Simple factors of the jacobian of a Fermat curve

and

the Picard number of a product of Fermat curves

by

Noboru Aoki

Max-Planck-Institut für Mathematik
Gottfried-Claren-Strasse 26
5300 Bonn 3, West Germany

and

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

MPI/89-82

Simple factors of the jacobian of a Fermat curve

and

the Picard number of a product of Fermat curves

by

Noboru AOKI

§0. Introduction

For any integer $m > 1$, let X_m^1 be the Fermat curve over the complex number field $\mathbf{C}$ defined by

$$x^m + y^m + z^m = 0.$$

The jacobian variety $J(X_m^1)$ of X_m^1 decomposes up to isogeny into a product of some smaller abelian varieties. To be more precise, let

$$\mathfrak{A}_m^1 = \{(a,b,c) \mid a,b,c \in \mathbf{Z}/m\mathbf{Z} \setminus \{0\}, a+b+c=0\}.$$

The group $(\mathbf{Z}/m\mathbf{Z})^\times$ acts on $\mathfrak{A}_m^1$ by $t \cdot (a,b,c) = (ta,tb,tc),\ t \in (\mathbf{Z}/m\mathbf{Z})^\times$, and we denote by $\mathfrak{S}_m$ the orbit space $(\mathbf{Z}/m\mathbf{Z})^\times \backslash \mathfrak{A}_m^1$. Then we have an isogeny

$$\pi : J(X_m^1) \longrightarrow \prod_{S \in \mathfrak{S}_m} A_S,$$

where A_S is an abelian variety of CM type in the sense of Shimura and Taniyama (see Theorem 1.3). In general, A_S is not always simple and it may happen that A_S and $A_{S'}$ are isogenuous for two distinct orbits S and S'. Thus there arise the following two natural questions:

(Q1) When are A_S and $A_{S'}$ isogenuous over $\mathbf{C}$?

(Q2) When is A_S absolutely simple?

In [**K-R**] Koblitz and Rohrlich gave the answer to these questions in three typical cases: (i) $gcd(m,6) = 1$ (see Theorem 1.8), (ii) $m = 2^n$ and (iii) $m = 3^n$. In this paper we give an almost complete answer to (Q1) and (Q2). To state our results, we introduce some notation. We denote by $[\alpha]$ the orbit of $\alpha \in \mathfrak{A}_m^1$. If $\alpha = (a, b, c), \alpha' = (a', b', c') \in \mathfrak{A}_m^1$ and $\{a, b, c\} = \{ta', tb', tc'\}$ for some $t \in (\mathbf{Z}/m\mathbf{Z})^\times$, we say that α is equivalent to α'. From the definition of A_S one can easily see that $A_{[\alpha]}$ is isomorphic to $A_{[\alpha']}$ if α is equivalent to α'. A result of Koblitz and Rohrlich (see Theorem 1.8) implies that the converse is true if m is prime to 6.

For any $a \in \mathbf{Z}/m\mathbf{Z}$, we donote by $\langle \frac{a}{m} \rangle$ the rational number such that $0 \leq \langle \frac{a}{m} \rangle < 1$ and $m\langle \frac{a}{m} \rangle \equiv a \pmod{m}$. We introduce the following set:

$$\mathfrak{B}_m^4 = \{\alpha = (a_0, ..., a_5) \in (\mathbf{Z}/m\mathbf{Z} \setminus \{0\})^6 \mid |t \cdot \alpha| = 3 \text{ for any } t \in (\mathbf{Z}/m\mathbf{Z})^\times\},$$

where $|t \cdot \alpha| = \langle \frac{ta_0}{m} \rangle + ... + \langle \frac{ta_5}{m} \rangle$. For any $\alpha = (a, b, c), \alpha' = (a', b', c') \in \mathfrak{A}_m^1$, put $\alpha * \alpha' = (a, b, c, a', b', c')$ and $-\alpha = (-a, -b, -c)$. Then it is known that A_S and $A_{S'}$ are isogenuous if and only if $\alpha * (-\alpha') \in \mathfrak{B}_m^4$ for some $\alpha \in S, \alpha' \in S'$ (see Proposition 1.4). To describe a decomposition of A_S into simple factors, we define a subgroup W_α of $(\mathbf{Z}/m\mathbf{Z})^\times$ by

$$W_\alpha = \{t \in (\mathbf{Z}/m\mathbf{Z})^\times \mid \alpha * (-t \cdot \alpha) \in \mathfrak{B}_m^4\}.$$

Then it is known that A_S is isogenuous to the product of $\sharp W_\alpha$ copies of a simple abelian variety (see Corollarly 1.7). Now let $\mathcal{E}$ be a finite set of nutural numbers defined by

$$\mathcal{E} = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30,$$
$$36, 39, 40, 42, 48, 54, 60, 66, 72, 78, 84, 90, 120, 156, 180\}.$$

If $a_1, ..., a_n$ are any elements of $\mathbf{Z}/m\mathbf{Z} \setminus \{0\}$, we denote by $GCD(a_1, ..., a_n)$ the greatest common divisor $GCD(\tilde{a}_1, ..., \tilde{a}_n, m)$, where $\tilde{a}_i$ is any positive integer such that $\tilde{a}_i \equiv a_i \pmod{m}$. Then the following theorem gives the answer to (Q1).

Theorem0.1. *Suppose $m \notin \mathcal{E}$ and let α, β be two elements of $\mathfrak{A}^1_m$. We assume that $GCD(\alpha, \beta) = 1$ and α is not equivalent to β. Then $A_{[\alpha]}$ and $A_{[\beta]}$ are isogenous if and only if α and β are equivalent to elements in one of the following three groups.*

(1) $(a, 3a, -4a),\ (\frac{m}{2} - a, \frac{m}{2} - 2a, 3a)$

(2) $(a, 2a, -3a),\ (\frac{m}{3} - a, \frac{2m}{3} - a, 2a)$

(3) $(a, a, -2a),\ (a, \frac{m}{2} - a, \frac{m}{2}),\ (\frac{m}{2} - a, \frac{m}{2} - a, 2a),\ (\frac{a}{2}, \frac{m}{2} + \frac{a}{2}, \frac{m}{2} - a),$
$(\frac{m-2a}{4}, \frac{3m-2a}{4}, a),$

where the fourth and fifth elements in (3) are defined only when $a \equiv 0 \pmod 2$ and $2a \equiv m \pmod 4$, respectively.

To state the answer to (Q2) we define five types for elements $\alpha \in \mathfrak{A}^1_m$ with $GCD(\alpha) = 1$ as follows.

$TypeI$: elements of $\mathfrak{A}^1_m$ which are not of the following types.

$TypeII-1$: elements of $\mathfrak{A}^1_m$ which are equivalent to $(1, w, -1-w)$ with $w^2 = 1$, $w \neq \pm 1$, and $w \neq \frac{m}{2} + 1$ if $ord_2 m \geq 3$.

$TypeII-2$: elements of $\mathfrak{A}^1_m$ which are equivalnt to $(1, 1, -2), ord_2 m \geq 2$.

$TypeII-3$: elements of $\mathfrak{A}^1_m$ which are equivalnt to $(1, \frac{m}{2} + 1, \frac{m}{2} - 2), ord_2 m \geq 3$.

$TypeIII$: elements of $\mathfrak{A}^1_m$ which are equivalnt to $(1, w, w^2), 1 + w + w^2 = 0$.

Theorem 0.2. *Suppose $m \notin \mathcal{E}$ and $\alpha \in \mathfrak{A}^1_m, GCD(\alpha) = 1$. Then W_α is given as follows.*

(i) $W_\alpha = \{1\}$ *if α is of Type I.*

(ii) $W_\alpha = \{1, w\}$ *if α is of Type II-1.*

(iii) $W_\alpha = \{1, \frac{m}{2} - 1\}$ *if* α *is of Type II-2.*

(iv) $W_\alpha = \{1, \frac{m}{4} - 1, \frac{m}{2} + 1, \frac{3m}{4} - 1\}$ *if* α *is of Type II-3.*

(v) $W_\alpha = \{1, w, w^2\}$ *if* α *is of Type III.*

In particular, $A_{[\alpha]}$ *is simple if and only if* α *is of Type I.*

We have seen that the problem can be reduced to the study of the structure of $\mathfrak{B}^4_m \cap (\mathfrak{A}^1_m * \mathfrak{A}^1_m)$. The large part of this paper will be devoted to the proof the following theorem from which one can easily deduce above two theorems.

Theorem 0.3. *Suppose* $m \notin \mathcal{E}$ *and* $\alpha \in \mathfrak{B}^4_m \cap (\mathfrak{A}^1_m * \mathfrak{A}^1_m)$ *with* $GCD(\alpha) = 1$. *Then* α *is equal (up to permutation) to one of the following elements:*

(1) $(a, b, c) * (-a, -b, -c)$

(2) $(a, a, -2a) * (-a, \frac{m}{2} + a, \frac{m}{2})$

(3) $(a, a, -2a) * (\frac{m}{2} + a, \frac{m}{2} + a, -2a)$

(4) $(a, \frac{m}{2} + a, \frac{m}{2} - 2a) * (-2a, \frac{m}{2} + 2a, \frac{m}{2})$

(5) $(a, \frac{m}{2} + a, \frac{m}{2} - 2a) * (\frac{m}{2} + 2a, \frac{m}{2} + 2a, -4a)$

(6) $(a, \frac{m}{2} + a, \frac{m}{2} - 2a) * (-2a, -2a, 4a)$

(7) $(a, \frac{m}{2} + a, \frac{m}{2} - 2a) * (\frac{m}{4} + a, \frac{3m}{4} + a, -2a)$

(8) $(a, 3a, -4a) * (\frac{m}{2} + a, \frac{m}{2} + 2a, -3a)$

(9) $(a, 2a, -3a) * (\frac{m}{3} + a, \frac{2m}{3} + a, -2a)$

These problems are related to the calculation of the Picard number $\rho(X^1_m \times X^1_m)$ of the surface $X^1_m \times X^1_m$. In a letter to Shioda, Zagier computed it for $m \le 110$ using the following relation due to Shioda:

$$X^1_m \times X^1_m = 2 + \sharp\{\mathfrak{B}^4_m \cap (\mathfrak{A}^1_m * \mathfrak{A}^1_m)\}. \tag{0.1}$$

He has conjectured Theorem 0.1 and the closed formula for $\rho(X_m^1 \times X_m^1)$. Using Theorem 0.3, we can prove the Picard number formula:

Theorem 0.4. *The Picard number of $X_m^1 \times X_m^1$ is given by*

$$\rho(X_m^1 \times X_m^1) = 6m^2 - 27m + 23 \\ + \begin{cases} 0 & (2 \nmid m) \\ 189m + 9 & (2 \| m) \\ 207m + 9 & (4 | m) \end{cases} + \begin{cases} 0 & (3 \nmid m) \\ 72m + 8 & (3 | m) \end{cases} + \sum_{\substack{d|m \\ d \in \mathcal{E}}} \Delta(d),$$

where $\Delta(d)$ is the values calculated in Table II of section 8.

The present paper is organized as follows. In section 1 we review some basic results on $J(X_m^1)$, and in section 2 we prepare some basic tools for the proof of Theorem 0.3. Section 3 is a preliminary section for the later sections. Section 4, 5 and 6 are devoted to the proof of Theorem 0.3. The proofs of Theorem 0.1, 0.2 and 0.4 are given in section 7. In section 8 we discuss three topics; (i) the defining field of the isogeny from A_S to the product of simple abelian varieties, (ii) ordinary primes for A_S and (iii) the Hodge conjecture for four dimensional Fermat varieties. In the last section we give the list of elements of $\mathfrak{A}_m^1, m \notin \mathcal{E}$ that give the same "CM-type".

I would like to thank Professor T.Shioda for helping and encouraging me during the course of this work. I also thank Professor R.Coleman for his useful comments.

§1. The jacobian variety of a Fermat curve.

In this section we recall some basic results on the jacobian variety of a Fermat curve. First let us define the Fermat variety X^n_m of dimension n and degree m as a hypersurface in $\mathbb{P}^{n+1}_{/\mathbb{C}}$ defined by

$$x_0^m + x_1^m + \dots + x_{n+1}^m = 0.$$

For the detail of Fermat varieties, see [S-K] or [Sh1]. Let μ_m be the group of m-th root of unity. Then $G^n_m = (\mu_m)^{n+2}/\text{diagonal}$ acts on X^n_m coordinatewise: $g = (\zeta_0, \dots, \zeta_{n+1}) : (x_0, \dots, x_{n+1}) \longrightarrow (\zeta_0 x_0, \dots, \zeta_{n+1}x_{n+1})$. This makes the cohomology groups $H^n(X^n_m, \mathbb{Q})$ and $H^n(X^n_m, \mathbb{C})$ into G^n_m-modules. The character group of G^n_m is identified with the following group

$$\hat{G}^n_m = \{ (a_0, \dots, a_{n+1}) \mid a_i \in \mathbb{Z}/m\mathbb{Z},\ a_0 + \dots + a_{n+1} = 0 \},$$

via $\alpha(g) = \zeta_0^{a_0} \dots \zeta_{n+1}^{a_{n+1}}$ for $\alpha = (a_0, \dots, a_{n+1}) \in \hat{G}^n_m$ and $g = (\zeta_0 : \dots : \zeta_{n+1}) \in G^n_m$. Following Shioda we define two subsets of $\hat{G}^n_m$

$$\mathfrak{A}^n_m = \{ (a_0, \dots, a_{n+1}) \in \hat{G}^n_m \mid a_i \neq 0 \text{ for all } i \},$$

$$\mathfrak{B}^n_m = \{ \alpha \in \mathfrak{A}^n_m \mid |t \cdot \alpha| = n/2 + 1 \text{ for all } t \in (\mathbb{Z}/m\mathbb{Z})^\times \},$$

where $|t \cdot \alpha| = \langle ta_0/m \rangle + \dots + \langle ta_{n+1}/m \rangle$. Moreover, if n is even, define a subset $\mathfrak{D}^n_m$ of $\mathfrak{A}^n_m$ by

$$\mathfrak{B}^n_m = \{ \alpha \in \mathfrak{A}^n_m \mid \alpha \sim (a_0, -a_0, \ldots, a_{n/2}, -a_{n/2}) \},$$

where $\sim$ denotes the equality up to permutation.

For each $\alpha \in \hat{G}^n_m$, let

$$V(\alpha) = \{ \xi \in H^n(X^n_m, \mathbb{C}) \mid g^*(\xi) = \alpha(g)\xi \text{ for any } g \in G^n_m \}.$$

The following theorem is well known.

Theorem 1.1. *Notation being as above the following statements hold.*
(i) *Let* 0 *denote the trivial character of* G^n_m, *then*

$$H^n(X^n_m, \mathbb{C}) = V(0) \oplus \bigoplus_{\alpha \in \mathfrak{A}^n_m} V(\alpha),$$

where $\dim V(\alpha) = 1$ *for any* $\alpha \in \mathfrak{A}^n_m$, *and* $\dim V(0) = 1$ (*resp.* 0) *if* $n =$ *even* (*resp. odd*).
(ii) *Let* $H^{p,q}(X^n_m)$ *be the subspace of* $H^n_{prim}(X^n_m, \mathbb{C})$ *of Hodge type* (p,q),

$$H^{p,q}(X^n_m) = \bigoplus_{\substack{\alpha \in \mathfrak{A}^n_m \\ |\alpha| = q+1}} V(\alpha).$$

(iii) *If* n *is even, then*

$$(H^n_{prim}(X^n_m, \mathbb{Q}) \cap H^{n/2,n/2}(X^n_m)) \otimes \mathbb{C} = \bigoplus_{\alpha \in \mathfrak{B}^n_m} V(\alpha).$$

Proof. See [K], [O], [R] and [Sh1]. □

The elements of $H^n(X_m^n,\mathbb{Q})\cap H^{n/2,n/2}(X_m^n)$ are called *Hodge cycles* of middle dimension on X_m^n.

Next let us consider the jacobian variety of a Fermat curve. The following proposition is a special case of Theorem 1.1 (ii).

Corollarly 1.2. The Hodge decomposition of $H^1(X_m^1,\mathbb{C})$ is as follows:

$$H^{1,0}(X_m^1) = \bigoplus_{\substack{\alpha\in\mathfrak{A}_m^1 \\ |\alpha|=1}} V(\alpha), \qquad H^{0,1}(X_m^1) = \bigoplus_{\substack{\alpha\in\mathfrak{A}_m^1 \\ |\alpha|=2}} V(\alpha).$$

The endomorphism ring of $J(X_m^1)$ contains $\mathbb{Z}[G_m^1]$ as a subring. For every $g \in G_m^1$ we denote by g^* the induced element of $\mathrm{End}(J(X_m^1))$. For each $S \in \mathfrak{S}_m$ we choose an element $\alpha \in S$, and put $m(S) = m/\mathrm{GCD}(\alpha)$. Let

$$\pi_S = \sum_{g\in G_m^1} \mathrm{Tr}_{\mathbb{Q}(S)/\mathbb{Q}}(\alpha(g))g^* \in \mathrm{End}(J(X_m^1)),$$

where $\mathbb{Q}(S) = \mathbb{Q}(\zeta_{m(S)})$, $\zeta_{m(S)} = \exp(2\pi i/m(S))$. This definition does not depend on the choice of α. Let us define an abelian variety A_S as the image of π_S:

$$A_S = \pi_S(J(X_m^1)).$$

If $\alpha \in S$, then $\mathrm{End}(A_S)$ contains a subring isomorphic to $\mathbb{Z}[G_m^1/\mathrm{Ker}(\alpha)]$ since the action of $\mathrm{Ker}(\alpha)$ on A_S is trivial. There is an isomorphism of G_m^1-modules

$$H^1(A_S,\mathbb{C}) \cong \bigoplus_{\alpha\in S} V(\alpha).$$

For each $\alpha \in \mathfrak{A}^1_m$, put

$$H_\alpha = \{\ t\in(\mathbb{Z}/m(S)\mathbb{Z})^\times \mid |t\cdot\alpha| = 1\ \},$$

$$W_\alpha = \{\ t\in(\mathbb{Z}/m(S)\mathbb{Z})^\times \mid t\cdot H_\alpha = H_\alpha\ \}.$$

Then for an appropreate element $\alpha \in S$ we have isomorphisms

$$H^{1,0}(A_S) \cong \bigoplus_{t\in H_\alpha} V(t\cdot\alpha), \qquad H^{0,1}(A_S) \cong \bigoplus_{t\in -H_\alpha} V(\alpha).$$

This shows that H_α is the CM-type of A_S. Combining these results, we obtain the following

Theorem 1.3. *The abelian varieties* A_S*'s are defined over* $\mathbb{Q}$, *and there is an isogeny defined over* $\mathbb{Q}$

$$\pi : J(X^1_m) \longrightarrow \prod_{S\in\mathfrak{S}_m} A_S.$$

Moreover A_S *satisfies the following properties:*

(i) *The dimension of* A_S *is* $\varphi(m(S))/2$.

