

Fermat 曲面の Picard 数

青木 昇 (東大・理)

0. $m > 1$ を整数とし、 n を偶数 > 0 とする。

X_m^n を n 次元 m 次の Fermat 多様体、即ち、

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

で定義された $\mathbb{P}_C^{n+1}$ 内の超曲面を表わすとする。

μ_m を 1 の m 乗根の群とすると、 $G_m^n = \underbrace{\mu_m \times \cdots \times \mu_m}_{n+2} / \text{diag.}$

は座標ごとに作用させることにより $\text{Aut } X_m^n$ の部分群とみなされる。そして、その指標群は

$$\hat{G}_m^n = \left\{ \alpha = (a_0, \dots, a_{n+1}) \mid a_i \in \mathbb{Z}, 0 \leq a_i < m, \sum_{i=0}^{n+1} a_i \equiv 0 \pmod{m} \right\}$$

と同一視される。 $(\alpha = (a_0, \dots, a_{n+1}), \beta = (\zeta_0, \dots, \zeta_{n+1}))$ に対し $\alpha(\beta) = \zeta_0^{a_0} \cdots \zeta_{n+1}^{a_{n+1}}$ とおく。)

その部分集合として、 $\mathcal{O}_m^n, \mathcal{B}_m^n, \mathcal{Q}_m^n$ を次のように定義する。

$$\mathcal{O}_m^n = \left\{ \alpha = (a_0, \dots, a_{n+1}) \in \hat{G}_m^n \mid 0 < a_i < m \right\}$$

$$\mathcal{B}_m^n = \left\{ \alpha = (a_0, \dots, a_{n+1}) \in \mathcal{O}_m^n \mid \sum_{i=0}^{n+1} \left\langle \frac{ta_i}{m} \right\rangle = \frac{n}{2} + 1, \forall t \in \mathbb{Z}, (t, m) = 1 \right\}$$

$$\mathcal{Q}_m^n = \left\{ \alpha \in \mathcal{O}_m^n \mid \alpha \sim (a_0, m-a_0, \dots, a_{n/2}, m-a_{n/2}) \right\}.$$

ここで、 $\langle x \rangle$ は x の小数部分を表わし、 $\sim$ は成分の置換を除いて等しいことを表わす。

定義から $\mathcal{O}_m^n \supset \mathcal{O}_m^{n-1} \supset \mathcal{O}_m^{n-2}$ が判る. 以上の記号の下に次のことが知られている。(cf. [4])

$$H^n(X_m^n, \mathbb{C}) = V(0) \oplus \bigoplus_{\alpha \in \mathcal{O}_m^n} V(\alpha), \quad \dim V(\alpha) = 1.$$

ここで, $V(\alpha) = \{ \xi \in H^n(X_m^n, \mathbb{C}) \mid g^*(\xi) = \alpha(g)\xi \quad \forall g \in G_m^n \}$,
 $V(0)$ は自明な指標に対する固有空間.

更に, Hodge cycle に関して

$$(H^{\frac{n}{2}, \frac{n}{2}}(X_m^n) \cap H^n(X, \mathbb{Q})) \otimes_{\mathbb{Q}} \mathbb{C} = V(0) \oplus \bigoplus_{\alpha \in \mathcal{O}_m^{2n}} V(\alpha).$$

特に $n = 2$, 即ち Fermat 曲面の場合には,

Lefschetz の定理により,

$$NS(X_m^2) \otimes_{\mathbb{Z}} \mathbb{C} = V(0) \oplus \bigoplus_{\alpha \in \mathcal{O}_m^2} V(\alpha)$$

となる. ここで $NS(X_m^2)$ は X_m^2 の Néron-Severi 群を表わす. よって, その Picard 数を $\rho(X_m^2)$ と書くと,

$$\rho(X_m^2) = 1 + \#\mathcal{O}_m^2.$$

が成り立つ. 塩田先生は次の式を予想された([5]).

Theorem A.

$$\rho(X_m^2) = 3(m-1)(m-2) + 1 + \delta_m + 48\left(\frac{m}{2}\right)^* + 24\left(\frac{m}{3}\right)^* + \varepsilon(m).$$

ここで, $\delta_m = 1$ if $m = \text{even}$, $= 0$ if $m = \text{odd}$,

$$(x)^* = x \text{ if } x \in \mathbb{Z}, = 0 \text{ otherwise.}$$

$$\varepsilon(m) = \sum_{1 < d \mid m} \Delta(d), \quad \Delta(d) = 0 \text{ for } d > 180.$$

詳しくは [5] を参照.

Th. A は次の Th. B を証明することにより示せる.

Theorem B $m > 180$ とする. $\alpha \in B_m^2$ が $G.C.D.(\alpha) = 1$ ならば、 α は次の 4 つの type のいずれかである.

(0) B_m^2 の元.

