-Verlag 1976.

[23] Stickelberger, L., Über eine Verallgemeinerung der Kreistheilung, Math. Ann., **37** (1890), 321–367.

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

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

[26] Shioda, T., Algebraic cycles on abelian varieties of Fermat type, Math. Ann., **258** (1981), 65–80.

[27] Shioda, T., What is known about the Hodge conjecture?, Adv. St. in Pure Math., **1** (1983), 55–68.

[28] Shioda, T. and Katsura, T., On Fermat varieties, Tôhoku Math. J., **31** (1979), 97–115.

[29] Washington, L. C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, **83**, Springer-Verlag 1982.

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

[31] Yamamoto, K., The gap group of multiplicative relationship of Gauss sums, Symp. Math., **XV** (1975), 427–440.

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Toshima-ku
Tokyo 171–8501, Japan
e-mail: aoki@rkmath.rikkyo.ac.jp