(ii) A_S *admits complex multiplication by* $\mathbb{Z}[\zeta_{m(S)}]$.

(iii) *The CM-type of* A_S *is given by* H_α *for some* $\alpha \in S$.

Proof. See [Sch](VI, Satz 1.2 and Satz 1.5). □

For $\alpha = (a, b, c)$ and $\alpha' = (a', b', c') \in \mathfrak{A}_m^1$, define

$$\alpha*(-\alpha') = (a, b, c, -a', -b', -c') \in \mathfrak{A}_m^4.$$

Proposition 1.4. *Let* $S, S' \in \mathfrak{S}_m$. *Then the following conditions are equivalent.*

(i) A_S *and* $A_{S'}$ *are isogenuous.*

(ii) *There exist* $\alpha \in S$ *and* $\alpha' \in S'$ *such that* $\gcd(\alpha) = \gcd(\alpha')$ *and* $\alpha*(-\alpha') \in \mathfrak{B}_m^4$.

Proof. Let α (resp. α') be an element of S (resp. S') such that H_α (resp. $H_{\alpha'}$) is the CM-type of A_S (resp. $A_{S'}$). By the theory of Shimura and Taniyama [S-T] we can see that A_S is isogenuous to $A_{S'}$ if and only if $\gcd(\alpha) = \gcd(\alpha')$ and $H_\alpha = aH_{\alpha'}$ for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. If we put $\alpha'' = a^{-1}\alpha'$, this shows that $|t\cdot\alpha| = |t\cdot\alpha''|$ for all $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ since $aH_{\alpha'} = H_{\alpha''}$. Here note that $|t\cdot\alpha''| = 3 - |t\cdot(-\alpha'')|$. Hence (i) is equivalent to the condition : $|t\cdot(\alpha*(-\alpha''))| = 3$ for all $t \in (\mathbb{Z}/m\mathbb{Z})^\times$, or equivalently $\alpha*(-\alpha'') \in \mathfrak{B}_m^4$. This proves the assertion. □

Remark 1.5. Let us introduce another proof due to Shioda which uses the inductive structure. For each $S \in \mathfrak{S}_m$, let

$$V_S = \bigoplus_{\alpha\in S} V(\alpha).$$

Let $S, S' \in \mathfrak{S}_m$ and suppose $\dim V_S = \dim V_{S'}$ (i.e. $\gcd(\alpha) = \gcd(\alpha')$

for $\alpha \in S$ and $\alpha' \in S'$). The proof proceeds as follows:

A_S and $A_{S'}$ are isogenuous.

$\Longleftrightarrow$ $V_S \otimes V_{(-S')}$ is spsnned by the classes of some algebraic cycles on $X_m^1 \times X_m^1$.

$\Longleftrightarrow$ $V(\alpha) \otimes V(-\alpha')$ is spanned by the classes of some algebraic cycles on $X_m^1 \times X_m^1$.

$\Longleftrightarrow$ $V(\alpha) \otimes V(\alpha')$ is spanned by some Hodge cycles on $X_m^1 \times X_m^1$ (since the Hodge conjecture is true for any surface).

$\Longleftrightarrow$ $V(\alpha * (-\alpha'))$ is spanned by spanned by some Hodge cycles on X_m^4 (by the inductive structure).

$\Longleftrightarrow$ $\alpha * (-\alpha') \in \mathfrak{B}_m^4$ (by Theorem 1.1 (*iii*)).

As for simplicity of an abelian variety with complex multiplicstion, we have a criterion due to Shimura and Taniyama ([S-T], Chap.II, §8). In our case it can be stated as follws:

Theorem 1.6. *Let* $S \in \mathfrak{S}_m$ *and choose* $\alpha \in S$ *so that the CM-type of* A_S *is given by* H_α. *Then* A_S *is isogenuous to the product of* $|W_\alpha|$ *copies of a simple abelian variety* B_S

(1.1) $$A_S \sim B_S \times \dots \times B_S.$$

In particular A_S *is simple if and only if* $W_\alpha = \{1\}$. *Moreover* B_S *satisfies the following properties:*

(i) $\dim B_S = \varphi(m(S))/2|W_\alpha|$.

(ii) $\mathrm{End}(B_S) \otimes \mathbb{Q} = \mathbb{Q}(\zeta_{m(S)})^{W_\alpha}$, *the fixed field of* W_α.

(iii) *The CM-type of* B_S *is* H_α/W_α.

Proof. See [K-R] or [Sch](VI, Satz 2.2). □

Corollarly 1.7. *Let the notation be as above. Then the following two conditions are equivalent.*

(i) A_S *is simple.*

(ii) $\alpha*((-t)\alpha) \in \mathfrak{B}_m^4$ *if and only if* $t \equiv 1 \pmod{m(S)}$.

Thus in order to prove Theorem 0.1 and Theorem 0.2, we must determine the structure of $\mathfrak{X}_m := \mathfrak{B}_m^4 \cap (\mathfrak{A}_m^1 * \mathfrak{A}_m^1)$. To investigate it we define the following sets:

$$(\mathfrak{A}_m^1 * \mathfrak{A}_m^1)^{dec} = \left\{ (a_1, a_2, a_3, b_1, b_2, b_3,) \in \mathfrak{A}_m^1 * \mathfrak{A}_m^1 \;\middle|\; \begin{array}{l} a_i + b_j = 0 \\ \text{for some } i,\ j \end{array} \right\},$$

$$\mathfrak{X}_m^{dec} = \mathfrak{B}_m^4 \cap (\mathfrak{A}_m^1 * \mathfrak{A}_m^1)^{dec},$$

$$\mathfrak{X}_m^{indec} = \mathfrak{X}_m \setminus \mathfrak{X}_m^{dec}.$$

We call the elements of $\mathfrak{X}_m^{dec}$ (resp. $\mathfrak{X}_m^{indec}$) *decomposable* (resp. *indecomposable*) *elements* of $\mathfrak{X}_m$.

The following theorem due to Koblitz and Rohrlich [K-R] is fundamental.

Theorem 1.8. *If* $\gcd(m,6) = 1$, *then*

$$\mathfrak{X}_m = \{ \alpha*(-\alpha') \mid \alpha \in \mathfrak{A}_m^1,\ \alpha' \sim \alpha \}.$$

§2. Some basic tools.

In this section we review some basic tools for the proof of Theorem 0.3 from our previous paper [A1]. Let m (>1) be an integer and R(m) the free abelian group generated by $\mathbb{Z}/m\mathbb{Z}\setminus\{0\}$. Then every element of R(m) is written as

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

For a, b $\in \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$, we define the product of (a) and (b) in R(m) by

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

Extending it linearly we define multiplication law in R(m), thus R(m) is a commutative ring with unit (1). If $\alpha = (a_1) + \dots + (a_r)$, we write it as $\alpha = (a_1, \dots, a_r)$. The number r will be called the *length* of α and denoted by $\ell(\alpha)$. For $r \geq 1$, define

$$R(m, r) = \{ \alpha \in R(m) \mid \alpha = (a_1, \dots, a_r) \}.$$

For the convenient we also define $R(m, 0) = \{0\}$. Let $PC^-(m)$ be the set of primitive odd Dirichlet characters on $\mathbb{Z}/m\mathbb{Z}$. For any $\chi \in PC^-(m)$ and $\alpha = \sum c_a(a) \in R(m)$, define $\chi(\alpha) = \sum c_a\chi(a)$. Moreover let

$$A(m) = \{ \alpha \in R(m) \mid \chi(\alpha) = 0 \text{ for all } \chi \in PC^-(m) \},$$

$$A(m, r) = A(m) \cap R(m, r),$$

$$A_m = \bigcup_{r>0} A(m, r).$$

Note that $PC^-(m) = \phi$ if $m = 12$ or $\mathrm{ord}_2(m) = 1$, in which case we define $A(m)$ to be $R(m)$. If $\alpha = \alpha_1 + \alpha_2$ with $\alpha_i \in A(m, r_i)$, then clearly $\alpha \in A(m, r_1+r_2)$, and we write

$$\alpha = \alpha_1 \oplus \alpha_2 \quad \in A(m, r_1)\oplus A(m, r_2).$$

Moreover let us define

$$A^{\circ}(m, r) = A(m, r) \setminus \bigcup_{0<i<r} A(m, i)\oplus A(m, r-i).$$

Now for each divisor d of m we introduce two important maps τ_d and T_d from $R(m)$ to $R(m/d)$: For $a \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$, put

$$T_d(a) = \frac{\varphi(m)}{\varphi(m/\delta)}\{\prod_{\substack{p|d/\delta \\ p\nmid m/d}} (p, -1)\}(a'),$$

where $\delta = \gcd(d, a)$ and a' is the element of $\mathbb{Z}/(m/d)\mathbb{Z}$ satisfying the following condition:

$$a' \equiv a/(\delta/\prod_{\substack{p|\delta \\ p\nmid m/d}} p) \qquad (\mathrm{mod}.\, m/d).$$

In particular $a' \equiv a \ (\mathrm{mod}.\, m/d)$ if $\gcd(\delta, m/d) = 1$. From the definition it follows that $T_1(\alpha) = \alpha$. Moreover, for $\alpha = \sum c_a(a) \in$

R(m), put

$$T_d(\alpha) = \sum c_a T(a) \in R(m/d).$$

We define *the primitive part* of $\sum c_a(a)$ to be $\sum_{\gcd(m,a)=1} c_a(a)$, and let $\tau_d(\alpha)$ be the primitive part of $T_d(\alpha)$. For example, when $\alpha = (a)$,

$$\tau_d((a)) = \begin{cases} \dfrac{\varphi(m)}{\varphi(m/\delta)}\{\prod_{\substack{p \mid d/\gcd(m,a) \\ p \nmid m/d}} (p, -1)\}(a') & \text{if } \gcd(m,a) \mid d, \\ 0 & \text{otherwise.} \end{cases}$$

In this notation the primitive part of α is $\tau_1(\alpha)$. (Note that this definition is slightly different from that of [A1].)

To understand the importance of T_d and τ_d, let us introduce the following subsets of R(m):

$$B(m) = \{ \sum c_a(a) \in R(m) \mid \sum c_a(\langle ta_i/m \rangle - 1/2) = 0 \ \forall t \in (\mathbb{Z}/m\mathbb{Z})^\times \},$$

$$B_m^n = B(m) \cap R(m, n+2),$$

$$B_m = \bigcup_{n \geq 0} B_m^n.$$

We have a natural map from $\mathfrak{A}_m^n$ to R(m, n+2), and we can easily see that the image of $\mathfrak{B}_m^n$ by this map is exactly B_m^n if n is even. The following characterization of B(m) and B_m is fundamental in this paper.

Proposition. 2.1. *The following conditions are equivalnt.*

(i) $\alpha \in B(m)$ *(resp.* B_m*).*

(ii) $\tau_d(\alpha) \in A(m/d)$ *(resp.* $A_{m/d}$*) for any divisor* d *of* m.

Proof. See [A1], Proposition 2.2. □

The map T_d is a natural one in the following sense.

Proposition 2.2. (i) *Let* d_1 *and* d_2 *be two divisors of* m *such that* $d_1 d_2 | m$. *Then, for any* $\alpha \in R(m)$, *we have*

$$T_{d_2}(T_{d_1}(\alpha)) = T_{d_1 d_2}(\alpha),$$

where in the left side T_{d_2} *is considered as a map from* $R(m/d_1)$ *to* $R(m/d_1 d_2)$.

(ii) *If* $\alpha \in B(m)$ *(resp.* B_m*), then* $T_d(\alpha) \in B(m/d)$ *(resp.* $B_{m/d}$*) for any divisor* d *of* m.

Proof. (i) It suufices to show the statement for $\alpha = (a) \in R(m, 1)$. Let $\delta_1 = \gcd(a, d_1)$ and $\delta_2 = \gcd(a/\delta_1, d_2)$. Then

$$T_{d_2}(T_{d_1}(\alpha))$$

$$= T_{d_2}\left(\frac{\varphi(m)}{\varphi(m/\delta_1)}\left(\prod_{\substack{p | d_1/\delta_1 \\ p \nmid m/d_1}} (p, -1)\right)(a')\right.$$

$$= \frac{\varphi(m)}{\varphi(m/\delta_1)}\cdot\frac{\varphi(m/d_1)}{\varphi((m/d_1)/\delta_2)}\Big(\prod_{\substack{p\mid d_1/\delta_1\\ p\nmid m/d_1}}(p,\ -1)\Big)\Big(\prod_{\substack{p\mid d_2/\delta_2\\ p\nmid m/d_1d_2}}(p,\ -1)\Big)(a'')$$

$$= \frac{\varphi(m)}{\varphi(m/\delta_1)}\cdot\frac{\varphi(m/\delta_1)}{\varphi(m/d_1\delta_2)}\Big(\prod_{\substack{p\mid d_1d_2/\delta_1\delta_2\\ p\nmid m/d_1d_2}}(p,\ -1)\Big)(a''),$$

where a' (resp. a") is an element of $\mathbf{Z}/(m/d_1)\mathbf{Z}$ (resp. $\mathbf{Z}/(m/d_1d_2)\mathbf{Z}$) such that

$$a' \equiv a/\delta_1' \pmod{m/d_1} \quad (\text{resp. } a'' \equiv a'/\delta_2' \pmod{m/d_1d_2}),$$

where

$$\delta_1' = \delta_1/\prod_{\substack{p\mid\delta_1\\ p\nmid m/d_1}} p \qquad (\text{resp. } \delta_2' = \delta_2/\prod_{\substack{p\mid\delta_2\\ p\nmid m/d_1d_2}} p\ ).$$

Here note that $\delta_1\delta_2 = \gcd(a,\ d_1d_2)$ and

$$\frac{\varphi(m)}{\varphi(m/\delta_1)}\cdot\frac{\varphi(m/d_1)}{\varphi(m/d_1\delta_2)} = \frac{\varphi(m)}{\varphi(m/\delta_1\delta_2)}\cdot\frac{\varphi(m/\delta_1\delta_2)\varphi(m/d_1)}{\varphi(m/\delta_1)\varphi(m/d_1\delta_2)}.$$

We want to show the following equality:

$$(*) \qquad \frac{\varphi(m/\delta_1\delta_2)\varphi(m/d_1)}{\varphi(m/\delta_1)\varphi(m/d_1\delta_2)} = 1.$$

For that purpose put $e_p = \mathrm{ord}_p(m/d_1)$ and $f_p = \mathrm{ord}_p(m/\delta_1)$. Then $e_p \geq f_p$ for evry p since $\delta_1 | d_1$. Moreover, if $p|\delta_2$, then $e_p = f_p$. Indeed, if $e_p > f_p$, then p does not divide a/δ_1, which implies that $p \nmid \delta_2$. Therefore we obtain

$$\frac{\varphi(m/d_1)}{\varphi(m/d_1\delta_2)} = \frac{\varphi(m/\delta_1)}{\varphi(m/\delta_1\delta_2)} \quad (= \varphi(\delta_2)),$$

which is equivalent to (*). Thus we obtain

$$\begin{aligned} T_{d_2}(T_{d_1}(a)) &= \frac{\varphi(m)}{\varphi(m/\delta_1\delta_2)}\Big\{ \prod_{\substack{p|d_1d_2/\delta_1\delta_2 \\ p\nmid m/d_1d_2}} (p, -1)\Big\}(a'') \\ &= T_{d_1d_2}(a). \end{aligned}$$

(ii) Put $\alpha' = T_d(\alpha) \in R(m')$, where $m' = m/d$. For any divisor d' of m' and any $\chi \in PC^-(m'/d')$, we have

$$\begin{aligned} \chi(\tau_{d'}(\alpha')) &= \chi(T_{d'}(\alpha')) \\ &= \chi(T_{d'}(T_d(\alpha))) \\ &= \chi(T_{dd'}(\alpha)) && \text{(by (i))} \\ &= \chi(\tau_{dd'}(\alpha)) \\ &= 0 && \text{(since } \alpha \in B(m)). \end{aligned}$$

This shows that $\alpha' \in B(m')$. □

For any $a \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$, the element (a, -a) of R(m, 2) belongs to

B_m^0. Therefore $(a_0, -a_0, \dots, a_r, -a_r)$ is an element of B_m^{2r} for any $a_i \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\}$. Moreover, if m is even, the element $(a_0, -a_0, \dots, a_r, -a_r, m/2)$ belongs to B_m^{2r+1}. Let us define the following subsets:

$D(m)$ = the subgroup of the abelian group $R(m)$ generated by $(a, -a)$ $(a \in \mathbb{Z}/m\mathbb{Z}\setminus\{0\})$ (and $(m/2)$ if m is even),

$$D_m^n = D(m) \cap R(m, n+2),$$

$$D_m = \bigcup_{n\geq 0} D_m^n.$$

Then it is easy to see that D_m^n corresponds to $\mathfrak{D}_m^n$ when n is even.

Let p be a prime factor of m. For any $a \in \mathbb{Z}/m\mathbb{Z}$ with $pa \neq 0$, put

$$\sigma_{p,a} = \begin{cases} (a, \frac{m}{p}+a, \dots, \frac{(p-1)m}{p}+a, -pa) & \text{if } p > 2, \\ (a, \frac{m}{2}+a, -2a, \frac{m}{2}) & \text{if } p = 2. \end{cases}$$

Then $\sigma_{p,a}$ belongs to B_m^{p-1} if $p > 2$, and $\sigma_{2,a}$ belngs to B_m^2. These are called *standard elements*. (See [A1] and [K-O].)