(1) $m = 2d$, $(i, d+i, m-2i, d)$; $(d, m) = 1$.

(2) $m = 2d$, $(i, d+i, d+2i, m-4i)$; $(d, m) = 1$.

(3) $m = 3d$, $(i, d+i, 2d+i, m-3i)$; $(d, m) = 1$.

(1), (2), (3) をそれぞれ type A, B, C と呼ぶ.

これまででは, (i) $(m, 6) = 1$ (ii) $m = 2$ の中, (iii) $m = 3$ の中なる場合について Th. B が成り立つことが [L1] の結果を用いて確かめられていた ([5]). $m \leq 180$ の時の例外的な元については [3] を参照. 我々の目標は Th. B の証明であるが, その前にいくつか準備しておく必要がある.

1. 以下当分の間, m はかつて自然数 ($m > 1$) とする. R_m を $\mathbb{Z}/m - \{0\}$ の元で生成された自由アーベル群とし, その元を $\sum_{a \in \mathbb{Z}/m - \{0\}} c_a(a)$; $c_a \in \mathbb{Z}$ と書くことにする. $a, b \in \mathbb{Z}/m - \{0\}$ に対し, $ab \neq 0$ ならば $(a)(b) = (ab)$, $ab = 0$ ならば $(a)(b) = 0$ とおく

ことにより R_m の乗法が定義できて R_m は環になる。 $\alpha = (a_0, \dots, a_{n+1}) \in \mathcal{O}_m^n$ に対し、 $i'(\alpha) = \sum_{i=0}^{n+1} (a_i) \in R_m$ とおくと、 $i: \mathcal{O}_m^n / \sim \hookrightarrow R_m$ である。次に、 G を $(\mathbb{Z}/m)^{\times}$ と同型な群とし、その同型を、 $t \in (\mathbb{Z}/m)^{\times} \mapsto \sigma_t \in G$ と書くことにする。 $a \in \mathbb{Z}/m - \{0\}$ に対し、

$$\theta(a) = \sum_{t \in (\mathbb{Z}/m)^{\times}} \left(\left\langle \frac{ta}{m} \right\rangle - \frac{1}{2} \right) \sigma_t \in \mathbb{Q}[G].$$

とおく。更に、 $\alpha = \sum c_a(a) \in R_m$ に対し、

$$\theta(\alpha) = \sum c_a \theta(a)$$

とすれば、 $\theta: R_m \rightarrow \mathbb{Q}[G]$ は加法群としての準同型になる。

$B_m = \text{Ker } \theta$ とおくと、 $i: \mathcal{O}_m^n / \sim \hookrightarrow B_m$ となる。又、

D_m を、 $\delta = (1) + (-1)$ で ($m = \text{偶数}$ のときは更に $m' = m/2$ で) 生成される R_m の ideal とすると、 $\theta(\delta) = \theta(m') = 0$ より $D_m \subset B_m$

となる。又、 $\mathcal{O}_m^n / \sim \xrightarrow{i} D_m$ も明らか。以上をまとめると、

$$\begin{array}{ccc} \text{Prop. 1-1} & i: \mathcal{O}_m^n / \sim & \hookrightarrow R_m \\ & \cup & \cup \\ & \mathcal{O}_m^n / \sim & \hookrightarrow B_m \\ & \cup & \cup \\ & \mathcal{O}_m^n / \sim & \hookrightarrow D_m \end{array}$$

(注: 左側は単なる集合であるが、右側は加法群 (更には自然に G -module) になっているので $\mathcal{O}_m^n$ の構造よりも B_m の構造の方が判りやすいのである。)

Def. 1-2 $\alpha = \sum c_a(a) \in R_m$ に対し, $|\alpha| = \sum |c_a|$ とおき,
 $l(\alpha) = \min \{|\beta| \mid \beta \equiv \alpha \pmod{D_m}\}$ とおく。これは
 α の長さと呼ぶ。

Lemma 1-3 $l(\alpha) = 0 \iff \alpha \in D_m$

Def. 1-4 $R_m^+ = \{\alpha = \sum c_a(a) \in R_m \mid c_a \geq 0\}$
 $B_m^+ = B_m \cap R_m^+.$

Lemma 1-5 R_m/D_m の代表元として R_m^+ の元がとれる。

☺ $-(\alpha) \equiv (-\alpha) \pmod{D_m}$ より明らか。 Q.E.D.

