# Properties of phase transformation equations for periodic products

Hajime Mashima

**Abstract**

General solution conditions applies when the equation of Fermat's proposition can be phase-transformed by a periodic product.

## Contents

# 1 introduction

この演算を算術の余白に書くには狭すぎる。

## 1.1 $\delta \perp xyz$ の導出

**Theorem 1 (Fermat's Last Theorem)**

$$x^p + y^p \neq z^p \quad (p \geqq 3 \text{ であり } x\ ,\ y\ ,\ z \text{ は互いに素で一つが偶数})$$

**Proposition 2** $p$ が奇素数で $x^p + y^p = z^p$ を満たすとき

$$p \mid x \quad , \ p \perp yz \quad \Rightarrow \quad p^n \mid x \ (n \geqq 2) \ , \ p^{np-1} \mid z - y$$

**Proof 3** $(x + y - z)^p = x^p + y^p - z^p + p\,(\cdots \text{省略})$

$x^p + y^p - z^p = 0 \Rightarrow p \mid (x + y - z)^p$

よって $p \mid x \Rightarrow p \mid (z - y)$

一般的に

$$(y + z - y)^p = y^p + (z - y)\,(\cdots)$$

$$z^p - y^p = (z - y)\left(py^{p-1} + \frac{p!}{(p-2)!2!}y^{p-2}(z-y) + \cdots + \frac{p!}{1!(p-1)!}y(z-y)^{p-2} + (z-y)^{p-1}\right)$$

$$x^p = (L)\,(R)$$

$$R = py^{p-1} + \frac{p!}{(p-2)!2!}y^{p-2}(z-y) + \cdots + \frac{p!}{1!(p-1)!}y(z-y)^{p-2} + (z-y)^{p-1}$$

$p^2 \mid R \Rightarrow p \mid y^{p-1}$ となり前提に反するので

$$R = pK \quad , \ (p \perp K) \tag{1}$$

また$p$ を除く素数に関して、$py^{p-1} \perp z - y$ なので

$$L \perp R \ (p \text{ を除く}) \tag{2}$$

**Definition 4** (1), (2) より $p \perp abc$ として以下のように置ける。

- $x^p = (z-y)(\cdots) = p^{p-1}a^p(\cdots)$
- $y^p = (z-x)(\cdots) = b^p(\cdots)$
- $z^p = (x+y)(\cdots) = c^p(\cdots)$

$$\begin{aligned}(z-x)-(x+y) &= b^p - c^p \\ (z-y)-2x &= b^p - c^p \equiv 0 \mod p\end{aligned}$$

$b^p - c^p = (b-c)R'$ と置くと $p \mid (b-c) \Leftrightarrow p \mid R'$ なので

$$p^{p-1}a^p - 2x = b^p - c^p \equiv 0 \mod p^2$$

よって、少なくとも

$$p^2 \mid x$$

$x = p^2 a\alpha$ と仮定すると

$$x^p = p^{2p}a^p\alpha^p$$

(1) より $x^p = (z-y)\cdot p\alpha^p$ なので

$$z - y = p^{2p-1}a^p$$

一般的に

$$p^n \mid x \ (n \geqq 2) \Rightarrow p^{np} \mid x^p \quad \Rightarrow \quad p^{np-1} \mid z-y$$

□

また

$$\begin{aligned}x+y-z &= x-(z-y) \\ x+y-z &= p^n a\alpha - p^{np-1}a^p \\ x+y-z &= p^n(a\alpha - p^{n(p-1)-1}a^p)\end{aligned}$$

$$p^n \mid x+y-z \tag{3}$$

### 1.1.1 $p \mid x$ のとき

$$
\begin{aligned}
x &= p^n a\alpha & z - y &= p^{np-1}a^p \\
y &= b\beta & z - x &= b^p \\
z &= c\gamma & x + y &= c^p \\
p &\perp a\alpha yz & \delta &= \text{奇素数 (definition)}
\end{aligned}
$$

**Proposition 5** $x + z - y = p^n aS \quad , \ \delta \mid S \ \Rightarrow \ \delta \perp xyz$

**Proof 6**

$$
\begin{aligned}
x + z - y &= p^n a\alpha + p^{np-1}a^p \\
&= p^n a(\alpha + p^{(p-1)n-1}a^{p-1}) \\
p &\perp S \quad , \ p \perp \delta \\
p\alpha^p &= R = py^{p-1} + (z - y)(\ldots) \\
R &\equiv py^{p-1} \mod a \\
py^{p-1} &\perp a \\
\alpha &\perp a
\end{aligned}
$$

$\delta \mid S$ のとき $\delta \mid a$ または $\delta \mid \alpha$ ならば上記と矛盾するので

$$\delta \perp x$$

$$
\begin{aligned}
2x &= (x + y - z) + (x + z - y) \\
bc &\mid x + y - z \\
x &\perp bc
\end{aligned}
$$

$\delta \mid bc$ ならば $\delta \mid 2x$ でなければならず矛盾するので

$$\delta \perp bc$$

$\delta \mid \beta$ ならば $\delta \mid x + z$

$$
\begin{aligned}
x &\equiv -z \mod \delta \\
x^p &\equiv -z^p \mod \delta \\
x^p + z^p &\equiv 0 \mod \delta
\end{aligned}
$$

$z^p - x^p = y^p \equiv 0 \mod \delta$ なので

$$
\begin{aligned}
x^p + z^p - (z^p - x^p) &\equiv 0 \mod \delta \\
2x^p &\not\equiv 0 \mod \delta
\end{aligned}
$$

よって $\delta \perp \beta$

$\delta \mid \gamma \quad , \ \delta \mid x - y$ ならば同様に

$$
\begin{aligned}
x^p - y^p + (x^p + y^p) &\equiv 0 \mod \delta \\
2x^p &\not\equiv 0 \mod \delta
\end{aligned}
$$

よって $\delta \perp \gamma$ □

### 1.1.2 $p \perp x$ のとき ($p \mid yz$ 条件は省略 )

$$\begin{aligned} x &= a'\alpha' & z - y &= a'^p \\ y &= b'\beta' & z - x &= b'^p \\ z &= c'\gamma' & x + y &= c'^p \\ p &\perp xyz & \delta &= \text{奇素数 (definition)} \end{aligned}$$

**Proposition 7** $x + z - y = a'S' \quad , \ \delta \mid S' \ \Rightarrow \ \delta \perp xyz$

**Proof 8**

$$\begin{aligned} x + z - y &= a'\alpha' + a'^p \\ &= a'(\alpha' + a'^{p-1}) \end{aligned}$$

$p \perp x$ , (3) より $p \perp S' \quad , \ p \perp \delta$

$$\begin{aligned} \alpha'^p = R &= py^{p-1} + (z - y)(\ldots) \\ R &\equiv py^{p-1} \mod a' \\ py^{p-1} &\perp a' \\ \alpha' &\perp a' \end{aligned}$$

$\delta \mid S'$ のとき $\delta \mid a'$ または $\delta \mid \alpha'$ ならば上記と矛盾するので

$$\delta \perp x$$

$$\begin{aligned} 2x &= (x + y - z) + (x + z - y) \\ b'c' &\mid x + y - z \\ x &\perp b'c' \end{aligned}$$

$\delta \mid b'c'$ ならば $\delta \mid 2x$ でなければならず矛盾するので

$$\delta \perp b'c'$$

$\delta \mid \beta'$ ならば $\delta \mid x + z$

$$\begin{aligned} x &\equiv -z \mod \delta \\ x^p &\equiv -z^p \mod \delta \\ x^p + z^p &\equiv 0 \mod \delta \end{aligned}$$

$z^p - x^p = y^p \equiv 0 \mod \delta$ なので

$$\begin{aligned} x^p + z^p - (z^p - x^p) &\equiv 0 \mod \delta \\ 2x^p &\not\equiv 0 \mod \delta \end{aligned}$$

よって $\delta \perp \beta'$

$\delta \mid \gamma' \quad , \ \delta \mid x - y$ ならば同様に

$$\begin{aligned} x^p - y^p + (x^p + y^p) &\equiv 0 \mod \delta \\ 2x^p &\not\equiv 0 \mod \delta \end{aligned}$$

よって $\delta \perp \gamma'$ □

$z-y \mid x^p$ , $z-x \mid y^p$ , $x+y \mid z^p$ であるから

$$\begin{aligned} z-y &\not\equiv 0 \mod \delta \\ z-x &\not\equiv 0 \mod \delta \\ x+y &\not\equiv 0 \mod \delta \end{aligned}$$

## 1.2 解の条件 (Solution conditions)

$\theta \perp xyzUT$ のとき、$y, z$ の逆元が存在するので合同式を満たす範囲で任意の文字式で表すことができる。

$$x^p + Uz^{p-1} \equiv Ty^{p-1} \mod \theta$$

$$\begin{aligned} z^p - y^p + Uz^{p-1} &\equiv Ty^{p-1} \mod \theta \\ z^p + Uz^{p-1} &\equiv Ty^{p-1} + y^p \mod \theta \\ z^{p-1}(z+U) &\equiv y^{p-1}(T+y) \mod \theta \\ z^{p-1}(yz+yU) &\equiv y \cdot y^{p-1}(T+y) \mod \theta \end{aligned} \tag{4}$$

$Uz^{p-1} \cdot Ty^{p-1} \equiv y^p z^p \mod \theta$ ならば

$$yz \equiv UT \mod \theta$$

$$\begin{aligned} z^{p-1}(UT+yU) &\equiv y^p(T+y) \mod \theta \\ Uz^{p-1}(T+y) &\equiv y^p(T+y) \mod \theta \end{aligned}$$

同様に

$$\begin{aligned} z \cdot z^{p-1}(z+U) &\equiv y^{p-1}(zT+yz) \mod \theta \\ z^p(z+U) &\equiv y^{p-1}(zT+UT) \mod \theta \\ z^p(z+U) &\equiv Ty^{p-1}(z+U) \mod \theta \end{aligned}$$

よって合同式 (4) および $Uz^{p-1} \cdot Ty^{p-1} \equiv y^p z^p \mod \theta$ を満たすとき
解の候補は 3 通りである。

$$\begin{aligned} Uz^{p-1} &\equiv y^p \mod \theta \\ Ty^{p-1} &\equiv z^p \mod \theta \\ &or \quad , \ and \\ Uz^{p-1} &\equiv -z^p \mod \theta \\ Ty^{p-1} &\equiv -y^p \mod \theta \end{aligned} \tag{5}$$

$\theta \perp xyzU'T'$ のとき、$x, z$ の逆元が存在するので合同式を満たす範囲で任意の文字式で表すことができる。

$$-U'z^{p-1} + y^p \equiv -T'x^{p-1} \mod \theta$$

$$\begin{aligned} -U'z^{p-1} + z^p - x^p &\equiv -T'x^{p-1} \mod \theta \\ -U'z^{p-1} + z^p &\equiv x^p - T'x^{p-1} \mod \theta \\ -z^{p-1}(U' - z) &\equiv x^{p-1}(x - T') \mod \theta \\ -z^{p-1}(U'x - xz) &\equiv x \cdot x^{p-1}(x - T') \mod \theta \end{aligned} \tag{6}$$

$-U'z^{p-1} \cdot -T'x^{p-1} \equiv x^p z^p \mod \theta$ ならば

$$xz \equiv U'T' \mod \theta$$

$$\begin{aligned} -z^{p-1}(U'x - U'T') &\equiv x^p(x - T') \mod \theta \\ -U'z^{p-1}(x - T') &\equiv x^p(x - T') \mod \theta \end{aligned}$$

同様に

$$\begin{aligned} -z \cdot z^{p-1}(U' - z) &\equiv x^{p-1}(xz - T'z) \mod \theta \\ -z^p(U' - z) &\equiv x^{p-1}(U'T' - T'z) \mod \theta \\ z^p(U' - z) &\equiv -T'x^{p-1}(U' - z) \mod \theta \end{aligned}$$