The proof of Theorem 0.3 is elementary but rather long. One of the reason lies in the fact that there may exist some $t(\neq 1) \in (\mathbb{Z}/m\mathbb{Z})^\times$ suth that $\chi(t) = 1$ for any $\chi \in PC^-(m)$. To be more precise, let

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

Then the following proposition holds.

Proposition 2.3. *Assume* $\mathrm{ord}_2(m) \neq 1$ *and* $m \neq 12$. *Then, for* $m \neq 15, 20$, *we have*

$$U(m) = \begin{cases} \{1\} & \text{if } 2\nmid m \text{ and } \mathrm{ord}_3(m) \neq 1, \\ \{1,\ u\} & \text{if } 2\mid m \text{ and } \mathrm{ord}_3(m) \neq 1, \\ \{1,\ v\} & \text{if } 2\nmid m \text{ and } \mathrm{ord}_3(m) = 1, \\ \{1,\ u,\ v,\ uv\} & \text{if } 2\mid m \text{ and } \mathrm{ord}_3(m) = 1, \end{cases}$$

where $u = m/2 - 1$ *and* v *is characterized by the condition* $v \equiv 1$ $(\mathrm{mod.}3)$, $\equiv -1$ $(\mathrm{mod.}m/3)$. *Moreover*

$$U(15) = \langle 2 \rangle = \{1,\ 2,\ 4,\ 8\},$$

$$U(20) = \langle 3 \rangle = \{1,\ 3,\ 7,\ 9\}.$$

Proof. See [A1], Proposition 6.1. □

Let $\alpha = (a_1, \ldots, a_r)$ and $\beta = (b_1, \ldots, b_r)$ be two elements of $R(m, r)$. If $a_i = u_i b_i$ with $u_i \in U(m)$ for all i, we write $\alpha \overset{U}{=} \beta$. In particular this implies that $\chi(\alpha) = \chi(\beta)$ for all $\chi \in PC^-(m)$. When $\alpha \overset{U}{=}$ (the primitive part of $\sigma_{p,a}$) for some p and a, we call α *p-quasi-standard element* and will be abbreviated by p-q.s..

Proposition 2.4. *Suppose* $m \neq 21$ *and* 28. *If* $\alpha \in A^0(m,3)$, *then* $\mathrm{ord}_3(m) > 1$ *and* α *is 3-quasi-standard, that is, for some* $a \in (\mathbb{Z}/m\mathbb{Z})^\times$

$$\alpha \overset{U}{=} (a,\ \tfrac{m}{3}+a,\ \tfrac{2m}{3}+a).$$

Proof. See [A1], Proposition 8.1. □

Proposition 2.5. *Suppose* $m \neq 15, 20, 27$ *and* 28. *If* $\alpha \in A(m,4)$, *then it is 5-quasi-standard* ($\mathrm{ord}_5(m) = 1$) *or* $\alpha \in A(m,2) \oplus A(m,2)$.

Proof. See [A1], Proposition 8.2. □

Proposition 2.6. *Suppose* $m \neq 15, 20, 27$ *and* 28. *Let* $\alpha \in R(m,2)$ *and suppose that* $(1, x)\alpha \in A(m)$ *with some* $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ *such that neither* $-x$ *nor* $-x^2$ *belongs to* $U(m)$. *Then* $\alpha \in A(m,2)$.

Proof. See [A1], Lemma 8.6. □

In the proof of Theorem 0.3, we will use the following result on the strucure of $\mathcal{B}_m^2$ which has been determined in [A1], [M-N] and [Sh3].

Theorem 2.7. *Assume* $m \neq 12, 14, 15, 18, 20, 21, 24, 28, 30, 36, 40, 42, 48, 60, 66, 72, 78, 84, 90, 120, 156, 180$. *Then every element of* $\mathcal{B}_m^2$ *with* $\gcd(\alpha) = 1$ *is equal to one of the following elements:*

(1) $(a, -a, b, -b)$

(2) $(a, \frac{m}{2}+a, -2a, \frac{m}{2})$

(3) $(a, \frac{m}{2}+a, \frac{m}{2}+2a, -4a)$

(4) $(a, \frac{m}{3}+a, \frac{2m}{3}+a, -3a)$

Now we define some notations which will be used later. Let $\alpha = (a_1, \dots, a_r) \in R(m,r)$. For each divisor d of m, let us define the d-part of α by

$$\alpha_d = \sum_{\gcd(m,a_i)=d} (a_i),$$

where the summation is taken over i's such that $\gcd(m,a_i) = d$. We define $N_d(\alpha)$ and $N_{(d)}(\alpha)$ as follows:

$$N_d(\alpha) = \ell(\alpha_d),$$

$$N_{(d)}(\alpha) = \sum_{d' \equiv 0 (\text{mod}.d)} N_{d'}(\alpha),$$

Moreover put

$$D(\alpha) = \min_{1 \leq i \leq r} \{ \gcd(m,a_i) \}.$$

An element α of $R(m,r)$ will be called *reduced* if it cannot expressed as $\alpha = \alpha' + \alpha''$ for any $\alpha' \in R(m,r')$ and $\alpha'' \in A(m,r'')$ with r', $r'' < r$.

§3. **Some fundamental lemmas.**

In this section we prove some fundamental lemmas which will be used in the later sections. Throughout this section we always assume that m is an odd integer. For any divisor d of m with $\gcd(d,m/d) = 1$, let us define the following subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$.

$$V_1(d) = \{ x \in (\mathbb{Z}/m\mathbb{Z})^\times \mid x^2 \equiv 1 \ (\mathrm{mod}.d) \},$$
$$V_2(d) = \{ x \in (\mathbb{Z}/m\mathbb{Z})^\times \mid x^{\kappa_p} \equiv 1 \ (\mathrm{mod}.p^{e_p}) \text{ for } {}^\forall p|d \},$$

where $e_p = \mathrm{ord}_p(m)$ and κ_p is defined by

$$\kappa_p = \begin{cases} p-1 & \text{if } p\| d \\ 2p & \text{if } p^2 | d \end{cases}.$$

For each integer $r \geq 2$, let

$$V(m,r) = V_1(m_1) \cap V_2(m),$$

where m_1 is a divisor of m defined as follows:

$$m_1 = \begin{cases} \displaystyle\prod_{\substack{p>r(\text{if } p^2|m) \\ p>r+1(\text{if } p\|m)}} p^{e_p} & \text{if } m \neq 3p,\ (p\geq 5), \\ 1 & \text{if } m = 3p,\ (5\leq p\leq 2r+1), \\ m & \text{if } m = 3p,\ (p>2r+1). \end{cases}$$

Lemma 3.1. *If* $\alpha = (a_1, \dots, a_r) \in A(m,r)$ *and* $a_i/a_j \notin V(m,r)$ *for some* i *and* j, *then* α *cannot belong to* $A^0(m,r)$.

Proof. It suffices to show the lemma for $\alpha = (1, x, \dots)$ with $x \notin V(m,r)$. If $\alpha \in A^0(m,r)$, then $x \in V_2(m)$ by [1], Corollarly 3.4. Moreover Proposition 6.4 and 6.5 [loc.cit.] implies that $x \in V_1(m_1)$. Therefore $x \in V(m,r)$, which is a contradiction. □

Corollarly 3.2. *Suppose* m *is odd. For* $\alpha \in A(m,r)$ *put* $V = V(m,r)$ *and* $f = [\langle 2\rangle V : V]$. *If we write* $\alpha = \alpha_0 + (2)\alpha_1 + \dots + (2^{f-1})\alpha_{f-1} + \alpha'$ *with* $\alpha_i \in \mathbb{Z}[V]$ *and* $\alpha' \in R(m)\setminus \mathbb{Z}[V]$, *then* $\alpha_i \in A(m)$ *for all* $i = 0, \dots, f-1$.

Lemma 3.3. *Suppose* m *is odd and* $m \neq 21$. *For* $\alpha, \beta \in R(m)$ *put* $V = V(m, 2\ell(\alpha)+\ell(\beta))$, $\ell = \ell(\alpha)$ *and* $f = [\langle 2\rangle V : V]$. *If* $\ell < 2f$, $\ell(\beta) \le 1$ *and* $(2,-1)\alpha + \beta \in A(m)$, *then the following statements hold.*

(i) *If* $\beta = 0$ *and* $\alpha \notin A(m)$, *then* $2^f \in U(m)$. *Moreover, if* $\ell \le f$, *then* $\ell = f$ *and*

$$\alpha \overset{U}{=} (a)(1, 2, 2^2, \dots, 2^{\ell-1}).$$

(ii) *If* $\ell(\beta) = 1$, *then* $\mathrm{ord}_3(m) > 1$ *and* $2^f \equiv -1 \pmod{m/3}$. *Moreover, if* $\ell \le f$, *then*

$$\alpha = (a)(1, 2, 2^2, \dots, 2^{\ell-1}), \quad \beta = (-2^{2\ell}a).$$

Proof. In order to prove the lemma we may assume that both α and β are reduced and that they are of the following forms:

$$\alpha = \alpha_0 + (2)\alpha_1 + \dots + (2^{f-1})\alpha_{f-1},$$
$$\beta = \beta_0 + (2)\beta_1 + \dots + (2^{f-1})\beta_{f-1}.$$

with α_i, $\beta_i \in Z[V]$. In paticular α_i(resp. β_i) $\notin A(m)$ whenever α_i (resp. β_i) $\neq 0$. Then

$$(2, -1)\alpha + \beta$$
$$= (2^f)\alpha_{f-1} + (-1)\alpha_0 + \beta_0 + \sum_{i=1}^{f-1}(2^i)\{\alpha_{i-1} + (-1)\alpha_i + \beta_i\},$$

and by Corollarly 3.2 we obtain

(3.1) $\quad (2^f)\alpha_{f-1} + (-1)\alpha_0 + \beta_0 \in A(m),$

(3.2) $\quad \alpha_{i-1} + (-1)\alpha_i + \beta_i \in A(m),\ i = 1, \dots, f-1.$

(i) If $\beta = 0$, then from (3.1) and (3.2) we obtain

(3.3) $\quad \alpha_0 \equiv \alpha_1 \equiv \dots \equiv \alpha_{f-1} \pmod{A(m)},$

(3.4) $\quad (2^f, -1)\alpha_i \in A(m)$ for $0 \leq i \leq f-1.$

If $\alpha_i \in A(m)$ for some i, then $\alpha_i \in A(m)$ for all i by (3.3), which is a contradiction. Therefore $\ell(\alpha_i) > 0$ for all i. Since $\ell < 2f$, this implies that $\ell(\alpha_i) = 1$ for some i, hence (3.4) implies that $2^f \in U(m)$. Now suppose $\ell \leq f$. Then (3.4) implies that $2^f \in U(m)$. The above argument shows that $\ell = f$ and $\ell(\alpha_i) = 1$ for all i, say $\alpha_i = (a_i)$.

Then (3.3) implies that $a_i \in (a_0)U(m)$ for all i, which proves (i).
(ii) If $\ell(\beta) = 1$, say $\beta = \beta_0 = (b)$ and $\beta_1 = \dots = \beta_{f-1} = 0$, then from (3.1) and (3.2) we obtain

(3.5) $\alpha_i \equiv \alpha_0 \pmod{A(m)}$ for $1 \le i \le f-1$,

(3.6) $(2^f, -1)\alpha_i + (b) \in A(m)$ for all i.

If $\alpha_i \in A(m)$ for some i, then $\alpha_0 \in A(m)$ by (3.5), and so $(b) \in A(m)$ by (3.6), which is impossible. Thus none of α_i's belongs to A(m), which implies $\ell(\alpha_i) \ge 1$ for all i. Since $\ell < 2f$, this shows that $\ell(\alpha_i) = 1$ for some i. It follows from this and Proposition 2.4 that $ord_3(m) > 1$ and $2^f \equiv -1$ (mod.m/3). If $\ell \le f$, then $\ell(\alpha_i) = 1$ for all i, say $\alpha_i = (a_i)$. Hence (3.5) and (3.6) implies that $a_i \in a_0U(m)$ and $(2^f, -1)(a_0) + (b) \in A(m)$. Therefore $b = -2^{2\ell}a_0$ by Proposition 2.4, which proves (ii). □

Corollarly 3.4. *Suppose* m *is odd and* m > 51. *Let* α *be an element of* R(m, ℓ) *with* $\ell \le 4$. *Then the following statements hold.*

(i) *If* $(2, -1)\alpha \in A(m)$, *then* $\alpha \in A(m)$.

(ii) *Assume, in addition,* $m \ne 225$ *if* $\ell(\alpha) = 3$ *or* 4. *Then* $(2, -1)\alpha + (b) \notin A(m)$ *for any* $b \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. If $m \ne 225$, the condition imposed on m insure that $2f > \ell(\alpha)$ and $2^f \notin U(m)$, and that $2^f \not\equiv -1$ (mod.m/3) if $ord_3(m) > 1$. Thus the assertion immediately follows from Lemma 3.1 when $m \ne 225$. If m =

225, $\chi(2) \neq 1$ for any $\chi \in PC^-(225)$. Therefore $(2, -1)\alpha \in A(225)$ if and only if $\alpha \in A(225)$, which proves (i) when $m = 225$. □

Lemma 3.5. *Suppose* m *is odd and does not divide* 105, $3p$ ($p \le 17$). *Let* α *and* β *be reduced elements of* $R(m)$ *such that* $2 \le \ell(\alpha) \le 4$ *and* $\ell(\beta) = 2$. *Let* f *be as in Lemma 3.3 and assume* $\ell(\alpha) \le f$. *Then, if* $(2, -1)\alpha + \beta \in A(m)$, *the following statements hold.*

(i) *If* $\ell(\alpha) = 4$ *and* $\alpha \notin A(m)$, *then there are five cases below:*

(a) $\alpha \overset{U}{\equiv} (a,2a,4a,8a)$, $\beta \overset{U}{\equiv} (a,-16a)$,

(b) $\alpha = (a,2a,\frac{m}{3}-a,\frac{2m}{3}-a)$, $(a,\frac{m}{3}-2a,\frac{2m}{3}-2a,4a)$, $(\frac{m}{3}-a,\frac{2m}{3}-a,2a,4a)$, $\beta = (a,-8a)$,

(c) $\alpha = (\frac{m}{3}-a,\frac{2m}{3}-a,\frac{m}{3}-2a,\frac{2m}{3}-2a)$, $\beta = (a,-4a)$,

(d) $\alpha \overset{U}{\equiv} (a,-2ga,-2g^2a,-2g^3a)$, $(-ga,-g^2a,-g^3a,2a)$, $\beta \overset{U}{\equiv} (a,-4a)$.

(e) $\alpha \overset{U}{\equiv} (\frac{m}{5}-a, \frac{2m}{5}-a, \frac{3m}{5}-a, \frac{4m}{5}-a)$, $\beta \overset{U}{\equiv} (a,-2a)$.

(ii) *If* $\ell(\alpha) = 3$, *then there are three cases below:*

(a) $\alpha \overset{U}{\equiv} (a,2a,4a)$, $\beta \overset{U}{\equiv} (a,-8a)$,

(b) $\alpha = (a,\frac{m}{3}-2a,\frac{2m}{3}-2a)$, $(\frac{m}{3}-a,\frac{2m}{3}-a,2a)$, $\beta = (a,-4a)$,

(c) $\alpha \overset{U}{\equiv} (-ga, -g^2a, -g^3a)$, $\beta = (a, -2a)$.

(iii) *If* $\ell(\alpha) = 2$, *then there are tow cases below:*

(a) $\alpha \overset{U}{\equiv} (a,2a)$, $\beta \overset{U}{\equiv} (a,-4a)$,

(b) $\alpha = (\frac{m}{3}-a,\frac{2m}{3}-a)$, $\beta = (a,-2a)$.

Here g *is an element of* $(\mathbb{Z}/m\mathbb{Z})^\times$ ($ord_5(m)=1$) *such that* $g \equiv 2 \pmod{5}$,

$\equiv 1 \pmod{m/5}$.

Proof. We prove only (i) because the other cases are similar. We have only to consider the case where $\beta = (1, 2^c b)$ with $b \in V$, $1 \leq c \leq f$. First consider the case $c < f$. Then from (3.1) and (3.2) we obtain

(3.7) $\alpha_0 \equiv \dots \equiv \alpha_{c-1}, \quad \alpha_c \equiv \dots \equiv \alpha_{f-1} \pmod{A(m)}$,

(3.8) $(2^f)\alpha_{f-1} + (-1)\alpha_0 + (1) \in A(m)$,

(3.9) $\alpha_{c-1} + (-1)\alpha_c + (b) \in A(m)$.