従って長さを問題にする時, $\alpha \in R_m^+$ と仮定してもかま
 ない。 R_m^+ の元 $\alpha = \sum c_a(a)$ を, $(\dots, \underbrace{a, \dots, a}_{c_a}, \dots)$ と
 書くことにする。 $i(\mathcal{O}_m^n/\mathcal{L}) \subseteq R_m^+$ であるから $\alpha = (a_0, \dots, a_{n+1})$
 $\in \mathcal{O}_m^n$ に対して, $i(\alpha)$ を, $(a_0, \dots, a_{n+1})$ と書く。

Prop. 1-6 $i(\mathcal{O}_m^n/\mathcal{L}) = \{\alpha \in B_m^+ \mid l(\alpha) = \text{even} \leq n+2\}$

特に $n=2$ の時, $i(\mathcal{O}_m^2/\mathcal{L}) = \{\alpha \in B_m^+ \mid l(\alpha) = 0 \text{ or } 4\}.$

☺ $\alpha = (a_0, \dots, a_{n+1}) \in B_m^+$

$$\iff \sum_{i=0}^{n+1} \varphi(a_i) = 0$$

$$\iff \sum_{i=0}^{n+1} \sum_{t \in \mathcal{O}_m^*} \left(\left\langle \frac{ta_i}{m} \right\rangle - \frac{1}{2} \right) \chi_t^{-1} = 0$$

$$\iff \sum_t \left(\sum_i \left(\left\langle \frac{ta_i}{m} \right\rangle - \frac{1}{2} \right) \right) \chi_t^{-1} = 0$$

$$\iff \sum_i \left(\left\langle \frac{ta_i}{m} \right\rangle - \frac{1}{2} \right) = 0 \quad \forall t \in \mathcal{O}_m^*$$

$$\iff \sum_i \left\langle \frac{ta_i}{m} \right\rangle = \frac{n}{2} + 1 \quad \forall t \in \mathcal{O}_m^* \iff \alpha \in \mathcal{L}_m^n.$$

$n=2$ の時, $l(x) \geq 2$ とおくと, $(a_0 + a_1 + a_2 + a_3 = 0 \text{ である})$
 $a_0 + a_1 = 0$ ならば " $a_2 + a_3 = 0$ とおき $l(x) = 0$ かつ $l(x) = 0$ である" である.

Def. 1-6 $\alpha = \sum C_a(a) \in R_m$ に対し, $\alpha = \sum_{d|m} (d) \alpha_d$;
 $\alpha_d = \sum_{(a,m)=d} C_a(a) \in R_{m/d}$ とおき, $\alpha_d \in \alpha$ の d -part と呼ぶ.
 特に, α_1 を α の primitive part と呼ぶ. したがって,

$$l_d(\alpha) = l(\alpha \text{ の } d\text{-part}) \text{ と書く.}$$

2. m の約数 f に対し, $PC(f)$ を $\text{mod } f$ の原始指標全体を表わす. (通常通り, $(a, f) > 1$ なる a に対しては $\chi(a) = 0$ としておく)
 自然な全射 $\mathbb{Z}/m \rightarrow \mathbb{Z}/f$ により $PC(f) \subseteq \mathbb{Z}/m$ に引きこまれたものも $PC(f)$ と書くことにする. 更に, $C(m) = \bigcup_{f|m} PC(f)$ とおく.

$C^-(m), C^+(m)$ をそれぞれ $\chi \in C(m)$ で $\chi(-1) = -1, 1$ となるものとし,
 $PC^-(f) = PC(f) \cap C^-(m), PC^+(f) = PC(f) \cap C^+(m)$ とおく. ここで
 $PC^-(f) = \emptyset$ となるのは $\text{ord}_2 m = 1$ 又は $m = 12$ の時であることに注意しておく.

$\chi \in C(m)$ 且, $\alpha = \sum C_a(a) \in R_m$ に対し,

$\chi(\alpha) = \sum C_a \chi(a)$ とおくと, $\chi: R_m \rightarrow \mathbb{C}$ は環の準同型になる.

Def. 2-1 各 $f|m$ に対し

$$A(f) \stackrel{\text{def}}{=} \bigcap_{\chi \in PC^-(f)} \text{Ker}(\chi: R_f \rightarrow \mathbb{C})$$

もしも, $PC^-(f) = \emptyset$ の時は便宜上 $A(f) = R_f$ とおく.

さて, m の約数 d に対し map $T_d: R_m \rightarrow R_{m/d}$ を
次のように定義する.

先づ, $a \in \mathbb{Z}/m - \{0\}$ に対し,

$$T_d(a) = \begin{cases} \frac{\varphi(m)}{\varphi(m')} \prod_{\substack{p|d, (m,a) \\ p \nmid m/d}} ((1 - (p^{-1})) (a')) & \dots \text{ if } (m,a) | d \\ 0 & \dots \text{ if } (m,a) \nmid d. \end{cases}$$

と置く. ここで, $m' = m/(m,a)$, $a' = a/(m,a)$.

次に, 一般の $\alpha = \sum c_a(a) \in R_m$ に対しては

$$T_d(\alpha) = \sum c_a T_d(a)$$

と定義する. 特に, $T_1(\alpha) = \alpha_1$: α の primitive part とする
ことに注意しておく. 次の Prop. の証明は [2] を参照.