よって合同式 (6) および $-U'z^{p-1} \cdot -T'x^{p-1} \equiv x^p z^p \mod \theta$ を満たすとき解の候補は 3 通りである。

$$\begin{aligned} -U'z^{p-1} &\equiv x^p \mod \theta \\ -T'x^{p-1} &\equiv z^p \mod \theta \\ \quad or \quad &, \ and \\ -U'z^{p-1} &\equiv -z^p \mod \theta \\ -T'x^{p-1} &\equiv -x^p \mod \theta \end{aligned} \tag{7}$$

$\theta \perp xyzU"T"$ のとき、$x, y$ の逆元が存在するので合同式を満たす範囲で任意の文字式で表すことができる。

$$-U"y^{p-1} - T"x^{p-1} \equiv z^p \mod \theta$$

$$\begin{aligned} -U"y^{p-1} - T"x^{p-1} &\equiv x^p + y^p \mod \theta \\ -x^p - T"x^{p-1} &\equiv U"y^{p-1} + y^p \mod \theta \\ -x^{p-1}(x + T") &\equiv y^{p-1}(U" + y) \mod \theta \\ -x^{p-1}(xy + T"y) &\equiv y \cdot y^{p-1}(U" + y) \mod \theta \end{aligned} \tag{8}$$

$-U"y^{p-1} \cdot -T"x^{p-1} \equiv x^p y^p \mod \theta$ ならば

$$xy \equiv U"T" \mod \theta$$

$$\begin{aligned} -x^{p-1}(U"T" + T"y) &\equiv y^p(U" + y) \mod \theta \\ -T"x^{p-1}(U" + y) &\equiv y^p(U" + y) \mod \theta \end{aligned}$$

同様に

$$\begin{aligned} -x \cdot x^{p-1}(x + T") &\equiv y^{p-1}(xU" + xy) \mod \theta \\ -x^p(x + T") &\equiv y^{p-1}(xU" + U"T") \mod \theta \\ x^p(x + T") &\equiv -U"y^{p-1}(x + T") \mod \theta \end{aligned}$$

よって合同式 (8) および $-U"y^{p-1} \cdot -T"x^{p-1} \equiv x^p y^p \mod \theta$ を満たすとき解の候補は 3 通りである。

$$\begin{aligned} -U"y^{p-1} &\equiv x^p \mod \theta \\ -T"x^{p-1} &\equiv y^p \mod \theta \\ or \quad &, \ and \\ -U"y^{p-1} &\equiv y^p \mod \theta \\ -T"x^{p-1} &\equiv x^p \mod \theta \end{aligned} \tag{9}$$

$U = y \ , \ T = z \ , \ U' = x \ , \ T' = z \ , \ U" = x \ , \ T" = y$ のとき

(4),(6),(8) から

$$\begin{aligned} z^{p-1}(z + y) &\equiv y^{p-1}(z + y) \mod \theta \\ -z^{p-1}(x - z) &\equiv x^{p-1}(x - z) \mod \theta \\ -x^{p-1}(x + y) &\equiv y^{p-1}(x + y) \mod \theta \end{aligned}$$

【Solution conditions】

$$\begin{aligned} x^p \quad &+yz^{p-1} \quad &&\equiv zy^{p-1} \mod \theta \\ -xz^{p-1} \quad &+y^p \quad &&\equiv -zx^{p-1} \mod \theta \\ -xy^{p-1} \quad &-yx^{p-1} \quad &&\equiv z^p \mod \theta \end{aligned}$$

### 1.3 $\left(x^{p-1}\right)^2 \equiv y^{p-1}z^{p-1} \mod \delta$ のとき

$x-y \equiv -z \mod \delta$ より

$$\begin{array}{rrrl} x^p & -yx^{p-1} & \equiv -zx^{p-1} & \mod \delta \\ -xy^{p-1} & +y^p & \equiv zy^{p-1} & \mod \delta \\ -xz^{p-1} & +yz^{p-1} & \equiv z^p & \mod \delta \end{array}$$

$$-yx^{p-1} \equiv y^p \mod \theta_1 \Rightarrow -zx^{p-1} \equiv z^p \mod \theta_1$$

ならば

$$-x^{p-1} \equiv y^{p-1} \mod \theta_1 \Rightarrow -x^{p-1} \equiv z^{p-1} \mod \theta_1$$

であるから自動的に

$$-xy^{p-1} \equiv x^p \mod \theta_1 \quad , \quad zy^{p-1} \equiv z^p \mod \theta_1$$

$$-xz^{p-1} \equiv x^p \mod \theta_1 \quad , \quad yz^{p-1} \equiv y^p \mod \theta_1$$

**Definition 9** $y \equiv rz \mod \delta \quad , \ z \equiv qy \mod \delta \quad , \ qr \perp \delta$

$$x+qy \equiv rz \mod \delta$$

$$\begin{array}{rrrl} x^p & +qyx^{p-1} & \equiv rzx^{p-1} & \mod \delta \\ q^{-1}xy^{p-1} & +y^p & \equiv q^{-1}rzy^{p-1} & \mod \delta \\ r^{-1}xz^{p-1} & +qr^{-1}yz^{p-1} & \equiv z^p & \mod \delta \end{array}$$

$$qyx^{p-1} \equiv y^p \mod \theta_2 \Rightarrow rzx^{p-1} \equiv z^p \mod \theta_2$$

ならば

$$x^{p-1} \equiv q^{-1}y^{p-1} \mod \theta_2 \Rightarrow x^{p-1} \equiv r^{-1}z^{p-1} \mod \theta_2$$

であるから自動的に

$$q^{-1}xy^{p-1} \equiv x^p \mod \theta_2 \quad , \quad q^{-1}rzy^{p-1} \equiv z^p \mod \theta_2$$

$$r^{-1}xz^{p-1} \equiv x^p \mod \theta_2 \quad , \quad qr^{-1}yz^{p-1} \equiv y^p \mod \theta_2$$

よって $\left(x^{p-1}\right)^2 \equiv y^{p-1}z^{p-1} \mod \delta$ のとき $x^p+y^p \equiv z^p \mod \delta$ が成り立つ可能性のある条件は

$$\begin{array}{rl} -x^{p-1} \equiv & y^{p-1} \equiv z^{p-1} \mod \theta_1 \\ & or \\ -x^{p-1} \not\equiv & y^{p-1} \not\equiv z^{p-1} \mod \theta_2 \end{array} \tag{10}$$

**Definition 10** 以降、例として $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta$ と表記する場合、$-x^{p-1} \not\equiv z^{p-1} \mod \theta$ とも意味する。

## 1.4 同値変換 (Equivalence transformation)

$s,t,u$ を変数とおく。
$\theta \perp stuxyz$ ならば、$xyz$ の逆元が存在するので異なる文字式で同値変換できる。

**Definition 11** 【Equivalence transformation】

$$s_1x^{p-1}+t_1y^{p-1}\equiv u_1z^{p-1} \mod \theta$$

$$s_2z^{p-1}+t_2x^{p-1}\equiv u_2y^{p-1} \mod \theta$$

$$s_3y^{p-1}+t_3z^{p-1}\equiv u_3x^{p-1} \mod \theta$$

このとき以下を同値変換の成立条件と呼び、以降 [ ] で示す。

$$[s_1\equiv u_3-t_2 \mod \theta]$$
$$[t_1\equiv u_2-s_3 \mod \theta]$$
$$[u_1\equiv s_2+t_3 \mod \theta]$$

## 1.5 一般的解の条件 (General solution conditions)

**Definition 12** 同値変換の成立条件が 3 組共通な以下の関係式を
General solution conditions と呼ぶ。

$$\begin{aligned} s_1x^{p-1} &+t_2x^{p-1} &&\equiv u_3x^{p-1} \mod \theta\\ s_3y^{p-1} &+t_1y^{p-1} &&\equiv u_2y^{p-1} \mod \theta\\ s_2z^{p-1} &+t_3z^{p-1} &&\equiv u_1z^{p-1} \mod \theta \end{aligned}$$

### 1.5.1 $-x^{p-1}\equiv y^{p-1}\equiv z^{p-1} \mod \theta_1$ のとき

$$\begin{aligned} s_1x^{p-1} &-t_2y^{p-1} &&\equiv -u_3z^{p-1} \mod \theta_1\\ -s_3x^{p-1} &+t_1y^{p-1} &&\equiv u_2z^{p-1} \mod \theta_1\\ -s_2x^{p-1} &+t_3y^{p-1} &&\equiv u_1z^{p-1} \mod \theta_1 \end{aligned}$$

$\mod \theta_1$ として

$$\begin{aligned} s_1 &\equiv x \ , \ t_1\equiv y \ , \ u_1\equiv z\\ s_2 &\equiv -x \ , \ t_2\equiv -y \ , \ u_2\equiv z\\ s_3 &\equiv -x \ , \ t_3\equiv y \ , \ u_3\equiv -z \end{aligned}$$

$$[x+z-y\equiv 0 \mod \delta]$$

【General solution conditions】

$$\begin{aligned} x^p &-yx^{p-1} &&\equiv -zx^{p-1} \mod \delta\\ -xy^{p-1} &+y^p &&\equiv zy^{p-1} \mod \delta\\ -xz^{p-1} &+yz^{p-1} &&\equiv z^p \mod \delta \end{aligned} \tag{11}$$

### 1.5.2 Common to $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta_2$

(5)、(10)、(11) より

$$\begin{aligned} Uz^{p-1} &\equiv -yx^{p-1} \mod \delta \\ Ty^{p-1} &\equiv -zx^{p-1} \mod \delta \end{aligned}$$

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \delta \\ &\Leftrightarrow \\ x^p \quad -yx^{p-1} \quad &\equiv -zx^{p-1} \mod \theta_1 \\ x^p \quad +zx^{p-1} \quad &\equiv yx^{p-1} \mod \theta_2 \end{aligned}$$

$$\begin{aligned} -yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \mod \delta \\ \left(x^{p-1}\right)^2 &\equiv y^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{12}$$

(7)、(10)、(11) より

$$\begin{aligned} -U'z^{p-1} &\equiv -xy^{p-1} \mod \delta \\ -T'x^{p-1} &\equiv zy^{p-1} \mod \delta \end{aligned}$$

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \delta \\ &\Leftrightarrow \\ -xy^{p-1} \quad +y^p \quad &\equiv zy^{p-1} \mod \theta_1 \\ -zy^{p-1} \quad +y^p \quad &\equiv xy^{p-1} \mod \theta_2 \end{aligned}$$

$$\begin{aligned} -xy^{p-1} \cdot zy^{p-1} &\equiv x^p z^p \mod \delta \\ \left(y^{p-1}\right)^2 &\equiv -x^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{13}$$

(9)、(10)、(11) より

$$\begin{aligned} -U"y^{p-1} &\equiv -xz^{p-1} \mod \delta \\ -T"x^{p-1} &\equiv yz^{p-1} \mod \delta \end{aligned}$$

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \delta \\ &\Leftrightarrow \\ -xz^{p-1} \quad +yz^{p-1} \quad &\equiv z^p \mod \theta_1 \\ yz^{p-1} \quad -xz^{p-1} \quad &\equiv z^p \mod \theta_2 \end{aligned}$$

$$\begin{aligned} -xz^{p-1} \cdot yz^{p-1} &\equiv x^p y^p \mod \delta \\ \left(z^{p-1}\right)^2 &\equiv -x^{p-1} y^{p-1} \mod \delta \end{aligned} \tag{14}$$