If $\ell(\alpha_i) \geq 1$ for all i, then $f = \ell(\alpha)$ and $\ell(\alpha_i) = 1$ for all i, say $\alpha_i = (a_i)$. It then follows from (3.7) that $a_i \in a_0 U(m)$ $(1 \leq i \leq c-1)$ and $a_j \in a_c U(m)$ $(c+1 \leq j \leq f-1)$, and $(2^f a_c, -a_0, 1)$, $(a_0, -a_c, b) \in A(m)$ by (3.8) and (3.9). Then Proposition 2.4 implies that $\mathrm{ord}_3(m) > 1$ and $2^f \equiv 1 \pmod{m/3}$. But this is impossible since $m \nmid 3^2 \cdot 5$. Thus $\alpha_i = 0$ for some i. We may assume $\alpha_i = 0$ for some i with $c \leq i \leq f-1$. Then (3.7) implies that $\alpha_c = \dots = \alpha_{f-1} = 0$ since α is reduced. Moreover, for $i = 0, \dots, c-1$, from (3.8) and (3.9) we obtain

(3.10) $\alpha_i + (-1) \in A(m)$,

(3.11) $\alpha_i + (b) \in A(m)$,

This implies, in particular, that b is an element of $-U(m)$, which shows that $\beta \overset{U}{=} (1, -2^c)$. Since α is reduced, $\ell(\alpha_i) \geq 1$ for $i = 0, \dots, c-1$, hence $c \leq 4$. If $c = 4$, then $\ell(\alpha_i) = 1$, say $\alpha_i = (a_i)$. Then

(3.10) shows that $a_i \in U(m)$, hence $\alpha \overset{U}{=} (1, 2, 4, 8)$, which shows (a). If $c = 3$, then one of $\ell(\alpha_i)$ is two and the others are one. In this case we obtain (b). Indeed, for example, in case $\ell(\alpha_0) = \ell(\alpha_1) = 1$ and $\ell(\alpha_2) = 2$, it follows from Proposition 2.4 that $\mathrm{ord}_3(m) > 1$ and $\alpha \overset{U}{=} (1, 2, \frac{m}{3}-4, \frac{2m}{3}-4)$. If $c = 2$, there are three cases: $(\ell(\alpha_0), \ell(\alpha_1)) = (1,3),(2,2)$ or $(3,1)$. In the first case, say $\alpha_0 = (a_0)$, $\alpha_1 = (a_1, a_2, a_3)$. Then (3.10) and (3.11) implies that $a_0 \in U(m)$ and $(-1, a_1, a_2, a_3) \in A(m)$. Since α is reduced this implies that $\mathrm{ord}_5(m) = 1$ and $(a_1, a_2, a_3) \overset{U}{=} (-g, -g^2, -g^3)$, hence $\alpha \overset{U}{=} (1, -g, -g^2, -g^3)$. Thus we obtain (d). The third case is similar. In the second case, say $\alpha_0 = (a_0, a_1)$ and $\alpha_1 = (a_2, a_3)$. Then (3.10) implies that both $(-1, a_0, a_1)$ and $(-1, a_2, a_3)$ belong to $A(m)$, hence $\mathrm{ord}_3(m) > 1$ and $(a_0, a_1) = (a_2, a_3) = (\frac{m}{3}-1, \frac{2m}{3}-1)$. Therefore $\alpha = (\frac{m}{3}-1, \frac{2m}{3}-1, \frac{m}{3}-2, \frac{2m}{3}-2)$, which is (c). If $c = 1$, then $\alpha = \alpha_0$, and (3.10) implies that $\alpha+(-1)$ belongs to $A(m)$. Since α is reduced, $\alpha+(-1) \in A^{o}(m,5)$. Proposition 6.6 of [A1] shows that $\mathrm{ord}_5(m) > 1$ and $\alpha = (\frac{m}{5}-1, \frac{2m}{5}-1, \frac{3m}{5}-1, \frac{4m}{5}-1)$, which is (e).

Next let us consider the case $c = f$. In this case from (3.1) and (3.2) we obtain

(3.12) $\quad \alpha_0 \equiv \ldots \equiv \alpha_{f-1} \pmod{A(m)}$,

(3.13) $\quad (2^f)\alpha_{f-1} + (-1)\alpha_0 + (1, 2^f b) \in A(m)$.

Since α is reduced this implies that $f \le \ell(\alpha)$, hence $f = \ell(\alpha) = 4$ and $\ell(\alpha_i) = 1$, say $\alpha_i = (a_i)$. Then (3.12) implies that $a_i \in a_0 U(m)$ for all i and that

(3.14) $(16, -1)(a_0)+(1, 16b) \in A(m)$.

Here note that $(16, -1)$ does not belong to $A(m)$ since $m \nmid 3\cdot5, 3\cdot17$. Moreover (3.14) cannot be 5-q.s. since $m \nmid 3\cdot5\cdot7, 3\cdot17$. Therefore $(16a_0, 16b)\oplus(-a_0, 1)$ or $(16a_0, 1)\oplus(-a_0, 16b)$. In the first case we have $a_0 \in U(m)$ and $b \in -U(m)$, hence $\alpha \overset{U}{=} (1, 2, 4, 8)$ and $\beta = (1, -16)$. In the second case we have $16a_0 \in -U(m)$ and $2^8b \in -U(m)$, hence $(-16)\alpha \overset{U}{=} (1, 2, 4, 8)$ and $(-16)\beta \overset{U}{=} (1, -16)$. This proves the lemma when m does not divide $3^3\cdot7^2$. By a similar argument as above we can see that the lemma holds for m which divides $3^3\cdot7^2$. □

Lemma 3.6. *Suppose* m *is odd and does not divide* $3p$ $(p\leq17)$, 45, 63, 105. *Let* $\alpha = (2, -1)(1, a) + \beta \in A(m)$ *with* $\ell(\beta) = 3$ *or* 4. *If* $\ell(\beta) = 4$, *say* $\beta = (b_1, b_2, b_3, b_4)$, *we assume that* $1 + a + b_1 = b_2 + b_3 + b_4 = 0$. *Then the following statements hold.*

(i) *If* $\ell(\beta) = 4$, *then there are three cases below:*

(i-1) $a = 1$, $\beta = (1, 1, -2, -2)$.

(i-2) $a = -2$, $\beta = (1, -2, -2, 4)$.

(i-3) $a = -2^{-1}$, $\beta = (1, 1, -2, -2^{-1})$.

(ii) *If* $\ell(\beta) = 3$, *then there are four cases below:*

(ii-1) $a = -1$, $\beta = (b, \frac{m}{3}+b, \frac{2m}{3}+b)$.

(ii-2) $a = 2$, $\beta = (\frac{m}{3}-1, \frac{2m}{3}-1, -4), (1, \frac{m}{3}-4, \frac{2m}{3}-4)$.

(ii-3) $a = \varepsilon\frac{m}{3}-2$, $\beta = (1, \varepsilon\frac{m}{3}+2, \varepsilon\frac{m}{3}+4)$.

(ii-4) $a = \varepsilon\frac{m}{3}+1$, $\beta = (1, \varepsilon\frac{m}{3}+1, -\varepsilon\frac{m}{3}+2)$, $(-2, \varepsilon\frac{m}{3}-2, -\varepsilon\frac{m}{3}-1)$.

Here ε *denotes* 1 *or* -1.

Proof. Let $V = V(m,8)$ and $f = [\langle 2\rangle V : V]$. Let k be an integer such that $0 \le k \le f-1$ and $a \in 2^k V$.

Case 1: If $k \ne 0, \pm 1$, then $\beta \overset{U}{\cong} (-2, 1)(1, a)$.

Case 2: If $k = 1$, then

$$(2, -1)(1, a)+\beta = (2, -a)+(-1)+(2a)+\beta.$$

Therefore $\ell_1(\beta) \ge 3$. If $\ell_1(\beta) = 4$, then there are four cases:

(3.15) $(2, -a, b_2, b_3)\oplus(-1, 2a, b_1, b_4)$,

(3.16) $(2, -a, b_1)\oplus(-1, 2a, b_2, b_3, b_4)$,

(3.17) $(2, -a, b_2)\oplus(-1, 2a, b_1, b_3, b_4)$,

(3.18) $(2, -a)\oplus(-1, 2a, b_1, b_2, b_3, b_4)$.

In the first case (3.15), we have $(-1, b_1)\oplus(2a, b_4)$ or $(-1, b_4)\oplus(2a, b_1)$ because $(-1, 2a, b_1, b_4)$ cannot be 5-q.s. since $f \ge 3$. If $b_1 \in U(m)$, then $a = -2$ or $v-1$ according to the case $b_1 = 1$ or v, hence $a = -2$, $b_1 = 1$ and $b_4 \overset{U}{\cong} 4$ since $(2a, b_4) \in A(m)$. Moreover $(2, 4, b_2, b_3) \in A(m)$, hence $(b_2, b_3) \overset{U}{\cong} (-2, -4)$. But this implies that $b_2 + b_3 + b_4 \ne 0$, which is a contradiction. On the other hand, if $b_4 \in U(m)$, then $b_1 = -2a$ or $-2va$, hence $a = 1$ or $(2v-1)^{-1}$. Since $k = 1$, a must be the latter. Therefore $(2, b_2)\oplus(-(2v-1)^{-1}, b_3)$, which implies that $b_2 + b_3$

$+ b_4 \neq 0$, a contradiction. Thus the first case cannot occur. The second case (3.16) also cannot occur. In fact, if $(2, -a, b_1) \in A(m)$, then $\mathrm{ord}_3(m) > 1$ and $-a \equiv b_1 \equiv 2 \pmod{m/3}$, hence $1 + a + b_1 \neq 0$. In the third case, $\mathrm{ord}_3(m) > 1$ and $a = \varepsilon\frac{m}{3}-2$, $b_2 = -\varepsilon\frac{m}{3}+2$. The second factor belongs to $A(m,3)\oplus A(m,2)$. For example, if $(-1, b_1, b_3)\oplus(2a, b_4)$, then $b_1 = \pm\frac{m}{3}-1$. Therefore $1 + a + b_1 \neq 0$, which is a contradiction. The other cases are also impossible. Finally let us consider the last case (3.18). In this case we have $a = 2$, $b_1 = -3$, hence $(-1, 4, -3, b_2, b_3, b_4) \in A(m)$. Therefore $(b_2, b_3, b_4) = (-1, -3, 4)$.

If $\ell_1(\beta) = 3$, then

(3.19) $\quad (2, -a, b_1)\oplus(-1, b_2)\oplus(2a, b_3)$

(3.20) $\quad (2, -a)\oplus(-1, b_1, b_2)\oplus(2a, b_3)$

(3.21) $\quad (2, -a)\oplus(-1, b_1)\oplus(2a, b_2, b_3)$.

Note that $\mathrm{ord}_3(m) > 1$ in any case. From the first case (3.19) we obtain

$$a = \varepsilon\frac{m}{3}-2, \qquad \beta = (1, \varepsilon\frac{m}{3}+2, \varepsilon\frac{m}{3}+4)$$

From the second case (3.20) (resp. (3.21)) we obtain

$$a = 2, \qquad \beta = (-4, \frac{m}{3}-1, \frac{2m}{3}-1) \text{ (resp. } (1, \frac{m}{3}+4, \frac{2m}{3}+4)).$$

Case 3: $k = -1$. This case is quite similar to Case 2.

Case 4: $k = 0$. If $\ell(\beta) = 4$, then

(3.23) $(2, 2a, b_1, b_2)\oplus(-1, -a, b_3, b_4)$,

(3.24) $(2, 2a, b_2, b_3)\oplus(-1, -a, b_1, b_4)$,

(3.25) $(2, 2a, b_1)\oplus(-1, -a, b_2, b_3, b_4)$,

(3.26) $(2, 2a, b_2)\oplus(-1, -a, b_1, b_3, b_4)$,

(3.27) $(2, 2a)\oplus(-1, -a, b_1, b_2, b_3, b_4)$.

First note that $a \notin -U(m)$. Indeed, if $a \in -U(m)$, then $\gcd(m,b_1) > 1$, which is a contradiction. In particular the last case (3.27) cannot occur. In case (3.23), we obtain $(-1, b_3)\oplus(-a, b_4)$, so $b_3 \overset{U}{\equiv} 1$ and $b_4 \overset{U}{\equiv} a$. Moreover, if $(b_1, 2)\oplus(b_2, 2a)$, then $a = 1$ and $\beta = (1, 1, -2, -2)$, which is (i-1). If $(2, b_2)\oplus(2a, b_1)$, then we obtain the same result as above. In case (3.24), if $(-1, b_1) \in A(m)$, then $b_1 = 1$ and $a = -2$. Hence $\beta = (1, -2, -2, 4)$, which is (i-2). If $(-a, b_1) \in A(m)$, then $b_1 = a$. Since $1 + a + b_1 = 0$, this implies that $a = -2^{-1}$, which is a contradiction because $k = 0$ now. In case (3.25) we have $\mathrm{ord}_3(m) > 1$ and $a \equiv 1$, $b_1 \equiv 2 \pmod{m/3}$, which is impossible. In case (3.26) we have

$$(2, 2a, b_2)\oplus(b_2, 2b_1, 2b_3, 2b_4).$$

Therefore $a = \varepsilon\frac{m}{3}+1$, $b_2 = -\varepsilon\frac{m}{3}+2$ and $b_1 = -\varepsilon\frac{m}{3}-2$, hence

$$(-\varepsilon\tfrac{m}{3}+2,\ \varepsilon\tfrac{m}{3}-4,\ 2b_3,\ 2b_4) \in A(m).$$

This implies $2b_3 = \varepsilon\frac{m}{3}-2$ and $2b_4 = -\varepsilon\frac{m}{3}+4$. Then $2b_2 + 2b_3 + 2b_4 \neq 0$, hence this case also cannot occur.

If $\ell(\beta) = 3$, then

(3.28) $(2, 2a)\oplus(-1, -a, b_1, b_2, b_3)$

(3.29) $(2, 2a, b_1)\oplus(-1, -a, b_2, b_3)$

(3.30) $(2, 2a, b_1, b_2)\oplus(-1, -a, b_3)$.

In case (3.28) we have $a \in -U(m)$ and $(b_1, b_2, b_3) \in A(m)$, hence $\mathrm{ord}_3(m) > 1$, $a = -1$ and $\beta = (b, \frac{m}{3}+b, \frac{2m}{3}+b)$, which is (ii-1). From (3.29) (resp. (3.30)) we obtain $a = \varepsilon\frac{m}{3}+1$ and $\beta = (1, -\varepsilon\frac{m}{3}+1, -\varepsilon\frac{m}{3}+2)$ (resp. $(-2, \varepsilon\frac{m}{3}-1, \varepsilon\frac{m}{3}-2)$) with $\varepsilon = \pm 1$, which is (ii-4). Thus we have proved our lemma. □

§4. Proof of Theorem 0.3 (the first case).

First we define three subsets of B_m^4 which corresponds to $\mathfrak{X}_m$, $\mathfrak{X}_m^{dec}$ and $\mathfrak{X}_m^{indec}$ defined in §1:

$$X_m = \{ (a_0, \dots , a_5) \in B_m^4 \mid a_0 + a_1 + a_2 = 0 \}.$$
$$X_m^{dec} = \{ (a_0, \dots , a_5) \in X_m \mid a_i + a_j = 0 \text{ for some } i \neq j \},$$
$$X_m^{indec} = X_m \setminus X_m^{dec}.$$

The aim of this section is to prove Proposition 4.9, which treat the case where $ord_2(m) \neq 1$ and $N_1(\alpha) > 0$. For that purpose we prove some lemmas.

Lemma 4.1. *Suppose* $ord_2(m) \neq 1$ *and* $m > 60$. *Then* $N_1(\alpha) \neq 3$ *if* $\alpha \in X_m$.

Proof. Suppose $N_1(\alpha) = 3$, then by Proposition 2.4 we obtain

$$\alpha = (a, \tfrac{m}{3}+a, \tfrac{2m}{3}+a, x, y, z).$$

We may assume it decomposes as follows:

$$(a, \tfrac{m}{3}+a, \tfrac{2m}{3}-2a)+(\tfrac{2m}{3}+a, x, y)$$
$$\equiv \sigma_{3,a} + (3a, \tfrac{2m}{3}-2a, x, y) \quad (\mathrm{mod}.D_m).$$

This implies that the last term is an element of B_m^2, which is however impossible by Theorem 2.7 and Table 1 of [M-N]. □

Lemma 4.2. *Suppose* $\mathrm{ord}_2(m) \neq 1$ *and* $m > 60$. *Let* $\alpha \in X_m \setminus D_m^4$ *and suppose* $N_1(\alpha) = n > 0$. *Then* $n = 2$ *or* 4, *and* $\tau_1(\alpha) \in A(m,2)$ *or* $A(m,2) \oplus A(m,2)$.

Proof. Let $\alpha = (a_0, a_1, a_2, a_3, a_4, a_5)$. First suppose m is even, then $n \leq 4$. If $n = 2$, then the assertion is clear. Hence we may assume $n = 4$ since $n \neq 3$ by Lemma 4.1, say $\gcd(a_i, m) = 1$ for $i = 0,1,2$ and 3. Then $(a_0, a_1, a_2, a_3) \in A(m)$. If it is 5-q.s., then $a_i (\mathrm{mod.}\, m/5) \in U(m/5)$ for $i = 0,1,2$ and 3. But then $\tau_5((a_0, a_1, a_2, a_3))$ does not belong to $A(m/5)$, which is however a contradiction. Hence $(a_0, a_1, a_2, a_3) \in A(m,2) \oplus A(m,2)$. This proves the assertion when m is even.

Next consider the case m is odd. Then $\alpha \in A^0(m,\ell) \oplus A(m, 6-\ell)$, $2 \leq \ell \leq 6$. Here we choose ℓ as large as possible. Then our aim is to show $\ell = 2$. If $\ell = 6$, then by [A1], Proposition 6.4 and 6.5

$$(4.1) \qquad a_i \equiv \pm 1 \ (\mathrm{mod.}\ p^{e_p}) \ \text{ for } {}^{\forall}p \geq 7,$$

$$(4.2) \qquad a_i \equiv \pm 1 \ (\mathrm{mod.}\ p^{e_p - 1}) \ \text{ for } p = 3 \text{ and } 5.$$

But then $a_i + a_j + a_k \neq 0$ for any i, j and k unless $m \mid 45$, which is a contradiction. When $\ell = 4$ or 5, it is easy to see $\alpha \equiv \sigma_{5,a}\ (\mathrm{mod.}\, D_m)$ for some a, which is impossible since $\sigma_{5,a} \notin X_m$. Since $\ell \neq 3$ by Lemma 4.1, ℓ must be 2. Now it remains to show $n \neq 6$. Suppose $n = 6$, then the above argument shows that $\mathrm{ord}_3(m) = 1$ and α is of the following form:

$$\alpha = (1, -v)(x, y, z),$$

where $\gcd(m,x) = \gcd(m,y) = \gcd(m,z) = 1$ and either $x + y + z = 0$ or $x + y - vz = 0$. In both cases $x + y + z \equiv 0 \pmod{m/3}$ and

$$T_3(\alpha) = (3, -1)(x, y, z) \in X_{m/3}.$$

But this happens if and only if $(x, y, z) = (3x, 3y, 3z)$ by Theorem 1.8 since $\gcd(m/3,6) = 1$. This implies that $1 + 3 + 9 \equiv 0 \pmod{m/3}$, that is, m is a divisor of 39, which is impossible. □

Proposition 4.3. *Suppose that* $\mathrm{ord}_2(m)\neq 1$ *and* $m > 60$. *Let* $\alpha \in X_m^{\mathrm{indec}}$ *and suppose* $N_1(\alpha) \geq 4$. *Then* $\mathrm{ord}_2(m) > 2$ *and* $\alpha = (a, \frac{m}{2}+a, \frac{m}{2}-2a)+(\frac{m}{4}+a, \frac{3m}{4}+a, -2a)$ *for some* $a \in (\mathbb{Z}/m\mathbb{Z})^{\times}$.