Prop. 2-2 $x \in C(m)$ に対し, $e_x = \frac{1}{\varphi(m)} \sum_{t \in (\mathbb{Z}/m)^*} \bar{x}(t) \sigma_t^{-1} \in \mathbb{C}[G]$

と置く. 更に $f \in m$ の約数とし, $d = m/f$ と置く. この時,

$\alpha \in R_m$, $x \in PC(f)$ に対し

$$\theta(\alpha) e_x = x(T_d(\alpha)) s(\bar{x}) e_x$$

が成り立つ. ここで $s(\bar{x}) = \sum_{t \in (\mathbb{Z}/f)^*} \bar{x}(t) (\langle \frac{t}{f} \rangle - \frac{1}{2})$.

Prop. 2-3 $\alpha \in R_m$ が B_m に入るための必要十分条件は,

すべての $d|m$ に対し $T_d(\alpha) \in A(m/d)$ とたつことである.

$$(i) \alpha \in B_m \iff \theta(\alpha) = 0$$

$$\iff \theta(\alpha) e_x = 0 \quad \forall x \in C(m)$$

$$\Leftrightarrow \chi(\tau_d(\alpha))s(\bar{x})e_x = 0 \quad \forall x \in PC(m_d), \quad \forall d|m$$

$$\Leftrightarrow \chi(\tau_d(\alpha)) = 0 \quad \forall x \in PC^-(m_d), \quad \forall d|m$$

$$\Leftrightarrow \tau_d(\alpha) \in A(m_d) \quad \forall d|m, \quad \text{Q.E.D.}$$

さて、自然数 $l \geq 1$ に対して $A(m, l) = \{\alpha \in A(f) \mid \ell(\alpha) \leq l\}$ とおく。 $\alpha \in A(m, l), \alpha' \in A(m, l')$ とすると、 $\alpha + \alpha' \in A(m, l+l')$ であるが、この時特に $\alpha \oplus \alpha'$ と書くことにする。更に $A(m, l) \oplus A(m, l')$ も同様である。 $A^0(m, l) = A(m, l) \setminus \bigcup_{0 \leq i \leq l} A(m, i) \oplus A(m, l-i)$ とおく。 $(a, m) > 1$ ならば $(a) \in A(m)$ であるから $l > 1$ の時、 $A^0(m, l)$ は $(PC^-(m) = \emptyset \text{ ではない限り})$ primitive part のみからなることに注意しておく。

3. ここで $PC^-(m) \neq \emptyset$ 、即ち、 $\text{ord}_2 m \neq 1, m \neq 12$ とおく。

$$\begin{aligned} \text{Def. 3-1. } U(m) & \stackrel{\text{def}}{=} \bigcap_{x \in PC^-(m)} \{a \in (\mathbb{Z}/m)^* \mid \chi(a) = 1\} \\ & = \{a \in (\mathbb{Z}/m)^* \mid (1, -a) \in A(m)\}. \end{aligned}$$

以下、 $U(m)$ の構造を調べる。先づ、 u_ε, v_δ を次のように定義する。 m が偶数のとき ($m = 2d$ とおいて) $\varepsilon = \pm 1$ に対して、

$$u_\varepsilon = u_{m, \varepsilon} = 1 \text{ if } \varepsilon = 1, \quad d-1 \text{ if } \varepsilon = -1.$$

とおく。 $\text{ord}_3 m = 1$ のとき ($m = 3d$ とおいて) $\delta = \pm 1$ に対して

$$v_\delta = v_{m, \delta} = \begin{cases} 1 & (\text{mod. } 3) \\ \delta & (\text{mod. } d) \end{cases}$$

で定まる $\mathbb{Z}/m$ の元. と定義する. 便宜上, $m = \text{奇数}$ の時 $u_\varepsilon = 1$.
and, $m \neq 1$ の時 $v_\sigma = 1$ としておく. この時, 容易に u_ε, v_σ
 $\in U(m)$ が成り立つ. ことが示せるが. 逆に次が成り立つ.

Prop. 3-2 $PC^-(m) \neq \emptyset$ とする. この時.

$$U(m) = \{ u_\varepsilon v_\sigma \mid \varepsilon, \sigma = \pm 1 \}.$$

Rem. 3-3 $u_{m, \varepsilon}, v_{m, \sigma}$ は m に依存する $\mathbb{Z}/m$ の元で
あるが. $\mathbb{Z}/m$ で考えていることが明らかな場合は m を省略
する.

4. この § において, $A(m)$ の構造に関するいくつかの事実を述べて
おく. ここで m 3. と同様に $PC^-(m) \neq \emptyset$ としておく.