(12)(13)(14) より

$$-\left(x^{p-1}\right)^3 \equiv \left(y^{p-1}\right)^3 \equiv \left(z^{p-1}\right)^3 \mod \delta$$

$$\begin{aligned}
\left(z^{p-1}\right)^3 - \left(y^{p-1}\right)^3 &\equiv (z^{p-1} - y^{p-1})((z^{p-1})^2 + y^{p-1}z^{p-1} + (y^{p-1})^2) \equiv 0 \mod \delta \\
\left(x^{p-1}\right)^3 + \left(z^{p-1}\right)^3 &\equiv (x^{p-1} + z^{p-1})((x^{p-1})^2 - x^{p-1}z^{p-1} + (z^{p-1})^2) \equiv 0 \mod \delta \\
\left(x^{p-1}\right)^3 + \left(y^{p-1}\right)^3 &\equiv (x^{p-1} + y^{p-1})((x^{p-1})^2 - x^{p-1}y^{p-1} + (y^{p-1})^2) \equiv 0 \mod \delta
\end{aligned}$$

$$\begin{aligned}
x^p + y^p &\equiv z^p \mod 3 \\
x \cdot x^{2n} + y \cdot y^{2n} &\equiv z \cdot z^{2n} \mod 3
\end{aligned}$$

$3 \perp xyz$ のとき Fermat's little theorem より

$$\begin{aligned}
x + y &\equiv z \mod 3 \\
x &\equiv \pm 1 \mod 3 \\
y &\equiv \pm 1 \mod 3 \\
z &\equiv \mp 1 \mod 3 \\
x + z &\equiv 0 \mod 3 \\
\delta &\neq 3
\end{aligned}$$

$$\begin{aligned}
A^3 - B^3 &= (A - B)(3AB + (A - B)^2) \\
A^3 + B^3 &= (A + B)(-3AB + (A + B)^2)
\end{aligned}$$

$\delta \perp 3AB$ なので

$$\begin{aligned}
\delta \mid (A - B) &\Rightarrow \delta \perp (3AB + (A - B)^2) \\
\delta \mid (3AB + (A - B)^2) &\Rightarrow \delta \perp (A - B)
\end{aligned}$$

2 つの因数のうち、一方は $\delta$ と互いに素である。 (15)

### 1.5.3 $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta_2$ のとき

(13)(14) より

$$\begin{aligned}(x^{p-1})^2 + (z^{p-1})^2 + (y^{p-1})^2 &\equiv 0 \mod \theta_2 \\ (x^{p-1})^2 - x^{p-1}y^{p-1} - x^{p-1}z^{p-1} &\equiv 0 \mod \theta_2 \\ x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \mod \theta_2\end{aligned}$$

$s'', t'', u''$ を変数とおく。
$\theta \perp s''t''u''xyz$ ならば、その逆元が存在するので異なる文字式で同値変換できる。

$$\begin{aligned}s_1''x + t_1''y &\equiv u_1''z \mod \theta \\ s_2''z + t_2''x &\equiv u_2''y \mod \theta \\ s_3''y + t_3''z &\equiv u_3''x \mod \theta\end{aligned}$$

$\theta_2 = \theta_3$ or $\theta_4$ とする。

### 1.5.4 $-y \equiv z \equiv x \mod \theta_3$ のとき

$$\begin{aligned}s_1''x + t_1''y &\equiv u_1''z \mod \theta_3 \\ s_2''x - t_2''y &\equiv -u_2''z \mod \theta_3 \\ -s_3''x - t_3''y &\equiv u_3''z \mod \theta_3\end{aligned}$$

$\mod \theta_3$ として

$$\begin{aligned}s_1'' &\equiv x^{p-1} \ , \ t_1'' \equiv y^{p-1} \ , \ u_1'' \equiv z^{p-1} \\ s_2'' &\equiv x^{p-1} \ , \ t_2'' \equiv -y^{p-1} \ , \ u_2'' \equiv -z^{p-1} \\ s_3'' &\equiv -x^{p-1} \ , \ t_3'' \equiv -y^{p-1} \ , \ u_3'' \equiv z^{p-1}\end{aligned}$$

$$[x^{p-1} - y^{p-1} - z^{p-1} \equiv 0 \mod \theta_2]$$

【General solution conditions】

$$\begin{aligned}x^p \quad -y^{p-1}x \quad &\equiv z^{p-1}x \mod \theta_2 \\ -x^{p-1}y \quad +y^p \quad &\equiv -z^{p-1}y \mod \theta_2 \\ x^{p-1}z \quad -y^{p-1}z \quad &\equiv z^p \mod \theta_2\end{aligned} \tag{16}$$

$$\begin{aligned}-y \equiv z &\equiv x \mod \theta_2 \\ or & \\ -y \not\equiv z &\not\equiv x \mod \theta_2\end{aligned} \tag{17}$$

### 1.5.5 Common to $-y \not\equiv z \not\equiv x \mod \theta_4$

(16)(17) より

$$\begin{aligned} -y^{p-1}x \cdot z^{p-1}x &\equiv y^p z^p \mod \theta_2 \\ -x^2 &\equiv yz \mod \theta_2 \\ x^2 &\equiv -yz \mod \theta_2 \end{aligned} \tag{18}$$

$$\begin{aligned} -x^{p-1}y \cdot -z^{p-1}y &\equiv x^p z^p \mod \theta_2 \\ y^2 &\equiv xz \mod \theta_2 \end{aligned} \tag{19}$$

$$\begin{aligned} x^{p-1}z \cdot -y^{p-1}z &\equiv x^p y^p \mod \theta_2 \\ -z^2 &\equiv xy \mod \theta_2 \\ z^2 &\equiv -xy \mod \theta_2 \end{aligned} \tag{20}$$

(18)(19)(20) より

$$-y^3 \equiv z^3 \equiv x^3 \mod \theta_2$$

$$\begin{aligned} z^3 + y^3 &\equiv (z+y)(z^2 - yz + y^2) \equiv 0 \mod \theta_2 \\ x^3 - z^3 &\equiv (x-z)(x^2 + xz + z^2) \equiv 0 \mod \theta_2 \\ x^3 + y^3 &\equiv (x+y)(x^2 - xy + y^2) \equiv 0 \mod \theta_2 \end{aligned}$$

$\theta_2 = \delta$ のとき $\theta_2 \perp 3xyz$、(15) より二つの因数の一方が解となる。

$$\begin{aligned} x^2 + xz + z^2 &\equiv 0 \mod \theta_4 \\ \text{(20) より } x^2 + xz - xy &\equiv 0 \mod \theta_4 \\ x + z - y &\equiv 0 \mod \theta_4 \end{aligned}$$

$\theta_4 = \delta$ が確定しているので $\theta_2 = \theta_4$ であり $\theta_3 \neq \delta$

ただし $\theta_1 = \delta$ のときは $\theta_4 \neq \delta$ であり (18)(19)(20) は成り立たない。この場合

$$x + z - y \not\equiv 0 \mod \theta_4$$

$$(12) \text{ より } \left(x^{p-1}\right)^2 \equiv y^{p-1}z^{p-1} \mod \theta_4$$
$$\left(x^2\right)^{p-1} \equiv y^{p-1}z^{p-1} \mod \theta_4$$
$$(18) \text{ より } (-yz)^{p-1} \equiv y^{p-1}z^{p-1} \mod \theta_4$$
$$y^{p-1}z^{p-1} \equiv y^{p-1}z^{p-1} \mod \theta_4$$

$$(13) \text{ より } \left(y^{p-1}\right)^2 \equiv -x^{p-1}z^{p-1} \mod \theta_4$$
$$\left(y^2\right)^{p-1} \equiv -x^{p-1}z^{p-1} \mod \theta_4$$
$$(19) \text{ より } (xz)^{p-1} \equiv -x^{p-1}z^{p-1} \mod \theta_4$$
$$x^{p-1}z^{p-1} \equiv -x^{p-1}z^{p-1} \mod \theta_4$$

$\delta$ の定義に反する。

$$(14) \text{ より } \left(z^{p-1}\right)^2 \equiv -x^{p-1}y^{p-1} \mod \theta_4$$
$$\left(z^2\right)^{p-1} \equiv -x^{p-1}y^{p-1} \mod \theta_4$$
$$(20) \text{ より } (-xy)^{p-1} \equiv -x^{p-1}y^{p-1} \mod \theta_4$$
$$x^{p-1}y^{p-1} \equiv -x^{p-1}y^{p-1} \mod \theta_4$$

$\delta$ の定義に反するので $\theta_4 \neq \delta$

$$[x^{p-1} - y^{p-1} - z^{p-1} \not\equiv 0 \mod \delta]$$

### 1.5.6 まとめ

【General solution conditions】

$$
\begin{aligned}
x^p \quad &+y^p \quad &&\equiv z^p \mod \theta_1 \\
&\Leftrightarrow \\
x^p \quad &-yx^{p-1} \quad &&\equiv -zx^{p-1} \mod \theta_1 \\
-xy^{p-1} \quad &+y^p \quad &&\equiv zy^{p-1} \mod \theta_1 \\
-xz^{p-1} \quad &+yz^{p-1} \quad &&\equiv z^p \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
x^p \quad &+y^p \quad &&\equiv z^p \mod \theta_4 \\
&\Leftrightarrow \\
x^p \quad &+zx^{p-1} \quad &&\equiv yx^{p-1} \mod \theta_4 \\
-zy^{p-1} \quad &+y^p \quad &&\equiv xy^{p-1} \mod \theta_4 \\
yz^{p-1} \quad &-xz^{p-1} \quad &&\equiv z^p \mod \theta_4
\end{aligned}
\tag{21}
$$

$$
\begin{aligned}
x^p \quad &+y^p \quad &&\equiv z^p \mod \theta_3 \\
&\Leftrightarrow \\
x^p \quad &-y^{p-1}x \quad &&\equiv z^{p-1}x \mod \theta_3 \\
-x^{p-1}y \quad &+y^p \quad &&\equiv -z^{p-1}y \mod \theta_3 \\
x^{p-1}z \quad &-y^{p-1}z \quad &&\equiv z^p \mod \theta_3
\end{aligned}
$$

$$
\begin{aligned}
x^p \quad &+y^p \quad &&\equiv z^p \mod \theta_4 \\
&\Leftrightarrow \\
x^p \quad &-z^{p-1}x \quad &&\equiv y^{p-1}x \mod \theta_4 \\
z^{p-1}y \quad &+y^p \quad &&\equiv x^{p-1}y \mod \theta_4 \\
-y^{p-1}z \quad &+x^{p-1}z \quad &&\equiv z^p \mod \theta_4
\end{aligned}
\tag{22}
$$

【Equivalence transformation】

$$
-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \theta_1
$$

$$
\begin{aligned}
xx^{p-1} \quad &+yy^{p-1} \quad &&\equiv zz^{p-1} \mod \theta_1 \\
-xz^{p-1} \quad &-yx^{p-1} \quad &&\equiv zy^{p-1} \mod \theta_1 \\
-xy^{p-1} \quad &+yz^{p-1} \quad &&\equiv -zx^{p-1} \mod \theta_1
\end{aligned}
$$

or

$$
x^{p-1} - y^{p-1} - z^{p-1} \equiv 0 \mod \theta_4
$$

$$
\begin{aligned}
xx^{p-1} \quad &+yy^{p-1} \quad &&\equiv zz^{p-1} \mod \theta_4 \\
yz^{p-1} \quad &+zx^{p-1} \quad &&\equiv xy^{p-1} \mod \theta_4 \\
-zy^{p-1} \quad &-xz^{p-1} \quad &&\equiv yx^{p-1} \mod \theta_4
\end{aligned}
$$

### 1.6 $-x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \mod \delta$ のとき

$x-y+k_1 \equiv -z+k_1 \mod \delta$ より

**Definition 13** $-y+k_1 \equiv -l_1 y \mod \delta$ , $-z+k_1 \equiv -m_1 z \mod \delta$ , $l_1 m_1 \perp \delta$

$$-l_1 y x^{p-1} \cdot -m_1 z x^{p-1} \equiv y^p z^p \mod \delta$$

$x - l_1 y \equiv -m_1 z \mod \delta$ より

$$\begin{array}{rrl} x^p & -l_1 y x^{p-1} & \equiv -m_1 z x^{p-1} \mod \delta \\ -l_1^{-1} x y^{p-1} & +y^p & \equiv l_1^{-1} m_1 z y^{p-1} \mod \delta \\ -m_1^{-1} x z^{p-1} & +l_1 m_1^{-1} y z^{p-1} & \equiv z^p \mod \delta \end{array} \tag{23}$$