Proof. By Lemma 4.1 and Lemma 4.2 it suffices to show the lemma assuming that $N_1(\alpha) = 4$ and α is of the following form:

$$\alpha = (1, -w_1)+(1, -w_2)(a)+(b, c),$$

where $w_i \in U(m)$, $\gcd(m,a) = 1$, $\gcd(m,b) > 1$ and $\gcd(m,c) > 1$. If $\mathrm{ord}_3(m) = 1$ and at least one of w_1 and w_2 is either v or uv, then it is easy to see that $\tau_3(\alpha) \equiv 2(3, -1)(a) \pmod{A(m/3)}$ if one of w_i is u, and $\tau_3(\alpha) \equiv 2(3, -1)(1, a) \pmod{A(m/3)}$ otherwise. The first case is impossible since $3 \notin U(m/3)$. (This is because $m/3 \neq 4, 8, 20$.) It follows from the second case that $a \pmod{m/3} \in -U(m/3)$, hence a =

-1, $-u$, v or uv. Since α is not decomposable, a cannot be -1, v and uv, hence $a = -u$ and $\alpha = (1, -u)(1, -v)+(b, c)$. Therefore we may assume that α is of the following form:

$$\alpha = (1, \tfrac{m}{2}+1)(1, a)+(b, c) = (1, \tfrac{m}{2}+1, a, \tfrac{m}{2}+a, b, c).$$

Then $(b, c) = (\frac{m}{2}-2, \frac{m}{2}-2a)$ or $a = \frac{m}{2}-2$. In the first case we have

$$\alpha \equiv \sigma_{2,1} + \sigma_{2,a} + (2, \tfrac{m}{2}-2, 2a, \tfrac{m}{2}-2a) \pmod{D_m},$$

which implies that the last term belongs to B_m^2. By Theorem 2.7 and the table in [M-N] we see that this is possible only if it belongs to D_m^2, hence $a = \pm\frac{m}{4}+1$ ($\mathrm{ord}_2(m) > 2$) and $\alpha = (1, \frac{m}{2}+1, \frac{m}{2}-2)+(\frac{m}{4}+1, \frac{3m}{4}+1, -2)$. In the second case we have

$$\alpha \equiv \sigma_{2,1} + (\tfrac{m}{2}, \tfrac{m}{2}-2, b, c) \pmod{D_m}.$$

Similarly as above this implies $(b, c) = (\frac{m}{4}+1, \frac{3m}{4}+1)$, hence $\alpha = (1, \frac{m}{2}+1, \frac{m}{2}-2)+(\frac{m}{4}+1, \frac{3m}{4}+1, -2)$. □

Lemma 4.4. *Suppose* $\mathrm{ord}_2(m) \neq 1$, $\mathrm{ord}_3(m) = 1$ *and* $m > 84$. *Let* α *be an element of* X_m *such that* $N_1(\alpha) = 2$, *and suppose that* $\alpha = (a, -va, x, y, z, w)$ *with* $\gcd(m,a) = 1$. *Then* α *is decomposable.*

Proof. First note that α is one of the following forms:

(4.3) $(1, -v, v-1)(a)+(x, y, z)$

(4.4) $(a, x, y)+(-va, z, w)$.

In case (4.3), we have

$$\tau_3((1,-v,v-1)(a)) = 2(3,-1)(a) \quad (\text{resp. } 2(3,-1,-2)(a))$$

if m = even (resp. odd). Since they cannot belong to $A(m/3)$, $N_3((x,y,z))$ must be positive. Then it is not hard to see that $N_{(3)}((x,y,z)) \geq 2$, and so $x \equiv y \equiv z \equiv 0$ (mod.3). If m is odd, then

$$T_3(\alpha) = 2(3a, -a, -2a, x, y, z) \in B_{m/3},$$

which implies that $\beta = (3a, -a, -2a, x, y, z) \in X_{m/3}$. Since $\gcd(m/3,6) = 1$, Theorem 1.8 shows that $\beta \in D_{m/3}$. Therefore $(x, y, z) = (-3a, -v'a, (1-v)a)$, which shows that α is decomposable. If m is even, then

$$\tau_3(\alpha) = 2(3a, -a, x, z) \in A(m/3).$$

Since m/3 is even and not equal to neither 20 nor 28, Proposition 2.5 shows that $(x, y) = (-3, -v')$, $(-3, \frac{m}{2}+v')$, $(\frac{m}{2}+3, -v')$ or $(\frac{m}{2}+3, \frac{m}{2}+v')$. In the first case α is decomposable. We can see that the other three cases are impossible. For example, in the second case, we have

$$\alpha = (1, -v, 2v', -3, \frac{m}{2}+v', \frac{m}{2}-4v')$$

$$\equiv \sigma_{3,1} + (v')(1,\ 2,\ \tfrac{m}{2}+1,\ \tfrac{m}{2}-4) \pmod{D_m},$$

which shows that the last term belongs to B_m^2. But it is impossible by Theorem 2.7. The other cases are similar.

Next consider the second case (4.4). In this case $N_{(3)}(\alpha) \le 2$. By the similar argument as above one can see that $N_{(3)}(\alpha) = 2$, say $x \equiv z \equiv 0$ (mod.3). Since $\tau_3(\alpha) \in A(m/3)$, $N_3((x,\ y,\ z,\ w)) > 1$. Then a simple calculation shows that $N_3 = 2$, say $\gcd(m,x) = \gcd(m,z) = 3$. Then

$$\tau_3(\alpha) = 2(3a,\ -a,\ x,\ z) \in A(m/3).$$

Since $m/3 \neq 20,\ 28$, Proposition 2.5 implies that $(x,\ z) = (-3a,\ -v'a)$, $(-3a,\ \frac{m}{2}+v'a)$, $(\frac{m}{2}+3a,\ -v'a)$ or $(\frac{m}{2}+3a,\ \frac{m}{2}+v'a)$. If $(x,\ z) = (-3a,\ -v'a)$, then

$$\alpha = (a,\ -3a,\ 2a)+(-va,\ -v'a,\ -2a),$$

hence α is decomposable. It is easy to see that the other cases are impossible. □

Lemma 4.5. *Suppose* $\mathrm{ord}_2(m) \ge 2$, $\mathrm{ord}_3(m) = 1$ *and* $m > 84$. *Let* $\alpha = (a,\ \frac{m}{2}+va,\ x,\ y,\ z,\ w)$ *with* $\gcd(m,a) = 1$ *and* $N_1(\alpha) = 2$. *Then* α *cannot belong to* X_m.

Proof. There are two cases:

(4.5) $(a, \frac{m}{2}+va, \frac{m}{2}-(v+1)a)+(x, y, z)$,

(4.6) $(a, x, y)+(\frac{m}{2}+va, z, w)$.

In the first case, we have $N_{(3)}((x, y, z)) \geq 2$. In fact, since $\frac{m}{2}-(v+1)a \equiv \alpha \pmod{3}$, $\equiv \frac{m}{2} \pmod{m/3}$, we obtain

$$\tau_3(\alpha) = (3, -1)(a, \frac{m}{2}-a) + \tau_3((x, y, z)) \in A(m/3),$$

which implies that $N_{(3)}((x, y, z)) \geq 2$. Therefore $x \equiv y \equiv z \equiv 0 \pmod{3}$. But then $\tau_2(\alpha)$ (resp. $\tau_4(\alpha)$) cannot belong to $A(m/2)$ (resp. $A(m/4)$) if $\mathrm{ord}_2(m) > 2$ (resp. $= 2$). In the second case (4.6), we have $N_3((x, y, z, w)) \geq 2$. Therefore

$$\tau_3(\alpha) = 2(3a, -a, x, z) \in A(m/3).$$

Hence Proposition 2.5 implies that $x = -3a$ and $z = v'a$. Thus

$$\alpha = (a, -3a, 2a)+(\frac{m}{2}+va, v'a, \frac{m}{2}+2a).$$

But this cannot belong to B_m, which proves the lemma. □

Corollarly 4.6. *Suppose* $\mathrm{ord}_2(m) \neq 1$ *and* $m > 84$. *Let* α *be an element of* X_m^{indec} *such that* $N_1(\alpha) = 2$. *Then*

$$\alpha = (a, \frac{m}{2}+a, x, y, z, w)$$

for some $a \in (\mathbb{Z}/m\mathbb{Z})^{\times}$.

Proof. The assertion follws from Lemm 4.4 and Lemma 4.5. □

Lemma 4.7. *Suppose* $ord_2(m) \geq 2$ *and suppose* $m > 204$. *Let* $\alpha = (1, \frac{m}{2}+1, \frac{m}{2}-2, a, b, c) \in X_m^{indec}$ *and suppose* $N_1(\alpha) = 2$. *Then* $(a, b, c) = (-2, -2, 4)$ *or* $(\frac{m}{4}+1, \frac{3m}{4}+1, -2)$.

Proof. If $ord_2(m) > 2$, then

$$\tau_2((1, \frac{m}{2}+1, \frac{m}{2}-2)) = 2(1, \frac{m}{4}-1) \overset{U}{\equiv} 4(1).$$

We may assume that $gcd(m,a) = gcd(m,b) = 2$, hence $a \equiv b \equiv c \equiv 0$ (mod.2). Then $\alpha' := T_2(\alpha) = (1, m'/2-1, m'/2, a', b', c') \in X_{m'}$, and $N_1(\alpha') \geq 4$, where $m' = m/2$. Since $ord_2(m') \geq 2$, Proposition 4.3 implies that α' is an element of $X_{m'}^{dec}$. We may assume that either $a' \equiv -1$ or $c' \equiv m'/2$ (mod.m'). The first cacs implies that $a = -2$ and $\alpha \equiv \sigma_{2,1} + (m/2, m/2-2, b, c)$ (mod. D_m), hence $(m/2, m/2-2, b, c) \in B_m^2 \setminus D_m^2$. Then Theorem 2.7 shows that $(b, c) = (-2, 4)$ or $(m/4+1, 3m/4+1)$, which implies the lemma. The second case implies that $c = m/2$ and $\alpha \equiv \sigma_{2,1} + (2, m/2-2, a, b)$ (mod.D_m), hence $(2, m/2-2, b, c) \in B_m^2 \setminus D_m^2$. But this is impossible by Theorem 2.7. Thus the assertion of the lemma holds when $ord_2(m) > 2$.

If $ord_2(m) = 2$, then

$$\tau_4((1, \frac{m}{2}+1, \frac{m}{2}-2)) = 2(4, -2, -2).$$

Therefore either N_2 or N_4 of (a, b, c) is positive. But if $(N_2, N_4) =$

(0, 1), (1, 0), (1, 1) or (2, 0), then using Cor.3.4 and Lemma 3.5 we can verify that $\tau_4(\alpha)$ cannot belongs to A(m/4). Let us consider the remaining cases: (N_2, N_4) = (0, 2), (0, 3) or (2, 1). First, if $N_2 = 0$ and $N_4 \geq 2$, then $a \equiv b \equiv c \equiv 0 \pmod{4}$, hence we obtain

$$(4.7) \qquad T_4(\alpha) = 2(4, -2, -2, a, b, c) \in B_{m/4}.$$

If we put β = (4, -2, -2, a, b, c) $\in$ R(m/4), then $N_1(\beta) \geq 5$ and (4.7) implies that $\beta \in X_{m/4}$. Since m/4 satisfies the condition of Lemma 4.2, we see that $\beta \in D_{m/4}$, that is, (a, b, c) $\equiv$ (2, 2, -4) (mod.m/4). Thus (a, b, c) = $(\frac{m}{2}+2, \frac{m}{2}+2, -4)$, which shows that α is decomposable. Next let us consider the case $N_2 = 2$, $N_4 = 1$. Say gcd(m,a) = gcd(m,b) = 2 and gcd(m,c) = 4. Then

$$(4.8) \qquad \tau_4(\alpha) = 2\{(2, -1)(2, a, b)+(-2, c)\} \in A(m/4).$$

If (2, a, b) $\in$ A(m/4), then (-2, c) $\in$ A(m/4). This implies that (a, b, c) = $(\frac{m}{3}+2, \frac{2m}{3}+2, \frac{m}{2}-2)$. But this is impossible since a + b + c = 0. Thus (2, a, b) $\notin$ A(m/4). Moreover, if $m/4 \neq 3^2 \cdot 5^2$ and (2, a, b) is reduced, Lemma 3.5 implies that (a, b, c) satisfies one of the followings:

$$(2, a, b) \overset{U}{=} (x, 2x, 4x), \qquad (-2, c) \overset{U}{=} (x, -8x),$$

$$(2, a, b) = (x, \frac{m}{3}-2x, \frac{2m}{3}-2x), \quad (-2, c) = (x, -4x),$$

$$(2, a, b) \overset{U}{=} (-gx, -g^2x, -g^3x), \quad (-2, c) \overset{U}{=} (x, -2x).$$

But in all cases we have $a + b + c \neq 0$, which is a contradiction. For $m = 4 \cdot 3^2 \cdot 5^2$ we can directly obtain the same result. Therefore we may assume that $(2, a, b)$ is not reduced, say $(2, a) \in A(m/4)$. Then $(2, -1)(b) + (-2, c) \in A(m/4)$ by (4.8). It follows that $(a, b, c) = (-2, -2, 4)$ or $(\frac{m}{4}+1, \frac{3m}{4}+1, -2)$. This completes the proof. □

Lemma 4.8. *Suppose* $\mathrm{ord}_2(m) \geq 2$ *and* $m > 204$. *Let* $\alpha = (1, a, -a-1) + (\frac{m}{2}+1, b, c) \in X_m$ *and* $N_1(\alpha) = 2$. *Then* α *is decomposable.*

Proof. There exists an odd divisor d of m such that $N_d(\alpha) = 2$, say $\gcd(m,a) = \gcd(m,b) = d$. Then $\tau_d((a, b)) \in A(m/d)$ since $\tau_\delta((1, m/2+1)) \in A(m/\delta)$ for any odd divisor δ. When $m/d \neq 20, 24$, considering τ_{3d} if necessary, Proposition 2.3 implies that $b = -a$ or $m/2 + a$. If $b = -a$, then α is decomposable. We show that b cannot equal $m/2 + a$. Suppose $b = m/2 + a$, then $\alpha = (1, m/2+1)(1, a, -a-1)$. If $\mathrm{ord}_2(m) > 2$, then $T_2(\alpha) = 2(1, a', -a-1)$ with $a' = a/2$. But this cannot belong to $B_{m/2}$. If $\mathrm{ord}_2(m) = 2$, then we may assume that $a + 1 \equiv 0 \pmod{4}$ and

$$T_4(\alpha) = 2\{(2, -1)(1, a, -a-1) + ((a+1)/2)\},$$

which cannot belong to $B_{m/4}$. This show that $b \neq m/2 + a$. Next let us consider the case where $m/d = 20$ or 24. The assumption on m then implies that $d > 3$. Hence both a and b do not affect $\tau_\delta(\alpha)$ so long as we suppose $\delta = 2, 3, 4$ or 6. Then, considering $\tau_\delta(\alpha)$ for such δ's and using Cor.3.4, we can see that α cannot belong to B_m. □

Combining Proposition 4.3, Corollarly 4.6 and Lemma 4.8 together we obtain the following

Proposition 4.9. *Suppose* $\mathrm{ord}_2(m) \neq 1$ *and* $m > 204$. *Let* $\alpha \in X_m^{\mathrm{indec}}$ *and suppose* $N_1(\alpha) > 0$. *Then* α *is one of the following elements:*

(1) $(a,\ a,\ -2a)+(\frac{m}{2}+a,\ \frac{m}{2}+a,\ -2a)$,

(2) $(a,\ \frac{m}{2}+a,\ \frac{m}{2}-2a)+(-2a,\ -2a,\ 4a)$,

(3) $(a,\ \frac{m}{2}+a,\ \frac{m}{2}-2a)+(\frac{m}{4}+a,\ \frac{3m}{4}+a,\ -2a)$,

where a *is an element of* $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

§5. Proof of Theorem 0.3 (the second case).

Throughout this section we assume $ord_2(m) = 1$. Our aim in this section is to prove Proposition 5.2.

Lemma 5.1. *Suppose* $ord_2(m) = 1$ *and* $m > 102$. *Let* $\alpha = (a_0, a_1, a_2) + (a_3, a_4, a_5) \in X_m^{indec}$ *and suppose* $gcd(m, a_i) = 1$ *for* $i = 0, 1, 3$ *and* 4. *Then* (a_0, a_1, a_3, a_4) (mod. $m/2$) *cannot belong to* $A(m/2)$.

Proof. If (a_0, a_1, a_3, a_4) (mod. $m/2$) is 5-q.s., then $ord_5(m) = 1$ and a_i (mod. $m/10$) $\in a_0 U(m/10)$ for $i = 1, 3$ and 4. Therefore a_2 (resp. a_5) $\equiv -2a_0$ or $-(v+1)a_0$ (resp. $-2a_3$ or $-(v+1)a_3$) (mod. $m/10$). Then

$$\tau_{10}(\alpha) \equiv \begin{cases} (5,-1)(2,-1,-1)(a_0) & \text{if } a_1 \equiv a_0,\ a_4 \equiv a_3 \pmod{m/10}, \\ (5,-1)\{3(2,-1)+(-1)\}(a_0) & \text{if } a_1 \equiv a_0,\ a_4 \equiv v a_3 \pmod{m/10}, \\ 4(5,-1)(2,-1)(a_0) & \text{if } a_1 \equiv v a_0,\ a_4 \equiv v a_3 \pmod{m/10}. \end{cases}$$

In the first case we have $T_{10}(\alpha) = (5,-1)(2,-1,-1)(a_0) \in B_{m/10}$, which is however impossible. The second case implies that $5 \in U(m/10)$ since $\chi(3(2,-1)+(-1)) \neq 0$ for all $\chi \in PC^-(m/10)$. But this is impossible. In the third case we have $(5,-1)(2,-1) \in A(m/10)$, which is also impossible by Corollarly 3.4 since $(5,-1) \notin A(m/10)$. Thus (a_0, a_1, a_3, a_4) is not 5-q.s..