Def. 4-1 p を m の素因数とす. $d = m/p$ とおき, $pi \not\equiv 0 \pmod{m}$

なる i に対して, $(i, d+i, 2d+i, \dots, (p-1)d+i, -pi) \in R_m$ なる

形の $\bar{\alpha} \in p\text{-standard type}$ と呼ぶ. ($p=2$ の時は上の代わりに

$(i, d+i, m-2i, d); d = \frac{m}{2}$ を取る.) 更に, $(a_1, \dots, a_k)$ が

ある $p\text{-standard type}$ の primitive part である時.

$\alpha = (a_1 u_1, \dots, a_k u_k); u_i \in U(m)$ なる形の $\alpha \in$.

$p\text{-quasi-standard type}$ と呼ぶ.

Prop. 4-2 (i) α が standard type ならば $\alpha \in B_m$

(ii) α が quasi-standard type ならば $\alpha \in A(m)$.

Prop. 4-3 $PC^-(m) \neq \emptyset$ となる。もし $\alpha = (1, a, b) \in A^0(m, 3)$ ならば

(1) $\text{ord}_3 m \leq 1$ のときは $m = 21$ or 28 .

(2) $\text{ord}_3 m > 1$ のときは α は 3-quasi-standard type

即ち $\alpha = (1, (d+1)u, (2d+1)u')$; $u, u' \in U(m)$, $d = m/3$

Prop. 4-4 $PC^-(m) \neq \emptyset$, $m > 28$ とする。もし $\alpha = (1, a, b, c) \in A^0(m, 4)$ の元ならば α は 5-quasi-standard である。

Prop. 4-5 m を奇数とする。 $\nu \in \mathbb{Z}/m$ を $2\nu \equiv -1$ となる元。

ℓ を 次を満足する最小の整数とする

(1) $m > 105$, $\neq 315$ のとき $4 \leq \ell \leq 8$

(2) $m = 315$ のとき $4 \leq \ell \leq 6$.

この時 $\alpha = (1, \nu, * \cdots *) \in A(m, \ell)$ は $A^0(m, \ell)$ に入らない。

Cor. 4-6 m を奇数 > 105 とする。 $\alpha = (1, a, b)$; $a, b \in (\mathbb{Z}/m)^*$ に対し、 $(1, \nu)\alpha \in A(m, 6)$ ならば $\alpha \in A(m, 3)$

Cor. 4-7 m を奇数 > 315 とする。 $\alpha = (1, a, b, c)$; $a, b, c \in (\mathbb{Z}/m)^*$ に対し、 $(1, \nu)\alpha \in A(m, 8)$ ならば $\alpha \in A(m, 4)$

Cor. 4-8 m を奇数 > 105 とする。 $\alpha = (1, \nu)(1, a) + (b)$; $a, b \in (\mathbb{Z}/m)^*$ に対し $\alpha \in A(m)$.

Cor. 4-9 m を奇数 > 105 とする。 $\alpha = (1, \nu)(1, a) + (b, c)$; $a, b, c \in (\mathbb{Z}/m)^*$ に対し、 $\alpha \in A(m, 6)$ ならば 次の 4) のとき

合のみが可能である。

$$(1) \quad (1, a), (b, c) \in A(m, 2)$$

$$(2) \quad (1, a, b) \in A(m, 3) \text{ から } (b, 2c) \in A(m, 2)$$

$$(3) \quad a = 2u, b = -2u', c = 2^{-1}u''$$

$$(4) \quad a = 2^{-1}u, b = -u, c = 4^{-1}u''$$

$$\text{ここで } u, u', u'' \in U(m).$$

5. いよいよ Th. B の証明に入る。その為、 $m > 630$ と仮定しておく。($m \leq 672$ の時は Th. B の成立することが [5] で確かめられている。) まず $\alpha = (a_0, a_1, a_2, a_3) \in \mathcal{O}_m^2$ に対して

$$a_0 + a_1 + a_2 + a_3 \equiv 0 \pmod{m} \text{ となることに注意しておく。}$$

$$d_i = \text{G.C.D.}(a_i, m) \text{ とおき、 } a_i' \text{ は } a_i/d_i \text{ を表すものとする。}$$

証明は $l_1(\alpha) = 0, 1, 2, 3, 4$ の場合に応じて 5 つの部分に分かれるが、ここでは $l_1(\alpha) = 2, 3$ の場合についてのみ述べることにする。(type A, B, C が出てくるのはこの場合と、 $l_1(\alpha) = 1$ なる場合である。)

(I). $l_1(\alpha) = 3$ の時.