ここで

$$-l_1 y x^{p-1} \equiv y^p \mod \delta \Rightarrow -m_1 z x^{p-1} \equiv z^p \mod \delta$$
$$-x^{p-1} \equiv l_1^{-1} y^{p-1} \mod \delta \Rightarrow -x^{p-1} \equiv m_1^{-1} z^{p-1} \mod \delta$$

であるから自動的に

$$-l_1^{-1} x y^{p-1} \equiv x^p \mod \delta \ , \ l_1^{-1} m_1 z y^{p-1} \equiv z^p \mod \delta$$
$$-m_1^{-1} x z^{p-1} \equiv x^p \mod \delta \ , \ l_1 m_1^{-1} y z^{p-1} \equiv y^p \mod \delta$$

よって $x^p + y^p \equiv z^p \mod \delta$ が成り立つ条件は

$$\begin{gathered} -x^{p-1} \equiv l_1^{-1} y^{p-1} \equiv m_1^{-1} z^{p-1} \mod \delta \\ or \\ -x^{p-1} \not\equiv l_1^{-1} y^{p-1} \not\equiv m_1^{-1} z^{p-1} \mod \delta \end{gathered}$$

#### 1.6.1 Common to $-x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \mod \delta$

(23) より

$$\begin{array}{rl} -l_1 y x^{p-1} \cdot -m_1 z x^{p-1} & \equiv y^p z^p \mod \delta \\ l_1 m_1 \left(x^{p-1}\right)^2 & \equiv y^{p-1} z^{p-1} \mod \delta \\ \left(x^{p-1}\right)^2 & \equiv l_1^{-1} m_1^{-1} y^{p-1} z^{p-1} \mod \delta \end{array} \tag{24}$$

$$\begin{array}{rl} -l_1^{-1} x y^{p-1} \cdot l_1^{-1} m_1 z y^{p-1} & \equiv x^p z^p \mod \delta \\ l_1^{-2} m_1 \left(y^{p-1}\right)^2 & \equiv -x^{p-1} z^{p-1} \mod \delta \\ \left(l_1^{-1} y^{p-1}\right)^2 & \equiv -m_1^{-1} x^{p-1} z^{p-1} \mod \delta \end{array} \tag{25}$$

$$\begin{array}{rl} -m_1^{-1} x z^{p-1} \cdot l_1 m_1^{-1} y z^{p-1} & \equiv x^p y^p \mod \delta \\ l_1 m_1^{-2} \left(z^{p-1}\right)^2 & \equiv -x^{p-1} y^{p-1} \mod \delta \\ \left(m_1^{-1} z^{p-1}\right)^2 & \equiv -l_1^{-1} x^{p-1} y^{p-1} \mod \delta \end{array} \tag{26}$$

(24)(25)(26) より

$$-\left(x^{p-1}\right)^3 \equiv \left(l_1^{-1}y^{p-1}\right)^3 \equiv \left(m_1^{-1}z^{p-1}\right)^3 \mod \delta$$

$$\left(m_1^{-1}z^{p-1}\right)^3-\left(l_1^{-1}y^{p-1}\right)^3 \equiv (m_1^{-1}z^{p-1}-l_1^{-1}y^{p-1})((m_1^{-1}z^{p-1})^2+l_1^{-1}m_1^{-1}y^{p-1}z^{p-1}+(l_1^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(x^{p-1}\right)^3+\left(m_1^{-1}z^{p-1}\right)^3 \equiv (x^{p-1}+m_1^{-1}z^{p-1})((x^{p-1})^2-m_1^{-1}x^{p-1}z^{p-1}+(m_1^{-1}z^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(x^{p-1}\right)^3+\left(l_1^{-1}y^{p-1}\right)^3 \equiv (x^{p-1}+l_1^{-1}y^{p-1})((x^{p-1})^2-l_1^{-1}x^{p-1}y^{p-1}+(l_1^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

### 1.6.2 $-x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \mod \delta$ のとき

(25)(26) より

$$\begin{aligned}
(x^{p-1})^2 + (m_1^{-1}z^{p-1})^2 + (l_1^{-1}y^{p-1})^2 &\equiv 0 \mod \theta_4 \\
(x^{p-1})^2 - l_1^{-1}x^{p-1}y^{p-1} - m_1^{-1}x^{p-1}z^{p-1} &\equiv 0 \mod \theta_4 \\
x^{p-1} - l_1^{-1}y^{p-1} - m_1^{-1}z^{p-1} &\equiv 0 \mod \theta_4 \\
x^{p-1} - l_1^{-1}y^{p-1} &\equiv m_1^{-1}z^{p-1} \mod \theta_4
\end{aligned}$$

【General solution conditions】

$$\begin{aligned}
x^p \quad -l_1^{-1}y^{p-1}x \quad &\equiv m_1^{-1}z^{p-1}x \mod \theta_4 \\
-l_1x^{p-1}y \quad +y^p \quad &\equiv -l_1m_1^{-1}z^{p-1}y \mod \theta_4 \qquad (27) \\
m_1x^{p-1}z \quad -l_1^{-1}m_1y^{p-1}z \quad &\equiv z^p \mod \theta_4
\end{aligned}$$

(21) と (22) が同値な事を参考にすると、(27) より以下が成り立つ。

$$\begin{aligned}
-l_1^{-1}y^{p-1}x \cdot m_1^{-1}z^{p-1}x &\equiv y^pz^p \mod \theta_4 \\
x^2 &\equiv -l_1m_1yz \mod \theta_4 \qquad (28)
\end{aligned}$$

$$\begin{aligned}
-l_1x^{p-1}y \cdot -l_1m_1^{-1}z^{p-1}y &\equiv x^pz^p \mod \theta_4 \\
y^2 &\equiv l_1^{-2}m_1xz \mod \theta_4 \qquad (29)
\end{aligned}$$

$$\begin{aligned}
m_1x^{p-1}z \cdot -l_1^{-1}m_1y^{p-1}z &\equiv x^py^p \mod \theta_4 \\
z^2 &\equiv -l_1m_1^{-2}xy \mod \theta_4 \qquad (30)
\end{aligned}$$

(28)(29)(30) より

$$-l_1^3y^3 \equiv m_1^3z^3 \equiv x^3 \mod \theta_4$$

$$\begin{aligned}
m_1^3z^3 + l_1^3y^3 &\equiv (m_1z + l_1y)(m_1^2z^2 - l_1m_1yz + l_1^2y^2) \equiv 0 \mod \theta_4 \\
x^3 - m_1^3z^3 &\equiv (x - m_1z)(x^2 + m_1xz + m_1^2z^2) \equiv 0 \mod \theta_4 \\
x^3 + l_1^3y^3 &\equiv (x + l_1y)(x^2 - l_1xy + l_1^2y^2) \equiv 0 \mod \theta_4
\end{aligned}$$

(15) より二つの因数の一方が解となる。

$$\begin{aligned}
x^2 + m_1xz + m_1^2z^2 &\equiv 0 \mod \theta_4 \\
\text{(30) より } x^2 + m_1xz - l_1xy &\equiv 0 \mod \theta_4 \\
x + m_1z - l_1y &\equiv 0 \mod \theta_4
\end{aligned}$$

$$
\begin{aligned}
(24)\ \text{より}\ \left(x^{p-1}\right)^2 &\equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_4\\
\left(x^2\right)^{p-1} &\equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_4\\
(28)\ \text{より}\ (-l_1m_1yz)^{p-1} &\equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_4\\
l_1^{p-1}m_1^{p-1}y^{p-1}z^{p-1} &\equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_4\\
l_1^{p}m_1^{p}y^{p-1}z^{p-1} &\equiv y^{p-1}z^{p-1} \mod \theta_4\\
l_1^{p}m_1^{p} &\equiv 1 \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
(25)\ \text{より}\ \left(y^{p-1}\right)^2 &\equiv -l_1^{2}m_1^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
\left(y^2\right)^{p-1} &\equiv -l_1^{2}m_1^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
(29)\ \text{より}\ \left(l_1^{-2}m_1xz\right)^{p-1} &\equiv -l_1^{2}m_1^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
l_1^{-2p+2}m_1^{p-1}x^{p-1}z^{p-1} &\equiv -l_1^{2}m_1^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
l_1^{-2p}m_1^{p}x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_4\\
l_1^{-2p}m_1^{p} &\equiv -1 \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
(26)\ \text{より}\ \left(z^{p-1}\right)^2 &\equiv -l_1^{-1}m_1^{2}x^{p-1}y^{p-1} \mod \theta_4\\
\left(z^2\right)^{p-1} &\equiv -l_1^{-1}m_1^{2}x^{p-1}y^{p-1} \mod \theta_4\\
(30)\ \text{より}\ \left(-l_1m_1^{-2}xy\right)^{p-1} &\equiv -l_1^{-1}m_1^{2}x^{p-1}y^{p-1} \mod \theta_4\\
l_1^{p-1}m_1^{-2p+2}x^{p-1}y^{p-1} &\equiv -l_1^{-1}m_1^{2}x^{p-1}y^{p-1} \mod \theta_4\\
l_1^{p}m_1^{-2p}x^{p-1}y^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \theta_4\\
l_1^{p}m_1^{-2p} &\equiv -1 \mod \theta_4
\end{aligned}
$$

$$\begin{aligned} l_1^p m_1^p &\equiv 1 \mod \theta_4 \\ l_1^{-2p} m_1^p &\equiv -1 \mod \theta_4 \\ l_1^p m_1^{-2p} &\equiv -1 \mod \theta_4 \end{aligned} \tag{31}$$

$$m_1^{3p} \equiv l_1^{3p} \mod \theta_4$$
$$m_1^{3p} - l_1^{3p} \equiv (m_1^p - l_1^p)(m_1^{2p} + l_1^p m_1^p + l_1^{2p}) \mod \theta_4$$

$$-m_1^p \equiv l_1^{2p} \mod \theta_4$$
$$l_1^p \equiv -m_1^{2p} \mod \theta_4$$

$$l_1^p - m_1^p \equiv l_1^{2p} - m_1^{2p} \mod \theta_4$$
$$l_1^p - m_1^p \equiv (l_1^p + m_1^p)(l_1^p - m_1^p) \mod \theta_4$$
$$1 \equiv l_1^p + m_1^p \mod \theta_4$$

$$(l_1^p + m_1^p)^2 \equiv 1^2 \mod \theta_4$$
$$l_1^{2p} + 2l_1^p m_1^p + m_1^{2p} \equiv 1 \mod \theta_4$$
$$l_1^{2p} + 2l_1^p m_1^p + m_1^{2p} \equiv l_1^p m_1^p \mod \theta_4$$
$$l_1^{2p} + l_1^p m_1^p + m_1^{2p} \equiv 0 \mod \theta_4$$

$m_1^p - l_1^p \not\equiv 0 \mod \theta_4$ なので $m_1 \equiv 1 \mod \theta_4$ , $l_1 \equiv 1 \mod \theta_4$ のとき
$x^p + y^p \not\equiv z^p \mod \theta_4$

$$l_1^p + m_1^p \equiv 1 \mod \theta_4$$
$$l_1^{2p} + l_1^p m_1^p \equiv l_1^p \mod \theta_4$$
$$l_1^{2p} - l_1^p + 1 \equiv 0 \mod \theta_4$$