Next suppose (a_0, a_1, a_2, a_3) belongs to $A(m/2,2) \oplus A(m/2,2)$, then there are two cases:

(5.1) $(a_0, a_1)\oplus(a_3, a_4)$

(5.2) $(a_0, a_3)\oplus(a_1, a_4)$.

We show that the both cases are impossible. In the first case we have $ord_3(m) = 1$ and $a_1 = -va_0$, $a_4 = -va_3$, hence $\alpha = (1, -v, v-1)(a_0, a_3)$. Therefore

$$\tau_6(\alpha) = \{2(3, -1)(2, -1)+(-2)\}(a_0, a_3) \in A(m/6),$$

which implies that $(a_0, a_3) \in A(m/6)$ since $\chi(2(3,-1)(2,-1)+(-2)) \neq 0$ for any $\chi \in PC^-(m/6)$. Thus the first case (5.1) cannot occur. If (5.2) hols, we have $a_3 = -va_0$, $a_4 = -va_1$, hence $\alpha = (a_0, a_1, a_2)(1,-v)$. Therefore

$$\tau_6(\alpha) = \begin{cases} (3,-1)\{2(2,-1)(a_0,a_1)+(a_2)\} & \text{if } \gcd(m,a_2) = 2, \\ 2\{(3,-1)(2,-1)(a_0,a_1)+(a_2)\} & \text{if } \gcd(m,a_2) = 6, \\ 2(2,-1)(3,-1)(a_0,a_1) & \text{if } \gcd(m,a_2) \neq 2,6. \end{cases}$$

It can be easily shown that the first and second cases are impossible. From the third case we obtain $a_1 = -a_0$ or va_0. Since α is indecomposable, $a_1 \neq -a_0$. On the other hand, if $a_1 = va_0$, then $a_2 = (v+1)a_0$, which implies that $\gcd(m,a_2) = 6$. But this is a contradiction. Therefore (5.2) cannot hold. □

Proposition 5.2. *Suppose* $ord_2(m) = 1$ *and* $m > 210$. *If* $\alpha \in X_m^{indec}$ *and* $N_1(\alpha) > 0$, *then* α *is one of the following elements*:

(1) $(a,\ a,\ -2a)+(\frac{m}{2}+a,\ \frac{m}{2}+a,\ -2a)$,

(2) $(a,\ \frac{m}{2}+a,\ \frac{m}{2}-2a)+(4a,\ -2a,\ -2a)$,

where a *is an element of* $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

Proof. Clearly $N_1(\alpha) \le 4$. Let α_1 (resp. α_2) be the primitive part (resp. 2-th part) of α.

Case 1: $N_1(\alpha) = 4$. First suppose that $N_2(\alpha) = 2$, then

$$\tau_2(\alpha) = (2,\ -1)\alpha_1 + \alpha_2 \ \in A(m/2).$$

If $\alpha_1 \notin A(m/2)$, Lemma 3.5 (i) implies that α is one of the following elements:

$$(a,\ \frac{m}{2}+2a,\ \frac{m}{2}+4a,\ \frac{m}{2}+8a,\ \frac{m}{2}+a,\ -16a),$$
$$(a,\ \frac{m}{2}+2a,\ \frac{m}{3}-a,\ \frac{2m}{3}-a,\ \frac{m}{2}+a,\ -8a),$$
$$(a,\ \frac{m}{6}-2a,\ \frac{5m}{6}-2a,\ \frac{m}{2}+4a,\ \frac{m}{2}+a,\ -8a),$$
$$(\frac{m}{3}-a,\ \frac{2m}{3}-a,\ \frac{m}{2}+2a,\ \frac{m}{2}+4a,\ \frac{m}{2}+a,\ -8a),$$
$$(\frac{m}{3}-a,\ \frac{2m}{3}-a,\ \frac{m}{6}-2a,\ \frac{5m}{6}-2a,\ \frac{m}{2}+a,\ -4a),$$
$$(\frac{m}{2}-2ga,\ \frac{m}{2}-2ga^2,\ \frac{m}{2}-2ga^3,\ \frac{m}{2}-2ga^4,\ \frac{m}{2}+a,\ -4a),$$
$$(-ga,\ -g^2a,\ -g^3a,\ \frac{m}{2}+2a,\ \frac{m}{2}+a,\ -4a).$$

But it is not hard to see that none of these belongs to X_m. Therefore $\alpha_1 \in A(m/2)$ if $N_2(\alpha) = 2$. If $m/2 = 225$, we can see that $\alpha \notin X_m$. In fact, when $m/2 = 225$ and $\alpha \in X_m$, then $T_3(\alpha) \in X_{150}$ and $T_5(\alpha) \in X_{90}$. But, looking at the table in §8 closely, we can see that this is impossible. Since $\alpha_1 \in A(m/2)$, it follows from [A1] Prop.6.5 that it is 5-q.s. or belongs to $A(m,2) \oplus A(m,2)$. If it is 5-q.s., then we can easily see that $\tau_{10}(\alpha) \notin A(m/10)$. If $\alpha_1 \in A(m,2) \oplus A(m,2)$, then $\mathrm{ord}_3(m) = 1$ and $\alpha_1 = (1, -v)(a, b)$. Here note that this implies, in particular, that any element α of X_m^{indec} cannot satisfy the condition $N_1(\alpha) = 1$, $N_2(\alpha) = 2$ if $3 \nmid m$. Now since $a - va \equiv 0 \pmod{3}$, this implies that $\alpha = (1, -v)(a, b, c)$ with $a + b + c = 0$. Therefore

$$T_3(\alpha) = (3, -1)(a, b, c) \in X_{m/3},$$

which is impossible by the above remark. Therefore $N_2(\alpha)$ cannot be 2. Corollarly 3.4 (ii) shows that $N_2(\alpha) \neq 1$. If $N_2(\alpha) = 0$, then $\alpha_1 \in A(m/2)$ by Corollarly 3.4 (i) since $2^4 \notin U(m/2)$. By a similar argument as above one can see that this case is also impossible.

Case 2: $N_1(\alpha) = 3$. In this case, clearly $N_2(\alpha) \leq 2$. If $N_2(\alpha) = 2$, then Lemma 3.5 (ii) implies that α is one of the following elements:

$$\begin{aligned} &(a, \ \tfrac{m}{2}+a, \ \tfrac{m}{2}+2a, \ \tfrac{m}{2}+4a, \ -8a, \ \tfrac{m}{2}), \\ &(a, \ \tfrac{m}{6}-2a, \ \tfrac{5m}{6}-2a, \ \tfrac{m}{2}+a, \ -4a, \ 6a), \\ &(\tfrac{m}{3}-a, \ \tfrac{2m}{3}-a, \ \tfrac{m}{2}+2a, \ \tfrac{m}{2}+a, \ -4a, \ 3a). \end{aligned}$$

But none of these belongs to X_m. By Corollarly 3.4 (ii), $N_2(\alpha) \neq 1$. If $N_2(\alpha) = 0$, then $\alpha_1 \in A(m/2)$ by Corollarly 3.4 (i), hence $\mathrm{ord}_3(m) >$

1 and $\alpha = (a, \frac{m}{3}+a, \frac{2m}{3}+a, x, y, z)$. But it is easy to see that $\alpha \notin X_m$.
Case 3: $N_1(\alpha) = 2$. In this case, if $N_2(\alpha) = 4$, Lemma 3.6 (i) implies that α is one of the elements listed in the statements. Moreover it is easy to see that $N_2(\alpha) \neq 1$, 2 and 3. Thus $N_2(\alpha) = 0$ and $\alpha_1 \in A(m/2)$ by Corollarly 3.4 (i), hence $ord_3(m) = 1$ and α is one of the following two elements:

(5.3) $\quad (1, -v, v-1)(a)+(b, c, d),$

(5.4) $\quad (a, b, c)+(-va, d, e).$

Then by a similar argument as in the proof of Lemma 4.4 we can show that α is decomposable.
Case 4: $N_1(\alpha) = 1$. For simplicity we assume that $\alpha = (1, a, b, c, d, e)$. If $N_2(\alpha) = 4$, say $\gcd(m,a) = \gcd(m,b) = \gcd(m,c) = \gcd(m,d) = 2$, then

$$\tau_2(\alpha) = (2, -1, a, b, c, d) \in A(m/2).$$

There are three cases:

(5.5) $\quad (2, a, b, c)\oplus(-1, d),$

(5.6) $\quad (2, a, b)\oplus(-1, c, d),$

(5.7) $\quad (2, a)\oplus(-1, b, c, d).$

We are going to show that they are all impossible. In case (5.5), we have $d = \frac{m}{2}+1$ or $\frac{m}{2}+v$, hence $e = \frac{m}{2}-2$ or $\frac{m}{2}-v-1$. Since $\gcd(m,e) > 1$, e =

$\frac{m}{2}-v-1 \equiv m/2 \pmod{m/3}$. Therefore $(2, a, b, c)$ is 5-q.s., hence we may assume $(b, c) \in A(m/2)$. But this is impossible since it would imply that $\gcd(m,a) > 1$. In case (5.6), we have $\mathrm{ord}_3(m) > 1$ and $\alpha = (1, \frac{m}{3}+2, \frac{2m}{3}+2, \frac{m}{6}-1, \frac{5m}{6}-1, -3)$. But this cannot belong to X_m. From (5.7) we obtain $a = -2$ or $-2v$. If $(-1, b, c, d)$ is 5-q.s., then $\tau_{10}(\alpha) \overset{U}{=} 4\{(5, -1)(-1)+(2, -1)(e)\}$, which cannot belong to $A(m/10)$. Thus we may assume $(-1, b, c, d) \in A(m/2,2)\oplus A(m/2,2)$. If $(-1, b)\oplus(c, d)$, then $b \overset{U}{=} 1$ and $d \overset{U}{=} -c$. Since $a + b + c = 0$, we have $(a, b, c) \equiv (-2, 1, 1)$ or $(-2v, v, v) \pmod{m/2}$. In both cases, $d = \frac{m}{2} -v$ and $e = \frac{m}{2}+v-1$. Therefore $\alpha = (1, \frac{m}{2}-v, \frac{m}{2}+v-1, -2, \frac{m}{2}+1, \frac{m}{2}+1)$ or $(1, \frac{m}{2}-v, \frac{m}{2}+v-1, -2v, \frac{m}{2}+v, \frac{m}{2}+v)$, both of which cannot belong to B_m. If $(-1, d)\oplus(b, c)$, then $\gcd(m,a) > 1$, hence this case cannot occur.

If $N_2(\alpha) = 3$, then

$$\tau_2(\alpha) = (2, -1, a, b, c).$$

There are two cases: $(2, a)\oplus(-1, b, c)$ or $(2, a, b)\oplus(-1, c)$. But in both cases we get a cotradiction to the assumption $N_1(\alpha) = 1$, $N_2(\alpha) = 3$.

If $N_2(\alpha) = 2$, then

$$\tau_2(\alpha) = (2, -1, a, b) \in A(m/2),$$

hence $(2, a)\oplus(-1, b)$. This implies that $a = -2$ or $-2v$ and $b = \frac{m}{2}+1$ or $\frac{m}{2}+v$. It is not difficult to see that α is of the following form:

$$\alpha = (1,\ \frac{m}{2}+v,\ \frac{m}{2}-v-1)+(a,\ *,\ *).$$

Considering $\tau_6(\alpha)$, one can see that $a = -2$, $N_3 = 0$ and $N_6 = 1$. In this case we have

$$\tau_6(\alpha) = 2(3,\ -1)(-1,\ x) \in A(m/6),$$

hence $x \equiv 1 \pmod{m/6}$. Therefore

$$\alpha = (1,\ \frac{m}{2}+v,\ \frac{m}{2}-v-1)+(-2,\ \varepsilon\frac{m}{6}+1,\ -\varepsilon\frac{m}{6}+1).$$

But this implies that $N_2(\alpha) = 3$, which is a contradiction. Since $N_1(\alpha) \neq 1$, this completes the proof. □

§6. Proof of Theorem 0.3 (the third case).

In this section we treat the case where $N_1(\alpha) = 0$, and prove Proposition 6.4. After that we complete the proof of Theorem 0.3 and Theorem 0.4. Define $X_m^{(1)}$ to be the set of $\alpha \in X_m$ with $GCD(\alpha) = 1$.

First let us note the following fact: For any $\alpha \in B_m$, if $d = D(\alpha)$, $N_d(\alpha) = 1$, $\mathrm{ord}_2(m/d) = 1$ and $m/d \neq 30$, then $N_{2d}(\alpha) \geq 1$. This is an easy consequence of Proposition 2.3.

Lemma 6.1. *Suppose* $m > 42$. *Let* $\alpha \in X_m^{(1)}$ *and* $d = D(\alpha)$. *Then, if* $d > 1$ *and* $N_{(d)}(\alpha) = 4$, α *is decomposable.*

Proof. We prove this by induction on d. If $d \geq m/2$, the assertion is clear. Suppose that every $\beta \in X_m^{(1)}$ with $D(\beta) > d$ and $N_{(D(\beta))}(\beta) = 4$ is decomposable. Put $\alpha = (a_0, a_1, a_2)+(a_3, a_4, a_5)$. Then we may assume that $a_0 \equiv a_1 \equiv a_2 \equiv a_3 \equiv 0$ (mod.d). Note that $\gcd(d, a_4) = \gcd(d, a_5) = 1$ since $a_3 + a_4 + a_5 = 0$ and $a_i \not\equiv 0$ (mod.d) for $i = 4$ and 5. If we put $d_i = \gcd(m, a_i)$, we may assume that $m/d_4 \neq 12, 30$. Then $\mathrm{ord}_2(m/d_4) = 1$ and $d = 2$ since $N_{d_4}(\alpha) = 1$. This implies, in particular, that both d_4 and d_5 are odd and that $\mathrm{ord}_2(m) = 1$. Therefore $N_2(\alpha) \neq 1$.
Case 1: $N_2(\alpha) = 4$. In this case we have

$$\tau_2(\alpha) = (a_0, a_1, a_2, a_3) \in A(m/2).$$

It is easy to see that $\tau_2(\alpha)$ is not 5-q.s.. Therefore we may assume $(a_0, a_1) \in A(m/2)$, which implies that $a_1 = -a_0$ or $-va_0$ since $m/2$ is odd.

But, if $a_1 = -va_0$, then $a_2 = (v-1)a_0 \equiv 0 \pmod{3}$, which is a contradiction. Thus $a_1 = -a_0$, that is, α is decomposable.

Case 2: $N_2(\alpha) = 3$. In this case we may assume

(6.1) $\tau_2(\alpha) = (a_0, a_1, a_2)$ or $(a_0, a_1, a_3) \in A(m/2)$.

By Proposition 2.4 the first case of (6.1) is impossible, and in the second case we have

$$\alpha = (a, \tfrac{m}{3}+a, -\tfrac{m}{3}-2a)+(-\tfrac{m}{3}+a, a_4, a_5),$$

where $a = a_0$ or a_1. But then, considering $\tau_6(\alpha)$, one can easily see that $N_3(\alpha) = 1$, say $d_4 = 3$. Therefore 3 does not divide d_5, hence

$$\tau_{2d_5}(\alpha) \equiv \tau_{2d_5}(a_5) \not\equiv 0 \pmod{A(m/2d_5)},$$

which is a contradiction.

Case 3: $N_2(\alpha) = 2$. In this case, we have the following decomposition:

$$\alpha = \alpha_1 + \alpha_2\ , \quad \alpha_1 \in A(m,2) \text{ and } \alpha_2 \in R(m,4).$$

Proposition 2.3 implies that $\alpha_1 = (a, -a)$ or $(a, -va)$ since $m/2$ is odd. The first case shows that α is decomposable. In the second case, we define a new element $\alpha' = \alpha_1' + \alpha_2$ with $\alpha_1' = (v'a, 3a)$. Then $\alpha' \in X_m$ since $\alpha_1 + (-1)\alpha_1' = \sigma_{3,a} \in B_m^2$. Moreover $N_{(2)}(\alpha') = 4$ and $D(\alpha') >$

2. Therefore by the inductive hypothesis α' is decomposable. This shows that α itself is decomposable as well. Thus the proof is complete. □

Lemma 6.2. *Suppose* $m > 132$. *If* $\alpha = (a_0, a_1, a_2)+(a_3, a_4, a_5) \in X_m^{(1)}$ *and* $d = D(\alpha) > 1$, *then* $N_{(d)}(\alpha) \neq 3$.

Proof. Let $\alpha_1 = (a_0, a_1, a_2)$ and $\alpha_2 = (a_3, a_4, a_5)$. Suppose $N_{(d)}(\alpha) = 3$, then we may assume $a_0 \equiv a_1 \equiv a_2 \equiv 0 \pmod{d}$. First note that $d \neq 2$. Indeed, if $d = 2$, then $N_{(2)}(\alpha) = 4$, which is a contradiction. Thus we may assume $d > 2$. Let

$$d' = \min\{ d_3, d_4, d_5 \}.$$

Then $a_3 \equiv a_4 \equiv a_5 \equiv 0 \pmod{d'}$, that is, $N_{(d')}(\alpha_2) = 3$. To see this, suppose $N_{(d')}(\alpha') < 3$. Then $N_{(d_i)}(\alpha_2) = 1$ for $i = 3$, 4 and 5. Therefore $m/d_i = 30$ for $i = 3$, 4 and 5, which is impossible. We are going to prove the assertion by induction on $d + d'$. If $d + d' \geq m$, the assertion is clear. We assume that the assertion holds for evry $\beta = \beta_1 + \beta_2 \in X_m^{(1)}$ with $D(\beta_1) + D(\beta_2) > d + d'$. Note that $m/d > 12$ since we are assuming $m > 132$.