$\alpha = (1, a, b, c)$; $\text{G.C.D.}(c, m) > 1$ としてよい。最初に $\gcd_2 m \neq 1$ の時を考える。この時は、 $T_1(\alpha) = (1, a, b) \in A(m, 3)$ だから Prop 4-3 により $\gcd_3 m > 1$ ($m = 3d$ とおく) であり

$\alpha = (1, (d+1)u, (2d+1)u', c)$; $u, u' \in U(m)$ である。
 ここで、もしも m が奇数ならば $U(m) = \{1\}$ から (Prop. 3-2)
 $u = u' = 1$ とより $\alpha = (1, d+1, 2d+1, m-3)$ 。即ち、type C。
 m が偶数ならば $u = u_\varepsilon, u' = u_{\varepsilon'}$ とおくと、

$1+a+b \equiv 1+\varepsilon+\varepsilon' \pmod{d/2}$ 。よって、 $c \equiv -3, \pm 1 \pmod{d/2}$ 。
 $G.C.D.(c, m) > 1$ から $c \equiv -3 \pmod{d/2}$ のみ
 可能であるが、これは $\varepsilon = \varepsilon' = 1$ のときである。即ち $u = u' = 1$ 。
 従って、この時も α は type C である。

次に、 $\text{ord}_2 m = 1$ の時。この時は、

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

従って、Cor 4-6 より (今は $m > 630$ から $m/2 > 315 > 105$)

$(1, a, b) \in A(m/2)$ を得る。以下、上と同様にして type C が示せる。

(II). $\ell_1(\alpha) = 2$ の時

$$\alpha = (1, a, b, c); G.C.D.(b, m) > 1, G.C.D.(c, m) > 1 \text{ としてよい。}$$

最初に $\text{ord}_2 m \neq 1$ の時を考へる。 $e = \text{ord}_2 m$ とおき、 $\lambda \in e=2a$ 時は
 $\lambda=2$ 、 $e \neq 2a$ 時は $\lambda=1$ とおく。 $\tau_1(\alpha) = (1, a) \in A(m)$ であるから
 $a = -u_\varepsilon v_\delta$ と書ける。

(1). もし、 $d_2, d_3 \nmid 2^\lambda$ ならば $e=1$ である。

⊙ 実際、 $d_2, d_3 \nmid 2^\lambda$ ならば、 $e=2, \neq 2$ に従い、

$$\tau_2(\alpha) = (1, -\varepsilon v_\delta), (1, -2^{-1})(1, -\varepsilon v_\delta)$$

と仮定から $(1, -\varepsilon v_0) \in A(m/2)$ を得る。これは $\varepsilon = 1$ を意味する。

(2). もしも、 $d_2, d_3 \neq 3$ ならば $\delta = 1$.

⊙ もしも $\delta = -1$ ならば (必然的に $\text{ord}_3 m = 1$ であり)

$$\tau_3(\alpha) = (1, -3^{-1})(1, -\delta u_\varepsilon) = (1, -3^{-1})(1, u_\varepsilon) \in A(m/3).$$

よって $(1, -3^{-1}) \in A(m/3)$ となるが ($m > 630$ である) これは不可能である。

(3). もし $\alpha \notin \mathcal{Q}_m^2$ ならば d_2 か d_3 の少なくとも一方は 2^k かつ $k \geq 1$ を割り切る。

⊙ これは (1) と (2) からの帰結である。(i.e. $\varepsilon = \delta = 1 \Rightarrow \alpha \in \mathcal{Q}_m^2$).

(4). もしも $d_2 = 3$ or $d_3 = 3$ ならば $d_2 = d_3 = 3$ である。

⊙ $d_2 = 3, d_3 \neq 3$ と仮定して矛盾を出す。実際この時は

$$\tau_3(\alpha) = \begin{cases} (1, -3^{-1})(1, -\delta u_\varepsilon) + 2(b') \in A(m/3) & \text{if } \text{ord}_3 m = 1 \\ (1, -u_\varepsilon) + 3(b') & \in A(m/3) \dots \text{if } \text{ord}_3 m \neq 1. \end{cases}$$

ここで $b' = b/3$ 。よってどちらの場合も不可能である。何故なら、例えば $\text{ord}_3 m = 1$ の時、もし $\delta = 1$ ならば $(b') \in A(m/3)$ となり矛盾、もし $\delta = -1$ ならば $(1, -3^{-1}, b') \in A(m/3)$ となり (今は $m > 630$ であるから $m/3 > 210 > 28$ である) Prop. 4-3 より) 矛盾。下の場合も同様である。

(5). もしも $d_2 = d_3 = 3$ ならば $\alpha \in \mathcal{Q}_m^2$ か type C である。

⊙ 先ず (1) より $\varepsilon = 1$ である。 $\delta = 1$ ならば $\alpha \in \mathcal{Q}_m^2$ であるから $\delta = -1$ (従って $\text{ord}_3 m = 1$) とする。この時は

$$\tau_3(\alpha) = (1, -3^{-1})(1, -\delta) + 2(b', c') = 2(1, -3^{-1}, b', c') \in A(m/3).$$

よって $b' = b/3, c' = c/3$ 。従って Prop. 4-4 より $(1, -3^{-1}$

$-3^{-1} + b' \equiv 1 + c' \equiv 0 \pmod{m/3}$ を得る。 $d = m/3$ とおいて。

$\alpha = (1, d+1, 2d+1, m-3)$ を得る。 実際 $b' \equiv 3^{-1} \pmod{d}$ より

$b \equiv 1 \pmod{d}$. $c' \equiv -1 \pmod{d}$ より $c \equiv -3 \pmod{d}$ であるから。

(6). $d_2, d_3 \neq 3$ ならば $\alpha \in \mathcal{Q}_m^2$ 又は type A or B.