$l_1^p m_1^p \equiv 1 \mod \theta_4$ なので

$$l_1^p \equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \tag{32}$$

$$m_1^p \equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4 \tag{33}$$

$x + k_2 - y \equiv -z + k_2 \mod \delta$ より

**Definition 14** $x + k_2 \equiv l_2 x \mod \delta$ , $-z + k_2 \equiv -m_2 z \mod \delta$ , $l_2 m_2 \perp \delta$

$$-l_2 x y^{p-1} \cdot m_2 z y^{p-1} \equiv x^p z^p \mod \delta$$

$l_2 x - y \equiv -m_2 z \mod \delta$ より

$$\begin{array}{rcl} x^p & -l_2^{-1} y x^{p-1} & \equiv -l_2^{-1} m_2 z x^{p-1} \mod \delta \\ -l_2 x y^{p-1} & +y^p & \equiv m_2 z y^{p-1} \mod \delta \\ -l_2 m_2^{-1} x z^{p-1} & +m_2^{-1} y z^{p-1} & \equiv z^p \mod \delta \end{array} \tag{34}$$

ここで

$$-l_2 x y^{p-1} \equiv x^p \mod \delta \Rightarrow m_2 z y^{p-1} \equiv z^p \mod \delta$$
$$-l_2 y^{p-1} \equiv x^{p-1} \mod \delta \Rightarrow m_2 y^{p-1} \equiv z^{p-1} \mod \delta$$

であるから自動的に

$$-l_2^{-1} y x^{p-1} \equiv y^p \mod \delta \quad , \quad -l_2^{-1} m_2 z x^{p-1} \equiv z^p \mod \delta$$
$$-l_2 m_2^{-1} x z^{p-1} \equiv x^p \mod \delta \quad , \quad m_2^{-1} y z^{p-1} \equiv y^p \mod \delta$$

よって $x^p + y^p \equiv z^p \mod \delta$ が成り立つ条件は

$$\begin{array}{c} -l_2^{-1} x^{p-1} \equiv y^{p-1} \equiv m_2^{-1} z^{p-1} \mod \delta \\ or \\ -l_2^{-1} x^{p-1} \not\equiv y^{p-1} \not\equiv m_2^{-1} z^{p-1} \mod \delta \end{array}$$

### 1.6.3 Common to $-l_2^{-1} x^{p-1} \not\equiv y^{p-1} \not\equiv m_2^{-1} z^{p-1} \mod \delta$

(34) より

$$\begin{array}{rl} -l_2^{-1} y x^{p-1} \cdot -l_2^{-1} m_2 z x^{p-1} & \equiv y^p z^p \mod \delta \\ l_2^{-2} m_2 \left(x^{p-1}\right)^2 & \equiv y^{p-1} z^{p-1} \mod \delta \\ \left(l_2^{-1} x^{p-1}\right)^2 & \equiv m_2^{-1} y^{p-1} z^{p-1} \mod \delta \end{array} \tag{35}$$

$$\begin{array}{rl} -l_2 x y^{p-1} \cdot m_2 z y^{p-1} & \equiv x^p z^p \mod \delta \\ l_2 m_2 \left(y^{p-1}\right)^2 & \equiv -x^{p-1} z^{p-1} \mod \delta \\ \left(y^{p-1}\right)^2 & \equiv -l_2^{-1} m_2^{-1} x^{p-1} z^{p-1} \mod \delta \end{array} \tag{36}$$

$$\begin{array}{rl} -l_2 m_2^{-1} x z^{p-1} \cdot m_2^{-1} y z^{p-1} & \equiv x^p y^p \mod \delta \\ l_2 m_2^{-2} \left(z^{p-1}\right)^2 & \equiv -x^{p-1} y^{p-1} \mod \delta \\ \left(m_2^{-1} z^{p-1}\right)^2 & \equiv -l_2^{-1} x^{p-1} y^{p-1} \mod \delta \end{array} \tag{37}$$

(35)(36)(37) より

$$-\left(l_2^{-1}x^{p-1}\right)^3 \equiv \left(y^{p-1}\right)^3 \equiv \left(m_2^{-1}z^{p-1}\right)^3 \mod \delta$$

$$\left(y^{p-1}\right)^3-\left(m_2^{-1}z^{p-1}\right)^3 \equiv (y^{p-1}-m_2^{-1}z^{p-1})((y^{p-1})^2+m_2^{-1}y^{p-1}z^{p-1}+(m_2^{-1}z^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(l_2^{-1}x^{p-1}\right)^3+\left(y^{p-1}\right)^3 \equiv (l_2^{-1}x^{p-1}+y^{p-1})((l_2^{-1}x^{p-1})^2-l_2^{-1}x^{p-1}y^{p-1}+(y^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(l_2^{-1}x^{p-1}\right)^3+\left(m_2^{-1}z^{p-1}\right)^3 \equiv (l_2^{-1}x^{p-1}+m_2^{-1}z^{p-1})((l_2^{-1}x^{p-1})^2-l_2^{-1}m_2^{-1}x^{p-1}z^{p-1}+(m_2^{-1}z^{p-1})^2) \equiv 0 \mod \delta$$

### 1.6.4 $-l_2^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv m_2^{-1}z^{p-1} \mod \delta$ のとき

(35)(37) より

$$\begin{aligned}
(m_2^{-1}z^{p-1})^2 + (y^{p-1})^2 + (l_2^{-1}x^{p-1})^2 &\equiv 0 \mod \theta_4 \\
-l_2^{-1}x^{p-1}y^{p-1} + (y^{p-1})^2 + m_2^{-1}y^{p-1}z^{p-1} &\equiv 0 \mod \theta_4 \\
-l_2^{-1}x^{p-1} + y^{p-1} + m_2^{-1}z^{p-1} &\equiv 0 \mod \theta_4 \\
-l_2^{-1}x^{p-1} + y^{p-1} &\equiv -m_2^{-1}z^{p-1} \mod \theta_4
\end{aligned}$$

【General solution conditions】

$$\begin{array}{rrl}
x^p & -l_2y^{p-1}x & \equiv l_2m_2^{-1}z^{p-1}x \mod \theta_4 \\
-l_2^{-1}x^{p-1}y & +y^p & \equiv -m_2^{-1}z^{p-1}y \mod \theta_4 \\
l_2^{-1}m_2x^{p-1}z & -m_2y^{p-1}z & \equiv z^p \mod \theta_4
\end{array} \tag{38}$$

(38) より

$$\begin{aligned}
-l_2y^{p-1}x \cdot l_2m_2^{-1}z^{p-1}x &\equiv y^pz^p \mod \theta_4 \\
x^2 &\equiv -l_2^{-2}m_2yz \mod \theta_4
\end{aligned} \tag{39}$$

$$\begin{aligned}
-l_2^{-1}x^{p-1}y \cdot -m_2^{-1}z^{p-1}y &\equiv x^pz^p \mod \theta_4 \\
y^2 &\equiv l_2m_2xz \mod \theta_4
\end{aligned} \tag{40}$$

$$\begin{aligned}
l_2^{-1}m_2x^{p-1}z \cdot -m_2y^{p-1}z &\equiv x^py^p \mod \theta_4 \\
z^2 &\equiv -l_2m_2^{-2}xy \mod \theta_4
\end{aligned} \tag{41}$$

$$
\begin{aligned}
(35)\ \text{より}\ \left(x^{p-1}\right)^2 &\equiv l_2^2 m_2^{-1} y^{p-1} z^{p-1} \mod \theta_4 \\
\left(x^2\right)^{p-1} &\equiv l_2^2 m_2^{-1} y^{p-1} z^{p-1} \mod \theta_4 \\
(39)\ \text{より}\ \left(-l_2^{-2} m_2 yz\right)^{p-1} &\equiv l_2^2 m_2^{-1} y^{p-1} z^{p-1} \mod \theta_4 \\
l_2^{-2p+2} m_2^{p-1} y^{p-1} z^{p-1} &\equiv l_2^2 m_2^{-1} y^{p-1} z^{p-1} \mod \theta_4 \\
l_2^{-2p} m_2^p &\equiv 1 \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
(36)\ \text{より}\ \left(y^{p-1}\right)^2 &\equiv -l_2^{-1} m_2^{-1} x^{p-1} z^{p-1} \mod \theta_4 \\
\left(y^2\right)^{p-1} &\equiv -l_2^{-1} m_2^{-1} x^{p-1} z^{p-1} \mod \theta_4 \\
(40)\ \text{より}\ \left(l_2 m_2 xz\right)^{p-1} &\equiv -l_2^{-1} m_2^{-1} x^{p-1} z^{p-1} \mod \theta_4 \\
l_2^{p-1} m_2^{p-1} x^{p-1} z^{p-1} &\equiv -l_2^{-1} m_2^{-1} x^{p-1} z^{p-1} \mod \theta_4 \\
l_2^p m_2^p &\equiv -1 \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
(37)\ \text{より}\ \left(z^{p-1}\right)^2 &\equiv -l_2^{-1} m_2^2 x^{p-1} y^{p-1} \mod \theta_4 \\
\left(z^2\right)^{p-1} &\equiv -l_2^{-1} m_2^2 x^{p-1} y^{p-1} \mod \theta_4 \\
(41)\ \text{より}\ \left(-l_2 m_2^{-2} xy\right)^{p-1} &\equiv -l_2^{-1} m_2^2 x^{p-1} y^{p-1} \mod \theta_4 \\
l_2^{p-1} m_2^{-2p+2} x^{p-1} y^{p-1} &\equiv -l_2^{-1} m_2^2 x^{p-1} y^{p-1} \mod \theta_4 \\
l_2^p m_2^{-2p} &\equiv -1 \mod \theta_4
\end{aligned}
$$

$$l_2^p m_2^p \equiv -1 \mod \theta_4$$
$$l_2^{-2p} m_2^p \equiv 1 \mod \theta_4$$
$$l_2^p m_2^{-2p} \equiv -1 \mod \theta_4$$

$$-m_2^{3p} \equiv l_2^{3p} \mod \theta_4$$
$$m_2^{3p} + l_2^{3p} \equiv (m_2^p + l_2^p)(m_2^{2p} - l_2^p m_2^p + l_2^{2p}) \mod \theta_4$$

$$m_2^p \equiv l_2^{2p} \mod \theta_4$$
$$l_2^p \equiv -m_2^{2p} \mod \theta_4$$

$$l_2^p + m_2^p \equiv l_2^{2p} - m_2^{2p} \mod \theta_4$$
$$l_2^p + m_2^p \equiv (l_2^p + m_2^p)(l_2^p - m_2^p) \mod \theta_4$$
$$1 \equiv l_2^p - m_2^p \mod \theta_4$$

$$(l_2^p - m_2^p)^2 \equiv 1^2 \mod \theta_4$$
$$l_2^{2p} - 2l_2^p m_2^p + m_2^{2p} \equiv 1 \mod \theta_4$$
$$l_2^{2p} - 2l_2^p m_2^p + m_2^{2p} \equiv -l_2^p m_2^p \mod \theta_4$$
$$l_2^{2p} - l_2^p m_2^p + m_2^{2p} \equiv 0 \mod \theta_4$$

よって $m_2^p + l_2^p \not\equiv 0 \mod \theta_4$

$$l_2^p - m_2^p \equiv 1 \mod \theta_4$$
$$l_2^{2p} - l_2^p m_2^p \equiv l_2^p \mod \theta_4$$
$$l_2^{2p} - l_2^p + 1 \equiv 0 \mod \theta_4$$

(23)(34) より

$$\begin{aligned} -l_2^{-1} y x^{p-1} &\equiv -l_1 y x^{p-1} \mod \delta \\ l_2^{-1} &\equiv l_1 \mod \delta \\ 1 &\equiv l_1^p l_2^p \mod \delta \end{aligned} \tag{42}$$

$l_2^p m_2^p \equiv -1 \mod \theta_4$ なので

$$l_2^p \equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4 \tag{43}$$
$$m_2^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4 \tag{44}$$