Case 1: $N_d(\alpha) = 3$. In this case, considering τ_d or τ_{2d}, we have

$$(a_0, a_1, a_2) = (a_0, \tfrac{m}{3}+a_0, \tfrac{2m}{3}+a_0).$$

by Proposition 2.4. (If $m/d = 21$ or 28, consider τ_{3d} or τ_{4d} respectively.) But then $d = m/3$ since $a_0 + a_1 + a_2 = 3a_0 = 0$. This implies that $a_3 = a_4 = a_5 = \frac{m}{2}$, which is impossible.

Case 2: $N_d(\alpha) = 2$. In this case Proposition 2.3 shows that

$$\alpha_1 = \begin{cases} (a, \frac{m}{2}+a, \frac{m}{2}-2a) \\ (a, -va, (v-1)a) \\ (a, \frac{m}{2}+va, \frac{m}{2}-(v+1)a) \end{cases} .$$

(If $m/d = 20$, consider τ_{4d}.) The third case is impossible sinse $\tau_{3d}(\alpha) \notin A(m/3d)$. In the first case, replacing α_1 by $\beta_1 = (2a, \frac{m}{2}, \frac{m}{2}-2a)$ and α by $\beta = \beta_1 + \alpha_2$, we have $\beta \in B_m$, $D(\beta_1) + D(\alpha_2) > d + d'$ and $N_{(\delta)}(\alpha') = 3$. Then inductive hypothesis implies that this case is also impossible. The second case is similarly impossible. (Replace α_1 by $(3a, v'a, (v-1)a)$.)

Case 3: $N_d(\alpha) = 1$. If $m/d = 30$, then $d > 4$ since we are assuming $m > 132$. Therefore, if $N_{d'}(\alpha) > 1$, the above proof goes for d'. Thus we may assume $N_{d'}(\alpha) = 1$. Then $ord_2(m/d) = ord_2(m/d') = 1$. This implies in particular that both d and d' are odd, hence $N_{2d}, N_{2d'} \leq 1$. Since $m/d \neq m/d'$, we may assume $m/d \neq 30$. Then $N_{2d}(\alpha) = 1$, and we have

$$\tau_{2d}(\alpha) = \frac{\varphi(m)}{\varphi(m/d)}\{(2, -1)(a_0') + (a_1')\} \in A(m/2d),$$

which is however impossible by Proposition 2.4. Thus the proof is complete. □

Lemma 6.3. *Suppose* $m > 165$. *Let* $\alpha \in X_m^{(1)}$ *and suppose that* $d = D(\alpha) > 1$ *and* $N_{(d)}(\alpha) = 2$, *then* α *is decomposable.*

Proof. We prove this by induction on d. If $d \geq m/2$, the assertion is clear. We assume that the lemma holds for every $\beta \in X_m^{(1)}$ with $N_{(D(\beta))}(\beta) = 2$ and $D(\beta) > d$. First observe that $d^3 < m$, and so $m/d > m^{2/3} > 30$ since we are assuming $m > 165$. Let $\alpha = (a_0, a_1, a_2)+(a_3, a_4, a_5)$. The assumption on α implies that $N_{(d)}((a_0, a_1, a_2)) = N_{(d)}((a_3, a_4, a_5)) = 1$, say $a_0 \equiv a_3 \equiv 0 \pmod{d}$. We may assume that $\gcd(a_0,m) = d$. Moreover $\gcd(a_i,d) = 1$ for $i = 1,2,4$ and 5. If $N_d(\alpha) = 1$, then $ord_2(m/d)=1$ and $\gcd(a_3,m) = 2d$. But this is impossible by Proposition 2.4. Thus $N_d(\alpha) = 2$, that is, $\gcd(a_3,m) = d$. Then it follows from Proposition 2.3 that $a_3 = -a_0, \frac{m}{2}+a_0, -va_0$ or $\frac{m}{2}+va_0$. In the first case α is decomposable. In the forth case, considering τ_{3d}, we can easily see that $d = 2$. But then $\tau_{hd}(\alpha) \notin A(m/hd)$ for $h = 4$ if $ord_2(m/d) = 2$ and $h = 2$ otherwise. Thus the fourth case cannot occur. In the second case, if we replace (a_0, a_3) by $(2a_0, \frac{m}{2})$ (resp. $(v'a_0, 3a_0)$) (denoting the new element by α'), the induction proceeds since $d' := D(\alpha') > d$ and $N_{(d')}(\alpha') = 2$. Therefore α' is decomposable, which shows that α itself is decomposable as well. This completes the proof. □

Proposition 6.4. *Suppose* $m > 165$. *Let* $\alpha \in X_m^{(1)}$ *and* $d = D(\alpha) > 1$. *Then* α *is decomposable.*

Proof. Let $\alpha = (a_0, \ldots, a_5)$. If $N_{(d)}(\alpha) > 1$, then the above three lemmas shows that α is decomposable. Hence it suffices to show that $N_{(d)}(\alpha) \neq 1$. Suppose on the contrary that $N_{(d)}(\alpha) = 1$, say $\gcd(m,a_0) = d$. This implies that $ord_2(m/d) = 1$ since $\tau_d(\alpha) \in A(m/d)$ and $m/d >$

30 (see the biginning of the proof of Lemma 6.2). But then $\tau_{2d}(\alpha) \notin A(m/2d)$ since $gcd(d, a_i) = 1$ and $gcd(m, a_i) > 2$ for $1 \leq i \leq 5$, which is a contradiction. This completes the proof. □

Proof of Theorem 0.3. By Proposition 4.9, Proposition 5.2 and Proposition 6.5, the assertion of the theorem is true for $m > 210$. For $m \leq 210$ we can directly check the theorem. The proof is now complete. □

§7. **Proofs of other theorems.**

In this section we give the proofs of Theorem 0.1, Theorem 0.2 and Theorem 0.4 stated in the introduction.

Proof of Theorem 0.1. Let α, β be two elements of $\mathfrak{A}^1_m$ such that $GCD(\alpha, \beta) = 1$. Then as is shown in section 1, $A_{[\alpha]}$ is isogenous to $A_{[\beta]}$ if and only if $\alpha * (-t \cdot \beta) \in \mathfrak{B}^4_m$ for some $t \in (\mathbf{Z}/m\mathbf{Z})^\times$. Since we are interested in the equivalence classes of α and β, we may assume without loss of generality that $\alpha * (-\beta) \in \mathfrak{B}^4_m$. By Theorem 0.3 there are nine possible cases for $\alpha * (-\beta)$. In the case of (1) of Theorem 0.3, we have $\alpha \sim \beta$. In the cases from (2) to (7), we see that both α and β are equal to elements listed in (3) of Theorem 0.1. In the case of (8) and (9) of Theorem 0.3, both α and β are equal to elements in (1) and (2) of Theorem 0.1, respectively. □

Proof of Theorem 0.2. Let α be an element of $\mathfrak{A}^1_m$ with $GCD(\alpha) = 1$. Suppose that $W_\alpha \neq \{1\}$. We want to show that α is either of Type II or of Type III. Once this has been proved the calculation of W_α is easy and we leave it to the reader. If $w \neq 1$ is an element of W_α, then $\alpha * (-w \cdot \alpha) \in \mathfrak{B}^4_m$. One can easily see that among nine cases of Theorem 0.3 only the elements of (1), (3) and (7) can be of the form $\alpha * (-w \cdot \alpha), w \neq 1$. In the case of (1), we have $w \cdot \alpha \sim \alpha$. Therefore

$$\alpha \sim (a, wa, -(1+w)a), \quad w^2 = 1, \quad w \neq \pm 1 \quad \text{or}$$

$$\alpha \sim (a, wa, w^2 a), \; 1 + w + w^2 = 0$$

for some $a \in (\mathbf{Z}/m\mathbf{Z})^\times$, hence α is of Type II-1, Type II-3 or Type III. In the case of (3), we have

$$\alpha \sim (a, a, -2a)$$

for some $a \in (\mathbf{Z}/m\mathbf{Z})^\times$ and $w = \frac{m}{2} - 1, ord_2 m \geq 2$, i.e., α is of Type II-2. In the case of (7) we have

$$\alpha \sim (a, \frac{m}{2} + a, \frac{m}{2} - 2a), \quad ord_2 m \geq 3$$

for some $a \in (\mathbf{Z}/m\mathbf{Z})^\times$ and $w = \frac{m}{2} + 1, \frac{m}{4} - 1$ or $\frac{3m}{4} - 1$, i.e., α is of Type II-3. The proof is now complete. □

Proof of Theorem 0.4. Let H be a subset of $(\mathbf{Z}/m\mathbf{Z})^\times$ such that $\sharp H = \varphi(m)/2$ and $H \cup (-H) = (\mathbf{Z}/m\mathbf{Z})^\times$ (i.e., a halfsystem of $(\mathbf{Z}/m\mathbf{Z})^\times$). If H and H' are two halfsystems such that $H = t \cdot H'$ for some $t \in (\mathbf{Z}/m\mathbf{Z})^\times$, we say that H are equivalent to H'. We define the numbers $\rho_1(m)$ and $\rho(H)$ by

$$\rho_1(m) = \sharp\{(\alpha, \beta) \in \mathfrak{A}^1_m * \mathfrak{A}^1_m \mid \alpha \sim \beta\} = \sharp\{(\mathfrak{A}^1_m * \mathfrak{A}^1_m) \cap \mathfrak{D}^4_m\},$$

$$\rho(H) = \sharp\left\{(\alpha, \beta) \in (\mathfrak{A}^1_m * \mathfrak{A}^1_m) \cap \mathfrak{B}^4_m \;\middle|\; \begin{array}{l} \alpha \not\sim \beta,\ GCD(\alpha, \beta) = 1 \\ \text{and } H_\alpha \text{ is equivalent to } H \end{array}\right\}.$$

Then by (0.1) the Picard number of $X^1_m \times X^1_m$ is calculated as follows:

$$\rho = \rho(X^1_m \times X^1_m) = 2 + \rho_1(m) + \sum_{d|m} \sum_{H \in \mathcal{H}(d)} \rho(H), \tag{7.1}$$

where $\mathcal{H}(d)$ denotes $(\mathbf{Z}/d\mathbf{Z})^\times$-orbits of the halfsystems of $(\mathbf{Z}/d\mathbf{Z})^\times$. It is easy to see that

$$\rho_1(m) = 6m^2 - 27m + 21 + \begin{cases} 9 & (2|m) \\ 0 & (2 \nmid m) \end{cases} + \begin{cases} 8 & (3|m) \\ 0 & (3 \nmid m) \end{cases}. \tag{7.2}$$

For $m \notin \mathcal{E}$, the representatives of all equivalence classes of halfsystems H with $\rho(H) > 0$ are listed in Table I of the last section. We denote by $\mathcal{H}_2(m)$ (resp. $\mathcal{H}_3(m)$) the halfsystems in Table I-1 and I-2 (resp. Table I-3). For any divisor d of m, $\mathcal{H}_2(d)$ and $\mathcal{H}_3(d)$ are defined similarly. We put

$$\rho_2(m) = \sum_{\substack{d|m \\ d \notin \mathcal{E}}} \sum_{H \in \mathcal{H}_2(d)} \rho(H), \qquad \rho_3(m) = \sum_{\substack{d|m \\ d \notin \mathcal{E}}} \sum_{H \in \mathcal{H}_3(d)} \rho(H).$$

Then by (7.1) we have

$$\rho = 2 + \rho_1(m) + \rho_2(m) + \rho_3(m) + \sum_{\substack{d|m \\ d\in\mathcal{E}}} \Delta'(d), \tag{7.3}$$

where $\Delta'(d) = \sum_{H\in\mathcal{H}(d)} \rho(H)$. We define two functions Δ_2 and Δ_3 on $\mathcal{E}$ by

$$\Delta_2(d) = \begin{cases} 0 & (2 \nmid d) \\ 378\varphi(d) & (2\|d) \\ 225\varphi(d) & (4\|d) \\ 207\varphi(d) & (8|d) \end{cases}, \qquad \Delta_3(d) = \begin{cases} 0 & (3 \nmid d) \\ 108\varphi(d) & (3\|d) \\ 72\varphi(d) & (9|d) \end{cases}.$$

Then from Table I-1 and Table I-2 we can caluculate $\rho_2(m)$ as follows:

(7.4)

$$\rho_2(m) + \sum_{\substack{d|m \\ d\in\mathcal{E}}} \Delta_2(d)$$

$$= \begin{cases} 0 & & (2 \nmid m) \\ 378\sum_{2\|d}\varphi(d) & = 189m & (2\|m) \\ 378\sum_{2\|d}\varphi(d) + 225\sum_{4|d}\varphi(d) & = 207m & (4\|m) \\ 378\sum_{2\|d}\varphi(d) + 225\sum_{4\|d}\varphi(d) + 207\sum_{8|d}\varphi(d) & = 207m & (8|m) \end{cases}.$$

Similarly from Table I-3 we obtain

$$\rho_3(m) + \sum_{\substack{d|m \\ d\in\mathcal{E}}} \Delta_3(d) = \begin{cases} 0 & & (3 \nmid m) \\ 108\sum_{3\|d}\varphi(d) & = 72m & (3\|m) \\ 108\sum_{3\|d}\varphi(d) + 72\sum_{9|d}\varphi(d) & = 72m & (9|m) \end{cases}. \tag{7.5}$$

If we define a function Δ on $\mathcal{E}$ by

$$\Delta(d) = \Delta'(d) - \Delta_2(d) - \Delta_3(d),$$

then from (7.3) we have

$$\rho = 2 + \rho_1(m) + \left\{\rho_2(m) + \sum_{\substack{d|m \\ d\in\mathcal{E}}} \Delta_2(d)\right\} + \left\{\rho_3(m) + \sum_{\substack{d|m \\ d\in\mathcal{E}}} \Delta_3(d)\right\} + \sum_{\substack{d|m \\ d\in\mathcal{E}}} \Delta(d).$$

Substituting (7.2), (7.4) and (7.5) into this formula, we obtain the desired formula for $\rho(X_m^1 \times X_m^1)$ of Theorem 0.4. □

§8. **Some remarks.**

1. The field of definition. The defining field of the isogeny (1.1) in Theorem 1.6 was studied by Schmidt ([**Sch**]) and Koblitz ([**Ko**]). For $\alpha = (a, b, c) \in \mathfrak{A}^1_m$, let

$$\Gamma(\alpha) = \Gamma\left(\left\langle\frac{a}{m}\right\rangle\right)\Gamma\left(\left\langle\frac{b}{m}\right\rangle\right)\Gamma\left(\left\langle\frac{c}{m}\right\rangle\right),$$
$$M_\alpha = K_\alpha(\Gamma(\alpha)/\Gamma(t\cdot\alpha)\ ;\ t \in W_\alpha),$$

where $K_\alpha = \mathbf{Q}(\zeta_{m(\alpha)})$. Then the isogeny (1.1) is defined over M_α ([**Sch**] V, Korollar 2.3). Note that $\Gamma(\alpha)/\Gamma(t\cdot\alpha) \in K_\alpha^{ab}$ for any $t \in W_\alpha$ since $\alpha * (-t\cdot\alpha)$ is an element of $\mathfrak{B}^4_m$ (see [**D**], Theorem 7.18 or [**K-O**]). Using a result of Koblitz and Rhorlich [**K-R**] (Theorem 1.8 in this paper), Schmidt showed that $M_\alpha = K_\alpha$ when $GCD(m, 6) = 1$ ([**Sch**] V, Korollar 2.4). Using Theorem 0.2 we can get M_α explicitly for any $\alpha \in \mathfrak{A}^1_m, m \notin \mathcal{E}$ with $GCD(\alpha) = 1$.

Theorem 8.1. *Let $K = \mathbf{Q}(\zeta_m)$ be the m-th cyclotomic field. Suppose that $m \notin \mathcal{E}$ and $GCD(\alpha) = 1$. Then M_α is given as follows.*

(i) If α is neither of Type II-2 nor of Type II-3, then $M_\alpha = K$.

(ii) If α is of Type II-2, then $M_\alpha = K(2^{4/m})$.

(iii) If α is of Type II-3, then $M_\alpha = K(2^{(m-4)/2m})$.