これを更にいくつかの step に分けて証明する。

(7). $d_2, d_3 \neq 3, \alpha \notin \mathcal{Q}_m^2$ ならば $a = d+1, d = m/2$.

☺ (2) と (4) より $\delta = 1$. $\alpha \notin \mathcal{Q}_m^2$ であるから $\varepsilon = -1$. 即ち $a = d+1$.

(8). $e = \text{ord}_2 m > 2$ ならば ($\alpha \notin \mathcal{Q}_m^2$ とし) α は type A or B.

☺ (7) より $a = d+1$. であるから $\tau_2(\alpha) = (1, 1) + \tau_2(b, c) \in A(d)$ より $d_2 = 2, d_3 \neq 2$ である。 何故なら. (3) より $d_2 = 2$ としてよいから. 更に $d_3 = 2$ とすると $\tau_2(\alpha) = 2(1, b', c') \in A(d)$. すると $\text{ord}_2 d > 1$ としてよいから $\tau_6(\alpha) = 2(1, b', c') \pmod{d/3} \in A(d/3)$. しかしこれは Prop. 4-3 より不可能. すると $d_3 \neq 2$. 従って $\tau_2(\alpha) = 2(1, b') \in A(d)$. 故に $b' = -u_{\varepsilon'} v_{\delta'}$; $u_{\varepsilon'}, v_{\delta'} \in U(d)$ を得る. (2) の時と同様にして $\delta' = 1$ としてよい. もしも $\varepsilon' = 1$ ならば $b' \equiv -1 \pmod{d}$ であるから $b \equiv -2 \pmod{d}$. これは $\alpha = (1, d+1, m-2, d)$ の時のみ可能である. 即ち. type A. もしも $\varepsilon' = -1$ ならば $b' \equiv d/2 + 1 \pmod{d}$. すると $b \equiv 2 \pmod{d}$. これは $\alpha = (1, d+1, d+2, m-4)$ の時のみ可能. 即ち. type B.

(9). $e = 2$ の時 次の 3 つの場合がある。

$$\begin{array}{ll}
 (i) & (b, 4) = (c, 4) = 2. \\
 (ii) & (b, 4) = 2, (c, 4) = 4 \\
 (iii) & (b, 4) = (c, 4) = 4.
 \end{array}
 \left\{ \begin{array}{l} \text{1x下.} \\ b' = b/(b, 4) \\ c' = c/(c, 4) \end{array} \right. \text{とおく.}$$

(10). (i) は不可能である。

⊙ $\tau_4(\alpha) = 2(1, -2^{-1})(1, b', c') \in A(m/4)$. ここで $m/4 > 630/4 > 105$ であるから Cor 4-6 により $(1, b', c') \in A(m/4)$. (7) のときの証明と同様にしてこれは不可能である。

(11) (ii) の時は α は type A である。

⊙ $\tau_4(\alpha) = 2\{(1, -2^{-1})(1, b') + (c')\} \in A(m/4)$. ここでこれは Cor 4-8 より $(c', m/4) > 1$ ではないと不可能である。即ち、実際には

$$\tau_4(\alpha) = 2(1, -2^{-1})(1, b') \text{ である。}$$

よて、 $(1, b') \in A(m/4)$ より、 $b' = -2b''; b'' \in U(m/4)$. $\tau_2(\alpha) \in A(m/2)$ を考えれば $b'' = 1$ が判るから $b' \equiv -1 \pmod{m/4}$. よて $b \equiv -2 \pmod{m/2}$. これは $\alpha = (1, d+1, m-2, d)$ の時のみ可能である。即ち、type A.

(12). (iii) の時は α は type B である。

⊙ $\tau_4(\alpha) = 2(1, -2^{-1}, b', c') \in A(m/4)$. 必要ならば $\tau_2(\alpha)$ を考えれば $-2^{-1} + b' \equiv 1 + c' \equiv 0 \pmod{m/4}$ が判る。即ち、

$b \equiv 2, c \equiv -4 \pmod{m/2}$. これは $\alpha = (1, d+1, d+2, m-4)$ の時のみ可能である。即ち type B.

以上で $\text{ord}_2 m \neq 1$ の時の証明が終ったことになる。

そこで次に $\text{ord } m = 1$ と仮定する.

(13). もし $d_2, d_3 \neq 2$ ならば $\alpha = -v_\delta$, $v_\delta \in U(m)$.