$x - k_3 - y + k_3 \equiv -z \mod \delta$ より

**Definition 15** $x - k_3 \equiv m_3 x \mod \delta$ , $-y + k_3 \equiv -l_3 y \mod \delta$ , $l_3 m_3 \perp \delta$

$$-m_3 x z^{p-1} \cdot l_3 y z^{p-1} \equiv x^p y^p \mod \delta$$

$m_3 x - l_3 y \equiv -z \mod \delta$ より

$$\begin{array}{ccc} x^p & -l_3 m_3^{-1} y x^{p-1} & \equiv -m_3^{-1} z x^{p-1} \mod \delta \\ -l_3^{-1} m_3 x y^{p-1} & +y^p & \equiv l_3^{-1} z y^{p-1} \mod \delta \\ -m_3 x z^{p-1} & +l_3 y z^{p-1} & \equiv z^p \mod \delta \end{array} \tag{45}$$

ここで

$$-m_3 x z^{p-1} \equiv x^p \mod \delta \Rightarrow l_3 y z^{p-1} \equiv y^p \mod \delta$$
$$-m_3 z^{p-1} \equiv x^{p-1} \mod \delta \Rightarrow l_3 z^{p-1} \equiv y^{p-1} \mod \delta$$

であるから自動的に

$$-l_3 m_3^{-1} y x^{p-1} \equiv y^p \mod \delta \quad , \quad -m_3^{-1} z x^{p-1} \equiv z^p \mod \delta$$
$$-l_3^{-1} m_3 x y^{p-1} \equiv x^p \mod \delta \quad , \quad l_3^{-1} z y^{p-1} \equiv z^p \mod \delta$$

よって $x^p + y^p \equiv z^p \mod \delta$ が成り立つ条件は

$$\begin{gathered} -m_3^{-1} x^{p-1} \equiv l_3^{-1} y^{p-1} \equiv z^{p-1} \mod \delta \\ or \\ -m_3^{-1} x^{p-1} \not\equiv l_3^{-1} y^{p-1} \not\equiv z^{p-1} \mod \delta \end{gathered}$$

### 1.6.5 Common to $-m_3^{-1} x^{p-1} \not\equiv l_3^{-1} y^{p-1} \not\equiv z^{p-1} \mod \delta$

(45) より

$$\begin{array}{cc} -l_3 m_3^{-1} y x^{p-1} \cdot -m_3^{-1} z x^{p-1} & \equiv y^p z^p \mod \delta \\ l_3 m_3^{-2} \left(x^{p-1}\right)^2 & \equiv y^{p-1} z^{p-1} \mod \delta \\ \left(m_3^{-1} x^{p-1}\right)^2 & \equiv l_3^{-1} y^{p-1} z^{p-1} \mod \delta \end{array} \tag{46}$$

$$\begin{array}{cc} -l_3^{-1} m_3 x y^{p-1} \cdot l_3^{-1} z y^{p-1} & \equiv x^p z^p \mod \delta \\ l_3^{-2} m_3 \left(y^{p-1}\right)^2 & \equiv -x^{p-1} z^{p-1} \mod \delta \\ \left(l_3^{-1} y^{p-1}\right)^2 & \equiv -m_3^{-1} x^{p-1} z^{p-1} \mod \delta \end{array} \tag{47}$$

$$\begin{array}{cc} -m_3 x z^{p-1} \cdot l_3 y z^{p-1} & \equiv x^p y^p \mod \delta \\ l_3 m_3 \left(z^{p-1}\right)^2 & \equiv -x^{p-1} y^{p-1} \mod \delta \\ \left(z^{p-1}\right)^2 & \equiv -l_3^{-1} m_3^{-1} x^{p-1} y^{p-1} \mod \delta \end{array} \tag{48}$$

(46)(47)(48) より

$$-\left(m_3^{-1}x^{p-1}\right)^3 \equiv \left(l_3^{-1}y^{p-1}\right)^3 \equiv \left(z^{p-1}\right)^3 \mod \delta$$

$$\left(z^{p-1}\right)^3-\left(l_3^{-1}y^{p-1}\right)^3 \equiv (z^{p-1}-l_3^{-1}y^{p-1})((z^{p-1})^2+l_3^{-1}y^{p-1}z^{p-1}+(l_3^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(m_3^{-1}x^{p-1}\right)^3+\left(z^{p-1}\right)^3 \equiv (m_3^{-1}x^{p-1}+z^{p-1})((m_3^{-1}x^{p-1})^2-m_3^{-1}x^{p-1}z^{p-1}+(z^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(m_3^{-1}x^{p-1}\right)^3+\left(l_3^{-1}y^{p-1}\right)^3 \equiv (m_3^{-1}x^{p-1}+l_3^{-1}y^{p-1})((m_3^{-1}x^{p-1})^2-l_3^{-1}m_3^{-1}x^{p-1}y^{p-1}+(l_3^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

### 1.6.6 $-m_3^{-1}x^{p-1} \not\equiv l_3^{-1}y^{p-1} \not\equiv z^{p-1} \mod \delta$ のとき

(46)(47) より

$$\begin{aligned}
(l_3^{-1}y^{p-1})^2 + (m_3^{-1}x^{p-1})^2 + (z^{p-1})^2 &\equiv 0 \mod \theta_4 \\
-m_3^{-1}x^{p-1}z^{p-1} + l_3^{-1}y^{p-1}z^{p-1} + (z^{p-1})^2 &\equiv 0 \mod \theta_4 \\
m_3^{-1}x^{p-1} - l_3^{-1}y^{p-1} - z^{p-1} &\equiv 0 \mod \theta_4 \\
m_3^{-1}x^{p-1} - l_3^{-1}y^{p-1} &\equiv z^{p-1} \mod \theta_4
\end{aligned}$$

【General solution conditions】

$$\begin{array}{rcl}
x^p & -l_3^{-1}m_3y^{p-1}x & \equiv m_3z^{p-1}x \mod \theta_4 \\
-l_3m_3^{-1}x^{p-1}y & +y^p & \equiv -l_3z^{p-1}y \mod \theta_4 \\
m_3^{-1}x^{p-1}z & -l_3^{-1}y^{p-1}z & \equiv z^p \mod \theta_4
\end{array} \tag{49}$$

(49) より

$$\begin{aligned}
-l_3^{-1}m_3y^{p-1}x \cdot m_3z^{p-1}x &\equiv y^pz^p \mod \theta_4 \\
x^2 &\equiv -l_3m_3^{-2}yz \mod \theta_4
\end{aligned} \tag{50}$$

$$\begin{aligned}
-l_3m_3^{-1}x^{p-1}y \cdot -l_3z^{p-1}y &\equiv x^pz^p \mod \theta_4 \\
y^2 &\equiv l_3^{-2}m_3xz \mod \theta_4
\end{aligned} \tag{51}$$

$$\begin{aligned}
m_3^{-1}x^{p-1}z \cdot -l_3^{-1}y^{p-1}z &\equiv x^py^p \mod \theta_4 \\
z^2 &\equiv -l_3m_3xy \mod \theta_4
\end{aligned} \tag{52}$$

$$
\begin{aligned}
(46)\ \text{より}\ \left(x^{p-1}\right)^2 &\equiv l_3^{-1}m_3^2y^{p-1}z^{p-1} \mod \theta_4\\
\left(x^2\right)^{p-1} &\equiv l_3^{-1}m_3^2y^{p-1}z^{p-1} \mod \theta_4\\
(50)\ \text{より}\ \left(-l_3m_3^{-2}yz\right)^{p-1} &\equiv l_3^{-1}m_3^2y^{p-1}z^{p-1} \mod \theta_4\\
l_3^{p-1}m_3^{-2p+2}y^{p-1}z^{p-1} &\equiv l_3^{-1}m_3^2y^{p-1}z^{p-1} \mod \theta_4\\
l_3^pm_3^{-2p} &\equiv 1 \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
(47)\ \text{より}\ \left(y^{p-1}\right)^2 &\equiv -l_3^2m_3^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
\left(y^2\right)^{p-1} &\equiv -l_3^2m_3^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
(51)\ \text{より}\ \left(l_3^{-2}m_3xz\right)^{p-1} &\equiv -l_3^2m_3^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
l_3^{-2p+2}m_3^{p-1}x^{p-1}z^{p-1} &\equiv -l_3^2m_3^{-1}x^{p-1}z^{p-1} \mod \theta_4\\
l_3^{-2p}m_3^p &\equiv -1 \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
(48)\ \text{より}\ \left(z^{p-1}\right)^2 &\equiv -l_3^{-1}m_3^{-1}x^{p-1}y^{p-1} \mod \theta_4\\
\left(z^2\right)^{p-1} &\equiv -l_3^{-1}m_3^{-1}x^{p-1}y^{p-1} \mod \theta_4\\
(52)\ \text{より}\ \left(-l_3m_3xy\right)^{p-1} &\equiv -l_3^{-1}m_3^{-1}x^{p-1}y^{p-1} \mod \theta_4\\
l_3^{p-1}m_3^{p-1}x^{p-1}y^{p-1} &\equiv -l_3^{-1}m_3^{-1}x^{p-1}y^{p-1} \mod \theta_4\\
l_3^pm_3^p &\equiv -1 \mod \theta_4
\end{aligned}
$$

$$l_3^p m_3^p \equiv -1 \mod \theta_4$$
$$l_3^{-2p} m_3^p \equiv -1 \mod \theta_4$$
$$l_3^p m_3^{-2p} \equiv 1 \mod \theta_4$$

$$-m_3^{3p} \equiv l_3^{3p} \mod \theta_4$$
$$m_3^{3p} + l_3^{3p} \equiv (m_3^p + l_3^p)(m_3^{2p} - l_3^p m_3^p + l_3^{2p}) \mod \theta_4$$

$$-m_3^p \equiv l_3^{2p} \mod \theta_4$$
$$l_3^p \equiv m_3^{2p} \mod \theta_4$$

$$-l_3^p - m_3^p \equiv l_3^{2p} - m_3^{2p} \mod \theta_4$$
$$-(l_3^p + m_3^p) \equiv (l_3^p + m_3^p)(l_3^p - m_3^p) \mod \theta_4$$
$$-1 \equiv l_3^p - m_3^p \mod \theta_4$$

$$(l_3^p - m_3^p)^2 \equiv (-1)^2 \mod \theta_4$$
$$l_3^{2p} - 2l_3^p m_3^p + m_3^{2p} \equiv 1 \mod \theta_4$$
$$l_3^{2p} - 2l_3^p m_3^p + m_3^{2p} \equiv -l_3^p m_3^p \mod \theta_4$$
$$l_3^{2p} - l_3^p m_3^p + m_3^{2p} \equiv 0 \mod \theta_4$$

よって $m_3^p + l_3^p \not\equiv 0 \mod \theta_4$

$$l_3^p - m_3^p \equiv -1 \mod \theta_4$$
$$l_3^{2p} - l_3^p m_3^p \equiv -l_3^p \mod \theta_4$$
$$l_3^{2p} + l_3^p + 1 \equiv 0 \mod \theta_4$$

(23)(34)(45) より

$$\begin{aligned} -m_1^{-1} x z^{p-1} &\equiv -m_3 x z^{p-1} \mod \delta \\ m_1^{-1} &\equiv m_3 \mod \delta \\ 1 &\equiv m_1^p m_3^p \mod \delta \end{aligned} \tag{53}$$

$$\begin{aligned} l_3^{-1} z y^{p-1} &\equiv m_2 z y^{p-1} \mod \delta \\ l_3^{-1} &\equiv m_2 \mod \delta \end{aligned} \tag{54}$$

$l_3^p m_3^p \equiv -1 \mod \theta_4$ なので

$$l_3^p \equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \tag{55}$$
$$m_3^p \equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \tag{56}$$