Proof. The first statement (i) is clear since $t\cdot\alpha$ is equal up to permutation to α in that case. To show that the other statements, we recall the following formulas:

$$\prod_{i=0}^{n-1}\Gamma(x+\frac{i}{n}) = (2\pi)^{\frac{n-1}{2}} n^{\frac{1}{2}-nx}\Gamma(nx), \tag{8.1}$$

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{sin\pi x}, \tag{8.2}$$

where $x \in \mathbf{R}$ and $n \in \mathbf{N}$. From these formulas we have

$$\Gamma(\sigma_{2,a}) = 2^{1-\langle\frac{2a}{m}\rangle}\cdot\frac{\pi^2}{sin(\langle\frac{2a}{m}\rangle\pi)}. \tag{8.3}$$

Moreover for any $\alpha = (a, b, c) \in \mathfrak{A}_m^1$ we have

$$\frac{\Gamma(\alpha)}{\Gamma(t \cdot \alpha)} = \Gamma(\alpha * (-t \cdot)\alpha) \cdot \frac{sin(\langle \frac{ta}{m} \rangle \pi) sin(\langle \frac{tb}{m} \rangle \pi) sin(\langle \frac{tc}{m} \rangle \pi)}{\pi^3}. \tag{8.4}$$

We want to show the following formula:

$$\frac{\Gamma(\alpha)}{\Gamma(t \cdot \alpha)} = \begin{cases} 2^{1-2\langle \frac{2a}{m} \rangle} cot(\langle \frac{a}{m} \rangle \pi) & \text{if } \alpha = (a, a, m-2a), \\ 2^{\frac{1}{2} - 2\langle \frac{2a}{m} \rangle} & \text{if } \alpha = (a, \frac{m}{2} + a, \frac{m}{2} - 2a), \end{cases} \tag{8.5}$$

where $t = \frac{m}{2} - 1$ in the first case and $t = \frac{m}{4} - 1$ or $\frac{3m}{4} - 1$ in the second case. (Note that $\Gamma(t \cdot \alpha) = \Gamma(\alpha)$ for any other $t \in W_\alpha$.) The statements (ii) and (iii) of the theorem immediately follow from (8.5). We now consider the first case of (8.5). In this case we have $-t = \frac{m}{2} + 1$ and

$$\alpha * ((\frac{m}{2} + 1) \cdot \alpha) = 2\sigma_{2,a} - (\frac{m}{2}, \frac{m}{2})$$

in R_m, and so by (8.3) and (8.4) we have

$$\begin{aligned} \frac{\Gamma(\alpha)}{\Gamma(t \cdot \alpha)} &= \frac{\Gamma(\sigma_{2,a})^2}{\Gamma(\frac{1}{2})^2} \cdot \frac{sin^2(\langle \frac{m/2-a}{m} \rangle \pi) sin(\langle \frac{2a}{m} \rangle \pi)}{\pi^3} \\ &= 2^{2-2\langle \frac{2a}{m} \rangle} \cdot \frac{cos^2(\langle \frac{a}{m} \rangle \pi)}{sin(2\langle \frac{a}{m} \rangle \pi)} \\ &= 2^{1-2\langle \frac{2a}{m} \rangle} \cdot cot(\langle \frac{a}{m} \rangle \pi). \end{aligned}$$

Next we consider the second case of (8.5). In this case we have

$$\alpha * (-t \cdot \alpha) = \sigma_{2,a} + \sigma_{2,\frac{m}{4}+a} - (\frac{m}{2}, \frac{m}{2})$$

in R_m, and so similarly as above we have

$$\begin{aligned} \frac{\Gamma(\alpha)}{\Gamma(t \cdot \alpha)} &= \frac{\Gamma(\sigma_{2,a})\Gamma(\sigma_{2,\frac{m}{4}+a})}{\Gamma(\frac{1}{2})^2} \cdot \frac{sin(\langle \frac{m/4-a}{m} \rangle \pi) sin(\langle \frac{3m/4-a}{m} \rangle \pi) sin(\langle \frac{2a}{m} \rangle \pi)}{\pi^3} \\ &= 2^{\frac{1}{2} - 2\langle \frac{2a}{m} \rangle}. \end{aligned}$$

The proof is now complete. □

2. *Ordinary reduction.* The abelian variety A_S is defined over $\mathbf{Q}$ and has good reduction at p if $GCD(p,m) = 1$. Moreover it has ordinary reduction at p if and only if $p \pmod{m(S)} \in W_\alpha, \alpha \in S$. Thus we can determine the set of ordinary primes for A_S. The following theorem is proved by Coleman ([Co]) when m is prime to 6.

Theorem 8.2. *Suppose $m \notin \mathcal{E}$ and let α be an element of $\mathfrak{A}^1_m$ with $GCD(\alpha) = 1$.*

(1) *If α is of Type I, then A_S has ordinary reduction at p if and only if $p \equiv 1 \pmod{m}$.*

(2) *If α is of Type II-1, then A_S has ordinary reduction at p if and only if $p \equiv 1$ or $w \pmod{m}$.*

(3) *If α is of Type II-2, then A_S has ordinary reduction at p if and only if $p \equiv 1$ or $\frac{m}{2} - 1 \pmod{m}$.*

(4) *If α is of Type II-3, then A_S has ordinary reduction at p if and only if $p \equiv 1, \frac{m}{2} + 1$ or $\pm\frac{m}{4} - 1 \pmod{m}$.*

(5) *If α is of Type III, then A_S has ordinary reduction at p if and only if $p \equiv 1, w$ or $w^2 \pmod{m}$.*

3. *Hodge conjecture for X^4_m.* In a similar way as in the proof of Theorem 0.3, we can determine the subset of elements $\alpha \in \mathfrak{B}^4_m$ with $GCD(\alpha) = 1$ for a sufficiently large m.

Theorem 8.3. *Suppose $m > 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ and let $\alpha \in \mathfrak{B}^4_m, GCD(\alpha) = 1$. Then α is equal (up to permutation) to one of the following elements:*

(1) $$(a, \quad b, \quad c, \quad d, x, \quad -x),$$

(2) $$(a, \quad \frac{m}{2} + a, \quad -2a, x, y, \quad z),$$

(3) $$(a, \quad \frac{m}{2} + a, \quad -2a, b, \frac{m}{2} + b, \quad -2b),$$

(4) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}+2a,\ \frac{m}{2}+4a,\ -8a,\ \frac{m}{2}\right),$

(5) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}+2a,\ \frac{m}{2}+4a,\ \frac{m}{2}+8a,\ -16a\right),$

(6) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}+2a,\ \frac{m}{4}+2a,\ \frac{3m}{4}+2a,\ -8a\right),$

(7) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}+4a,\ \frac{m}{4}+a,\ \frac{3m}{4}+a,\ -8a\right),$

(8) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}-3a,\ \frac{m}{3}+a,\ \frac{m}{3}+2a,\ \frac{m}{3}-2a\right),$

(9) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}-3a,\ \frac{m}{3}+2a,\ \frac{2m}{3}+2a,\ -3a\right),$

(10) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}+6a,\ \frac{m}{3}+2a,\ \frac{2m}{3}+2a,\ -12a\right),$

(11) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{2}+6a,\ \frac{m}{6}-2a,\ \frac{5m}{6}-2a,\ -4a\right),$

(12) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{3}+2a,\ \frac{2m}{3}+2a,\ -6a,\ \frac{m}{2}\right),$

(13) $\left(a,\ \frac{m}{2}+a,\ \frac{\varepsilon m}{3}+2a,\ \frac{\varepsilon m}{3}+4,\ \frac{-\varepsilon m}{6}-2a,\ 6a\right),$

(14) $\left(a,\ \frac{m}{2}+a,\ \frac{m}{4}+a,\ \frac{3m}{4}+a,\ -4a,\ \frac{m}{2}\right),$

(15) $\left(a,\ \frac{m}{2}+2a,\ \frac{m}{2}+2a,\ \frac{m}{6}-a,\ \frac{5m}{6}-a,\ -4a\right),$

(16) $\left(a,\ \frac{m}{2}+3a,\ \frac{m}{3}+a,\ \frac{2m}{3}+a,\ -6a,\ \frac{m}{2}\right),$

(17) $\left(a,\ \frac{m}{2}+3a,\ \frac{m}{2}+6a,\ \frac{m}{3}+a,\ \frac{2m}{3}+a,\ -12a\right),$

(18) $\left(a,\ \frac{m}{2}+3a,\ \frac{m}{6}-a,\ \frac{5m}{6}-a,\ -2a,\ \frac{m}{2}\right),$

(19) $\left(a,\ \frac{m}{3}+a,\ \frac{2m}{3}+a,\ \frac{m}{3}+3a,\ \frac{2m}{3}+3a,\ -9a\right),$

(20) $\left(a,\ \frac{m}{3}+2a,\ \frac{2m}{3}+2a,\ \frac{m}{6}-a,\ \frac{5m}{6}-a,\ -3a\right),$

(21) $\left(a,\ \frac{m}{5}+a,\ \frac{2m}{5}+a,\ \frac{3m}{5}+a,\ \frac{4m}{5}+a,\ -5a\right),$

(22) $\left(a,\ \frac{m}{6}-a,\ \frac{5m}{6}-a,\ -2a,\ -3a,\ 6a\right),$

(23) $\left(3a,\ \frac{m}{2}+3a,\ \frac{m}{3}-2a,\ \frac{2m}{3}-2a,\ -2a,\ -2a\right),$

(24) $\left(3a,\ \frac{m}{2}+3a,\ \frac{m}{2}+6a,\ \frac{m}{3}-4a,\ \frac{2m}{3}-4a,\ -4a\right),$

where both (a, b, c, d) *in (1) and* $(x, y, z, \frac{m}{2})$ *in (2) are elements of* $\mathfrak{B}_m^2$ *and where* $\varepsilon = \pm 1$ *in (13).*

Note that every element in the above theorem is generated by standard elements and soeme elements in $\mathfrak{B}_m^2$. It is shown in [Sh3], [A-S] and [A2] that the one-dimensional subspace $V(\alpha)$ of $H^4(X_m^4, \mathbf{C})$ is spanned by the cohomology classes of some algebraic cycles for any element α generated by standard elements. Since the Hodge conjecture holds true for any surface, we obtain the following

Corollarry 8.4. *If the Hodge conjecture for* X_d^4 *is true for every proper divisor* d *of* m *such that* $d \leq 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, *then the Hodge conjecture for* X_m^4 *is also true.*

§9. Tables.

In Table I-1,2 and 3, we list up halfsystems H of $(\mathbf{Z}/m\mathbf{Z})^\times$ $(m \notin \mathcal{E})$ and $\alpha \in \mathfrak{A}_m^1$ for which $\rho(H) > 0$ and $H_\alpha = H$. (For the definition of $\rho(H)$, see section 7.) In the tables e_2 and e_3 denote $ord_2(m)$ and $ord_3(m)$, respectively. In Table I-1 and 2 (resp. Table I-3) we treat the case where $e_2 > 0$ (resp. $e_3 > 0$). (Note that $\rho(H) = 0$ if $e_2 = e_3 = 0$ by Theorem 1.8.) If $e_3 = 1$, ε denotes 1 or -1 satisfying $m/3 \equiv \varepsilon \pmod 3$. Moreover we adopt the following notation.

$$\mathbf{N}(m) = \{t \in \mathbf{N} \mid 0 < t < m,\ gcd(t,m) = 1\},$$
$$\mathbf{N}(m)^\varepsilon = \{t \in \mathbf{N}(m) \mid t \equiv \varepsilon \pmod 3\}.$$

We identify $(\mathbf{Z}/m\mathbf{Z})^\times$ with $\mathbf{N}(m)$ in the obvious manner. Then the halfsystems in the tables below are defined as follows:

$$H(2) = \mathbf{N}(m) \cap [0, \frac{m}{2}],$$
$$H(4) = \mathbf{N}(m) \cap ([0, \frac{m}{4}] \cup [\frac{m}{2}, \frac{3m}{4}]),$$
$$H(2,3) = \mathbf{N}(m) \cap ([0, \frac{m}{3}] \cup [\frac{m}{2}, \frac{2m}{3}]),$$
$$H(3,4) = \mathbf{N}(m) \cap ([0, \frac{m}{4}] \cup [\frac{m}{3}, \frac{m}{2}] \cup [\frac{2m}{3}, \frac{3m}{4}]),$$
$$H(4,6) = \mathbf{N}(m) \cap ([0, \frac{m}{6}] \cup [\frac{m}{4}, \frac{m}{2}] \cup [\frac{3m}{4}, \frac{5m}{6}]),$$
$$H(6)^\varepsilon = (\mathbf{N}(m) \cap [0, \frac{m}{6}])$$
$$\cup \{\mathbf{N}(m)^\varepsilon \cap ([\frac{m}{6}, \frac{m}{3}] \cup [\frac{2m}{3}, \frac{5m}{6}])\} \cup (\mathbf{N}(m)^{-\varepsilon} \cap ([\frac{m}{3}, \frac{2m}{3}]),$$

where, for any real number a, b, $[a, b]$ denotes the closed interval $\{x \in \mathbf{R} \mid a \leq x \leq b\}$.

Table I–1

<table>
<tr><th></th><th>α</th><th>H</th><th>W</th><th>$\rho(H)/\varphi(m)$</th></tr>
<tr><td>$e_1=1$</td><td>$(1, 1, -2)$
$(1, \frac{m}{2}-1, \frac{m}{2})$
$(1, \frac{m-2}{4}, \frac{3m-2}{4})$
$(2, \frac{m}{2}-1, \frac{m}{2}-1)$</td><td>H(2)</td><td>$\{1\}$</td><td>234</td></tr>
<tr><td rowspan="2">$e_2=2$</td><td>$(1, 1, -2)$
$(1, \frac{m}{2}-1, \frac{m}{2})$</td><td>H(2)</td><td>$\{1, \frac{m}{2}-1\}$</td><td>45</td></tr>
<tr><td>$(1, \frac{m}{2}-2, \frac{m}{2}+1)$
$(2, 2, -4)$
$(2, \frac{m}{2}-2, \frac{m}{2})$
$(2, \frac{m}{4}-1, \frac{3m}{4}-1)$
$(4, \frac{m}{2}-2, \frac{m}{2}-2)$</td><td>H(4)</td><td>$\{1, \frac{m}{2}+1\}$</td><td>108</td></tr>
<tr><td rowspan="2">$e_2\geq 3$</td><td>$(1, 1, -2)$
$(1, \frac{m}{2}-1, \frac{m}{2})$</td><td>H(2)</td><td>$\{1, \frac{m}{2}-1\}$</td><td>45</td></tr>
<tr><td>$(1, \frac{m}{2}-2, \frac{m}{2}+1)$
$(2, 2, -4)$
$(2, \frac{m}{2}-2, \frac{m}{2})$</td><td>H(4)</td><td>$\{1, \frac{m}{4}-1, \frac{m}{2}+1, \frac{3m}{4}-1\}$</td><td>90</td></tr>
</table>

Table I–2

	α	H	W	$\rho(H)/\varphi(m)$
$e_2=1$	$(1, 3, -4)$ $(3, \frac{m}{2}-2, \frac{m}{2}-1)$	H(3,4)	{1}	72
	$(1, \frac{m}{2}-3, \frac{m}{2}+2)$ $(4, \frac{m}{2}-3, \frac{m}{2}-1)$	H(4,6)	{1}	72
$e_2\geq 2$	$(1, 3, -4)$ $(3, \frac{m}{2}-2, \frac{m}{2}-1)$	H(3,4)	{1}	72

Table I–3 $(m/3 \equiv \varepsilon \pmod{3})$

	α	H	W	$\rho(H)/\varphi(m)$
$e_3=1$	$(1, 2, -3)$ $(2, \frac{m}{3}-1, \frac{2m}{3}-1)$	H(2,3)	{1}	72
	$(1, \frac{\varepsilon m}{3}+1, \frac{-\varepsilon m}{3}-2)$ $(3, \frac{\varepsilon m}{3}-1, \frac{-\varepsilon m}{3}-2)$	$H(6)^{\varepsilon}$	$\{1, \frac{\varepsilon m}{3}+1\}$	36
$e_3\geq 2$	$(1, 2, -3)$ $(2, \frac{m}{3}-1, \frac{2m}{3}-1)$	H(2,3)	{1}	72

In the following table we give the values of $\Delta(m)$ for $m \in \mathcal{S}$.

Table II

m	Δ(m)	m	Δ(m)	m	Δ(m)
2	–378	20	6336	48	6918
3	–216	21	2592	54	2592
4	–450	22	720	60	65760
6	–864	24	11136	66	8640
8	–576	26	864	72	4320
9	–216	28	3024	78	12960
10	–576	30	29664	84	20304
12	1008	36	7776	90	7776
14	432	39	864	120	23040
15	1728	40	6336	156	6912
18	4824	42	56160	180	6912

References.

[A1] Aoki, N., On Some Arithmetic Problems Related to the Hodge Cycles on the Fermat Varieties, Math. Ann. 266 (1983), 23-54.

[A2] Some new algebraic cycles on Fermat varieties, J. Math. Soc. Japan. 39 (1987), 385-396.

[A-S] Aoki, N., and Shioda, T. Generators of Néron-Severi group of Fermat surfaces, Progress in Math. 35 (1983), 1-12.

[C] Coleman, R., Torsion points on abelian etale coverings of $\mathbf{P}^1 - \{0, 1, \infty\}$ (preprint).

[D] Deligne, P., Hodge cycles on abelian varieties, Springer Lect. Notes in Math. 900 (1982).

[Ka] Katz, N., On the intersection matrix of a hypersurfase, Ann. Sci. Ecole Norm. Sup. 2 (1969), 583-598.

[Ko] Koblitz, N., Gamma function identities and elliptic differentials on Fermat curves, Duke Math. 45 (1978), 87-99.

[K-O] Koblitz, N. and Ogus, A., Algebraicity of some products of values of the Γ function, Appendix to Deligne's article in AMS Proc. Symp. Pure Math. 33 (1979), 343-345.

[K-R] Koblitz, N. and Rohrlich, D., Simple factors in the jacobian of a Fermat curve, Can. J. Math. 30 (1978), 1188-1205.

[K-L] Kubert, D. and Lang, S., *Modular Units,* Springer 1981.

[M-N] Meyer, W. and Neutsh, W., Fermatquadruple, Math. Ann. 256 (1981), 51-62.

[O] Ogus, A., Griffiths transversality in cristalline cohomology, Math. Ann. 108 (1978), 395-419.

[R] Ran, Z., Cycles on Fermat hypersurfaces, Comp. Math. 42 (1981), 121-142.

[Schm] Schmidt, C.-G., *Zur Arithmetik abelscher Varietäten mit komplexer Multiplikation,* Springer Lect. Notes in Math. 1082 (1984).

[S-T] Shimura, G. and Taniyama, Y., *Complex Multiplication of Abelian Varieties and its Applications to Number Theory,* Publ. Math. Soc. Japan 1961.

[S-K] Shioda, T. and Katsura, T., On Fermat varieties, Tôhoku Math.31 (1979), 97-115.

[S1] Shioda, T., The Hodge Conjecture for Fermat Varieties Math. Ann. 245 (1979), 175-184.

[S2] Shioda, T., Algebraic cycles on Abelian Varieties of Fermat Type, Math. Ann. 258 (1981), 65-80.

[S3] Shioda, T., On the Picard number of a Fermat surface, J. Fac. Sci. Univ. Tokyo 28 (1982), 725-734.

Noboru Aoki

Max-Planck-Institut für Mathematik

Gottfried-Claren-strasse 26

5300 Bonn 3, BRD

and

Department of Mathematics

Rikkyo University

Nishi-ikebukuro, Tokyo, 171 Japan