⊙ 実際 $\tau_2(\alpha) = (1, -2^{-1})(1, a) \in A(m/2)$. よって $(1, a) \in A(m/2)$.

従って Prop. 3-2 から (13) は明らか.

(14). $\alpha \notin \mathfrak{A}_m^2$ ならば d_2 か d_3 の少なくとも一つは $6 \nmid$ 割る.

⊙ $d_2, d_3 \nmid 6$ と仮定する. この時 $\text{ord } m = 1, \neq 1$ に依りて

$\tau_6(\alpha) = (1, -3^{-1})(1, \sigma)$, $(1, \sigma) \in A(m/6)$. 従って $\sigma = 1$, i.e. $\alpha \in \mathfrak{A}_m^2$.

(15). $d_2 = d_3 \mid 6$. ($\alpha \notin \mathfrak{A}_m^2$ の仮定の下で).

⊙ (14) より $d_2 \mid 6$ と仮定してよい.

(i) $d_2 = 2$ の時. $\checkmark$ $\tau_2(\alpha) = (1, -2^{-1})(1, a) + (b') \in A(m/2)$. $b' \neq 0$ かつ Con. 4-8 よりこれは不可能. よって $d_2 = d_3 = 2$.

(ii) $d_2 = 3$ の時. この時は (4) と同様にして $d_3 = 3$ が示せる.

(iii) $d_2 = 6$ の時. $d_2 = d_3 = 6$ を示すには (i)(ii) より $d_3 \mid 6$ を示さなければよい. 仮に $d_3 \nmid 6$ とすると. (13) より $\alpha = -v_\delta$, $\delta = -1$ としてよい. $\tau_6(\alpha) = 2 \{ (1, -2^{-1})(1, -3^{-1}) + (b') \} \notin A(m/6)$ (Prop. 4-8) となり矛盾. よって $d_2 = d_3 = 6$.

(16). $d_2 = d_3 = 2$ の時. α は type B.

⊙ $\tau_2(\alpha) = (1, -2^{-1})(1, a) + (b', c') \in A(m/2)$. 従って Con. 4-9 により 4つの場合が可能であるが. 実際には (1) と (3) の場合のみ可能である. (1) の時には $\alpha \in \mathfrak{A}_m^2$. (3) の時には $\alpha = (1, d+2, m-4, d+1)$ と

たり type B である。

(17). $d_2 = d_3 = 3$ の時. α は type C である。

(*) $\tau_6(\alpha) = (1, -2^{-1})(1, -3^{-1}, b', c') \in A(m/6)$ であるか. $m > 630$

より $m/6 > 105$, $m/6 \neq 315$. 故から $(1, -3^{-1}, b', c') \in A(m/6)$.

これから容易に. $b' \equiv 3^{-1}$, $c' \equiv -1 \pmod{m/6}$ としてよいことが判る。

よて. $b \equiv 1$, $c \equiv -3 \pmod{m/6}$. これは $\alpha = (1, m^2+1, 2m^2+1, m^3)$

即ち. type C のときのみ可能である。

(18). $d_2 = d_3 = 6$ のときは起こらない。

(*) $\tau_6(\alpha) = \sum \{ (1, -2^{-1})(1, -3^{-1}) + (b', c') \}$ であるか. Con 4-9.

における (1) ~ (4) のすべての場合が不可能なことが判るのである。

以上で $\text{ord}_2 m = 1$ の時. Th. B の証明が完成した。従って. $l_1(\alpha) = 2$ 或 3 の時の証明が終った訳である。最後にその他の場合について簡単に述べておく。

ておく。 $l_1(\alpha) = 4$ となるときは. $\alpha \in \mathcal{O}_m^2$. $l_1(\alpha) = 1$ となるのは.

$\text{ord}_2 m = 1$ で. $\alpha = (1, d+1, m-2, d)$; $d = m/2$. i.e. type A. となる時。

である。さて. $l_1(\alpha) = 0$ の時は $\alpha \in \mathcal{O}_m^2$. 証明は $l_1(\alpha) = 2, 3$ の場合と同様な (そして退屈な) 計算で示せる。

文献.

- [1] N. Koblitz, D. Rohrlich : Simple factors in the Jacobian of a Fermat curve. *Can. J. Math.* 30 (1978) 1183-1205.
- [2] D. Kubert, S. Lang : *Modular Units*, Springer Verlag (1981)
- [3] W. Meyer, W. Neutsh : Fermatquadrupel. *Math. Ann.* 256 (1981) 51-62.
- [4] T. Shioda : The Hodge conjecture for Fermat varieties. *Math. Ann.* 245 (1979) 175-184.
- [5] T. Shioda : On the Picard number of a Fermat surface. *J. Fac. Sci. Univ. Tokyo* 28 (1982) 725-734.