### 1.6.7 Cycle

$$\begin{aligned}
\left(\frac{-1 \pm \sqrt{-3}}{2}\right)^1 &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta \\
\left(\frac{-1 \pm \sqrt{-3}}{2}\right)^2 &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta \\
\left(\frac{-1 \pm \sqrt{-3}}{2}\right)^3 &\equiv 1 \mod \theta
\end{aligned}$$

$$\begin{aligned}
\left(\frac{1 \pm \sqrt{-3}}{2}\right)^1 &\equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta \\
\left(\frac{1 \pm \sqrt{-3}}{2}\right)^2 &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta \\
\left(\frac{1 \pm \sqrt{-3}}{2}\right)^3 &\equiv -1 \mod \theta \\
\left(\frac{1 \pm \sqrt{-3}}{2}\right)^4 &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta \\
\left(\frac{1 \pm \sqrt{-3}}{2}\right)^5 &\equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta \\
\left(\frac{1 \pm \sqrt{-3}}{2}\right)^6 &\equiv 1 \mod \theta
\end{aligned}$$

### 1.6.8 A splice

(28) より

$$\begin{aligned} x^2 &\equiv -l_1 m_1 yz \mod \theta_4 \\ -x^2 &\equiv -l_1 y \cdot -m_1 z \mod \theta_4 \\ -x^2 &\equiv (-y+k_1)(-z+k_1) \mod \theta_4 \\ -x^2 &\equiv yz-(y+z)k_1+k_1^2 \mod \theta_4 \\ 0 &\equiv k_1^2-(y+z)k_1+yz+x^2 \mod \theta_4 \end{aligned}$$

$$\begin{aligned} k_1 &\equiv \frac{y+z\pm\sqrt{(y+z)^2-4(yz+x^2)}}{2} \mod \theta_4 \\ k_1 &\equiv \frac{y+z\pm\sqrt{(y-z)^2-4x^2}}{2} \mod \theta_4 \\ k_1 &\equiv \frac{y+z\pm\sqrt{x^2-4x^2}}{2} \mod \theta_4 \\ k_1 &\equiv \frac{y+z\pm\sqrt{-3x^2}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -y+k_1 &\equiv \frac{-y+z\pm\sqrt{-3x^2}}{2} \mod \theta_4 \\ -z+k_1 &\equiv \frac{y-z\pm\sqrt{-3x^2}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -l_1 y &\equiv x\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_4 \\ -m_1 z &\equiv x\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -l_1 y x^{p-1} &\equiv x^p\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_4 \\ -m_1 z x^{p-1} &\equiv x^p\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -z^p &\equiv x^p\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_4 \\ -y^p &\equiv x^p\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_4 \end{aligned} \tag{57}$$

$$
\begin{aligned}
-y &\equiv xl_1^{-1} \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \\
-z &\equiv xm_1^{-1} \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

(42)(53) より

$$
\begin{aligned}
-y &\equiv xl_2 \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \\
-z &\equiv xm_3 \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
-y^p &\equiv x^p l_2^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4 \\
-z^p &\equiv x^p m_3^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4
\end{aligned}
$$

(57) より

$$
\begin{aligned}
\frac{1 \pm \sqrt{-3}}{2} &\equiv l_2^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4 \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv m_3^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4
\end{aligned}
$$

(43)(56) より

$$
\begin{aligned}
\frac{1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \mp \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4 \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \pm \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4
\end{aligned}
$$

$l_1^p \equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4$ のとき

$$
\begin{aligned}
\frac{1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \pm \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4 \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \mp \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4
\end{aligned}
$$

(40) より

$$\begin{aligned} y^2 &\equiv l_2 m_2 xz \mod \theta_4 \\ -y^2 &\equiv l_2 x \cdot -m_2 z \mod \theta_4 \\ -y^2 &\equiv (x+k_2)(-z+k_2) \mod \theta_4 \\ -y^2 &\equiv -xz + (x-z)k_2 + k_2^2 \mod \theta_4 \\ 0 &\equiv k_2^2 + (x-z)k_2 - xz + y^2 \mod \theta_4 \end{aligned}$$

$$\begin{aligned} k_2 &\equiv \frac{z-x \pm \sqrt{(x-z)^2 - 4(-xz+y^2)}}{2} \mod \theta_4 \\ k_2 &\equiv \frac{z-x \pm \sqrt{(x+z)^2 - 4y^2}}{2} \mod \theta_4 \\ k_2 &\equiv \frac{z-x \pm \sqrt{y^2 - 4y^2}}{2} \mod \theta_4 \\ k_2 &\equiv \frac{z-x \pm \sqrt{-3y^2}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} x + k_2 &\equiv \frac{z+x \pm \sqrt{-3y^2}}{2} \mod \theta_4 \\ -z + k_2 &\equiv \frac{-z-x \pm \sqrt{-3y^2}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} l_2 x &\equiv y \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \\ -m_2 z &\equiv y \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} l_2 x y^{p-1} &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \\ -m_2 z y^{p-1} &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} z^p &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \\ x^p &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \end{aligned} \tag{58}$$

$$
\begin{aligned}
x &\equiv yl_2^{-1} \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \\
-z &\equiv ym_2^{-1} \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

(42)(54) より

$$
\begin{aligned}
x &\equiv yl_1 \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \\
-z &\equiv yl_3 \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
x^p &\equiv y^p l_1^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4 \\
-z^p &\equiv y^p l_3^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4
\end{aligned}
$$

(58) より

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv l_1^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4 \\
\frac{-1 \mp \sqrt{-3}}{2} &\equiv l_3^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4
\end{aligned}
$$

(32)(55) より

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \left(\frac{1 \pm \sqrt{-3}}{2}\right) \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4 \\
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{-1 \pm \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4
\end{aligned}
$$

$l_1^p \equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4$ のとき

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \left(\frac{1 \mp \sqrt{-3}}{2}\right) \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4 \\
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{-1 \mp \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4
\end{aligned}
$$

(52) より

$$\begin{aligned} z^2 &\equiv -l_3 m_3 xy \mod \theta_4 \\ -z^2 &\equiv -m_3 x \cdot -l_3 y \mod \theta_4 \\ -z^2 &\equiv (-x+k_3)(-y+k_3) \mod \theta_4 \\ -z^2 &\equiv xy-(x+y)k_3+k_3^2 \mod \theta_4 \\ 0 &\equiv k_3^2-(x+y)k_3+xy+z^2 \mod \theta_4 \end{aligned}$$

$$\begin{aligned} k_3 &\equiv \frac{x+y\pm\sqrt{(x+y)^2-4(xy+z^2)}}{2} \mod \theta_4 \\ k_3 &\equiv \frac{x+y\pm\sqrt{(x-y)^2-4z^2}}{2} \mod \theta_4 \\ k_3 &\equiv \frac{x+y\pm\sqrt{z^2-4z^2}}{2} \mod \theta_4 \\ k_3 &\equiv \frac{x+y\pm\sqrt{-3z^2}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -y+k_3 &\equiv \frac{-y+x\pm\sqrt{-3z^2}}{2} \mod \theta_4 \\ -x+k_3 &\equiv \frac{y-x\pm\sqrt{-3z^2}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -l_3 y &\equiv z\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_4 \\ -m_3 x &\equiv z\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} -l_3 y z^{p-1} &\equiv z^p\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_4 \\ -m_3 x z^{p-1} &\equiv z^p\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_4 \end{aligned}$$

(57) より ± の調整

$$\begin{aligned} -x^p &\equiv z^p\cdot\frac{-1\mp\sqrt{-3}}{2} \mod \theta_4 \\ y^p &\equiv z^p\cdot\frac{1\mp\sqrt{-3}}{2} \mod \theta_4 \end{aligned} \tag{59}$$

$$
\begin{aligned}
-y &\equiv zl_3^{-1}\cdot\frac{-1\mp\sqrt{-3}}{2} \mod \theta_4\\
-x &\equiv zm_3^{-1}\cdot\frac{1\mp\sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

(54)(53) より

$$
\begin{aligned}
-y &\equiv zm_2\cdot\frac{-1\mp\sqrt{-3}}{2} \mod \theta_4\\
-x &\equiv zm_1\cdot\frac{1\mp\sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
-y^p &\equiv z^p m_2^p\cdot\left(\frac{-1\mp\sqrt{-3}}{2}\right)^p \mod \theta_4\\
-x^p &\equiv z^p m_1^p\cdot\left(\frac{1\mp\sqrt{-3}}{2}\right)^p \mod \theta_4
\end{aligned}
$$

(59) より

$$
\begin{aligned}
\frac{-1\pm\sqrt{-3}}{2} &\equiv m_2^p\cdot\left(\frac{-1\mp\sqrt{-3}}{2}\right)^p \mod \theta_4\\
\frac{-1\mp\sqrt{-3}}{2} &\equiv m_1^p\cdot\left(\frac{1\mp\sqrt{-3}}{2}\right)^p \mod \theta_4
\end{aligned}
$$

(44)(33) より

$$
\begin{aligned}
\frac{-1\pm\sqrt{-3}}{2} &\equiv \left(\frac{-1\mp\sqrt{-3}}{2}\right)\cdot\left(\frac{-1\mp\sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4\\
\frac{-1\mp\sqrt{-3}}{2} &\equiv \left(\frac{1\mp\sqrt{-3}}{2}\right)\cdot\left(\frac{1\mp\sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4
\end{aligned}
$$

$l_1^p \equiv \frac{1\mp\sqrt{-3}}{2} \mod \theta_4$ のとき

$$
\begin{aligned}
\frac{-1\pm\sqrt{-3}}{2} &\equiv \left(\frac{-1\pm\sqrt{-3}}{2}\right)\cdot\left(\frac{-1\mp\sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4\\
\frac{-1\mp\sqrt{-3}}{2} &\equiv \left(\frac{1\pm\sqrt{-3}}{2}\right)\cdot\left(\frac{1\mp\sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4
\end{aligned}
$$

### 1.6.9 $p = 6n + 1$ のとき

$$
\begin{aligned}
l_1^p \equiv l_1 &\equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4 \\
m_1^p \equiv m_1 &\equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4 \\
l_2^p \equiv l_2 &\equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4 \\
m_2^p \equiv m_2 &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4 \\
l_3^p \equiv l_3 &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4 \\
m_3^p \equiv m_3 &\equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4
\end{aligned}
$$

(28)(40)(52) より

$$
\begin{aligned}
x^2 &\equiv -l_1 m_1 yz \mod \theta_4 \\
x^2 &\equiv -yz \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
y^2 &\equiv l_2 m_2 xz \mod \theta_4 \\
y^2 &\equiv -xz \mod \theta_4
\end{aligned}
$$

$$
\begin{aligned}
z^2 &\equiv -l_3 m_3 xy \mod \theta_4 \\
z^2 &\equiv xy \mod \theta_4
\end{aligned}
$$

$$
-z^3 \equiv x^3 \equiv y^3 \mod \theta_4
$$

$$
\begin{aligned}
z^3 + y^3 &\equiv (z+y)(z^2 - yz + y^2) \equiv 0 \mod \theta_4 \\
x^3 + z^3 &\equiv (x+z)(x^2 - xz + z^2) \equiv 0 \mod \theta_4 \\
x^3 - y^3 &\equiv (x-y)(x^2 + xy + y^2) \equiv 0 \mod \theta_4
\end{aligned}
$$

$x + z - y \equiv 0 \mod \theta_4$ なので

$$
x + z \not\equiv 0 \mod \theta_4
$$

$$
\begin{aligned}
x^2 - xz + z^2 &\equiv 0 \mod \theta_4 \\
x^2 - xz + xy &\equiv 0 \mod \theta_4 \\
x - z + y &\not\equiv 0 \mod \theta_4
\end{aligned}
$$

よって $p = 6n + 1$ は満たさない。

### 1.6.10 $p = 6n + 3$ のとき

$p$ は素数なので $n = 0$ ， $p = 3$、$x^3 + y^3 \equiv z^3 \mod \theta_4$

$$
\begin{aligned}
(x + z - y)^3 &\equiv x^3 + z^3 - y^3 - 3x^2y + 3x^2z + 3xy^2 + 3xz^2 + 3y^2z - 3yz^2 - 6xyz \mod \theta_4 \\
(x + z - y)^3 &\equiv 2x^3 + 3(-x^2y + x^2z + xy^2 + xz^2 + y^2z - yz^2 - 2xyz) \mod \theta_4 \\
(x + z - y)^3 &\equiv 2x^3 + 3(-y(x^2 + 2xz + z^2) + (x + z)xz + (x + z)y^2) \mod \theta_4 \\
(x + z - y)^3 &\equiv 2x^3 + 3(-y(x + z)^2 + (x + z)xz + (x + z)y^2) \mod \theta_4 \\
(x + z - y)^3 &\equiv 2x^3 + 3(x + z)(-xy - yz + xz + y^2) \mod \theta_4 \\
(x + z - y)^3 &\equiv 2x^3 + 3(x + z)(-x(y - z) + y(y - z)) \mod \theta_4 \\
(x + z - y)^3 &\equiv 2x^3 + 3(x + z)(y - z)(y - x) \mod \theta_4 \\
0 &\equiv 2x^3 + 3yxz \mod \theta_4 \\
-2x^2 &\equiv 3yz \mod \theta_4
\end{aligned}
$$

(28) より

$$
\begin{aligned}
2l_1m_1yz &\equiv 3yz \mod \theta_4 \\
2l_1m_1 &\equiv 3 \mod \theta_4 \\
2^p l_1^p m_1^p &\equiv 3^p \mod \theta_4
\end{aligned}
$$

(31) より

$$
\begin{aligned}
2^3 &\equiv 3^3 \mod \theta_4 \\
8 &\equiv 27 \mod \theta_4 \\
0 &\equiv 19 \mod \theta_4
\end{aligned}
$$

## 1.7 $-x^{p-1} \equiv l_1^{-1} y^{p-1} \equiv m_1^{-1} z^{p-1} \mod \delta$ のとき

$x - y + k_1 \equiv -z + k_1 \mod \delta$ より

$-y + k_1 \equiv -l_1 y \mod \delta \quad , \ -z + k_1 \equiv -m_1 z \mod \delta$

$$\begin{aligned} x & \quad -l_1 y & & \equiv -m_1 z \mod \delta \\ x^p & \quad -l_1 y x^{p-1} & & \equiv -m_1 z x^{p-1} \mod \delta \\ x^p & \quad -z^p & & \equiv -y^p \mod \theta_4 \\ x^p & \quad +(-y + k_1) x^{p-1} & & \equiv (-z + k_1) x^{p-1} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} x^p & \quad +y^p & & \equiv z^p \mod \theta_4 \\ x^p & \quad +(z - k_1) x^{p-1} & & \equiv (y - k_1) x^{p-1} \mod \theta_4 \\ x^p & \quad +m_1 z x^{p-1} & & \equiv l_1 y x^{p-1} \mod \theta_4 \\ x & \quad +m_1 z & & \equiv l_1 y \mod \theta_4 \end{aligned}$$

**Definition 16** $z - k_1 \equiv q_1 y \mod \delta \quad , \ y - k_1 \equiv r_1 z \mod \delta \quad , \ q_1 r_1 \perp \delta$

$$\begin{aligned} m_1 z & \equiv q_1 y \mod \delta \\ l_1 y & \equiv r_1 z \mod \delta \end{aligned}$$

$$x + q_1 y \equiv r_1 z \mod \delta$$

$$\begin{aligned} x^p & \quad +q_1 y x^{p-1} & & \equiv r_1 z x^{p-1} \mod \delta \\ q_1^{-1} x y^{p-1} & \quad +y^p & & \equiv q_1^{-1} r_1 z y^{p-1} \mod \delta \\ r_1^{-1} x z^{p-1} & \quad +q_1 r_1^{-1} y z^{p-1} & & \equiv z^p \mod \delta \end{aligned} \tag{60}$$

### 1.7.1 Common to $x^{p-1} \not\equiv q_1^{-1} y^{p-1} \not\equiv r_1^{-1} z^{p-1} \mod \delta$

(60) より

$$\begin{aligned} q_1 y x^{p-1} \cdot r_1 z x^{p-1} & \equiv y^p z^p \mod \delta \\ q_1 r_1 \left(x^{p-1}\right)^2 & \equiv y^{p-1} z^{p-1} \mod \delta \\ \left(x^{p-1}\right)^2 & \equiv q_1^{-1} r_1^{-1} y^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{61}$$

$$\begin{aligned} q_1^{-1} x y^{p-1} \cdot q_1^{-1} r_1 z y^{p-1} & \equiv x^p z^p \mod \delta \\ q_1^{-2} r_1 \left(y^{p-1}\right)^2 & \equiv x^{p-1} z^{p-1} \mod \delta \\ \left(q_1^{-1} y^{p-1}\right)^2 & \equiv r_1^{-1} x^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{62}$$

$$\begin{aligned} r_1^{-1} x z^{p-1} \cdot q_1 r_1^{-1} y z^{p-1} & \equiv x^p y^p \mod \delta \\ q_1 r_1^{-2} \left(z^{p-1}\right)^2 & \equiv x^{p-1} y^{p-1} \mod \delta \\ \left(r_1^{-1} z^{p-1}\right)^2 & \equiv q_1^{-1} x^{p-1} y^{p-1} \mod \delta \end{aligned} \tag{63}$$

(61)(62)(63) より

$$\left(x^{p-1}\right)^3 \equiv \left(q_1^{-1}y^{p-1}\right)^3 \equiv \left(r_1^{-1}z^{p-1}\right)^3 \mod \delta$$

$$\left(r_1^{-1}z^{p-1}\right)^3-\left(q_1^{-1}y^{p-1}\right)^3 \equiv (r_1^{-1}z^{p-1}-q_1^{-1}y^{p-1})((r_1^{-1}z^{p-1})^2+q_1^{-1}r_1^{-1}y^{p-1}z^{p-1}+(q_1^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(x^{p-1}\right)^3-\left(r_1^{-1}z^{p-1}\right)^3 \equiv (x^{p-1}-r_1^{-1}z^{p-1})((x^{p-1})^2+r_1^{-1}x^{p-1}z^{p-1}+(r_1^{-1}z^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(x^{p-1}\right)^3-\left(q_1^{-1}y^{p-1}\right)^3 \equiv (x^{p-1}-q_1^{-1}y^{p-1})((x^{p-1})^2+q_1^{-1}x^{p-1}y^{p-1}+(q_1^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

### 1.7.2 $x^{p-1} \not\equiv q_1^{-1}y^{p-1} \not\equiv r_1^{-1}z^{p-1} \mod \delta$ のとき

(62)(63) より

$$\begin{aligned}(x^{p-1})^2 + (r_1^{-1}z^{p-1})^2 + (q_1^{-1}y^{p-1})^2 &\equiv 0 \mod \theta_1\\ (x^{p-1})^2 + q_1^{-1}x^{p-1}y^{p-1} + r_1^{-1}x^{p-1}z^{p-1} &\equiv 0 \mod \theta_1\\ x^{p-1} + q_1^{-1}y^{p-1} + r_1^{-1}z^{p-1} &\equiv 0 \mod \theta_1\\ x^{p-1} + q_1^{-1}y^{p-1} &\equiv -r_1^{-1}z^{p-1} \mod \theta_1\end{aligned}$$

【General solution conditions】

$$\begin{aligned}x^p \quad +q_1^{-1}y^{p-1}x \quad &\equiv -r_1^{-1}z^{p-1}x \mod \theta_1\\ q_1x^{p-1}y \quad +y^p \quad &\equiv -q_1r_1^{-1}z^{p-1}y \mod \theta_1\\ -r_1x^{p-1}z \quad -q_1^{-1}r_1y^{p-1}z \quad &\equiv z^p \mod \theta_1\end{aligned} \tag{64}$$

(64) より

$$\begin{aligned}q_1^{-1}y^{p-1}x \cdot -r_1^{-1}z^{p-1}x &\equiv y^pz^p \mod \theta_1\\ x^2 &\equiv -q_1r_1yz \mod \theta_1\end{aligned} \tag{65}$$

$$\begin{aligned}q_1x^{p-1}y \cdot -q_1r_1^{-1}z^{p-1}y &\equiv x^pz^p \mod \theta_1\\ y^2 &\equiv -q_1^{-2}r_1xz \mod \theta_1\end{aligned} \tag{66}$$

$$\begin{aligned}-r_1x^{p-1}z \cdot -q_1^{-1}r_1y^{p-1}z &\equiv x^py^p \mod \theta_1\\ z^2 &\equiv q_1r_1^{-2}xy \mod \theta_1\end{aligned} \tag{67}$$

$$
\begin{aligned}
\text{(61) より } \left(x^{p-1}\right)^2 &\equiv q_1^{-1} r_1^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
\left(x^2\right)^{p-1} &\equiv q_1^{-1} r_1^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
\text{(65) より } (-q_1 r_1 yz)^{p-1} &\equiv q_1^{-1} r_1^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
q_1^{p-1} r_1^{p-1} y^{p-1} z^{p-1} &\equiv q_1^{-1} r_1^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
q_1^p r_1^p y^{p-1} z^{p-1} &\equiv y^{p-1} z^{p-1} \mod \theta_1 \\
q_1^p r_1^p &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
\text{(62) より } \left(y^{p-1}\right)^2 &\equiv q_1^2 r_1^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
\left(y^2\right)^{p-1} &\equiv q_1^2 r_1^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
\text{(66) より } \left(-q_1^{-2} r_1 xz\right)^{p-1} &\equiv q_1^2 r_1^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
q_1^{-2p+2} r_1^{p-1} x^{p-1} z^{p-1} &\equiv q_1^2 r_1^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
q_1^{-2p} r_1^p x^{p-1} z^{p-1} &\equiv x^{p-1} z^{p-1} \mod \theta_1 \\
q_1^{-2p} r_1^p &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
\text{(63) より } \left(z^{p-1}\right)^2 &\equiv q_1^{-1} r_1^2 x^{p-1} y^{p-1} \mod \theta_1 \\
\left(z^2\right)^{p-1} &\equiv q_1^{-1} r_1^2 x^{p-1} y^{p-1} \mod \theta_1 \\
\text{(67) より } \left(q_1 r_1^{-2} xy\right)^{p-1} &\equiv q_1^{-1} r_1^2 x^{p-1} y^{p-1} \mod \theta_1 \\
q_1^{p-1} r_1^{-2p+2} x^{p-1} y^{p-1} &\equiv q_1^{-1} r_1^2 x^{p-1} y^{p-1} \mod \theta_1 \\
q_1^p r_1^{-2p} x^{p-1} y^{p-1} &\equiv x^{p-1} y^{p-1} \mod \theta_1 \\
q_1^p r_1^{-2p} &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$\begin{aligned} q_1^p r_1^p &\equiv 1 \mod \theta_1 \\ q_1^{-2p} r_1^p &\equiv 1 \mod \theta_1 \\ q_1^p r_1^{-2p} &\equiv 1 \mod \theta_1 \end{aligned} \tag{68}$$

$$\begin{aligned} r_1^{3p} &\equiv q_1^{3p} \mod \theta_1 \\ r_1^{3p} - q_1^{3p} &\equiv (r_1^p - q_1^p)(r_1^{2p} + q_1^p r_1^p + q_1^{2p}) \mod \theta_1 \end{aligned}$$

$$\begin{aligned} r_1^p &\equiv q_1^{2p} \mod \theta_1 \\ q_1^p &\equiv r_1^{2p} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} r_1^p - q_1^p &\equiv q_1^{2p} - r_1^{2p} \mod \theta_1 \\ r_1^p - q_1^p &\equiv (q_1^p + r_1^p)(q_1^p - r_1^p) \mod \theta_1 \\ -1 &\equiv q_1^p + r_1^p \mod \theta_1 \end{aligned}$$

$$\begin{aligned} (q_1^p + r_1^p)^2 &\equiv (-1)^2 \mod \theta_1 \\ q_1^{2p} + 2q_1^p r_1^p + r_1^{2p} &\equiv 1 \mod \theta_1 \\ q_1^{2p} + 2q_1^p r_1^p + r_1^{2p} &\equiv q_1^p r_1^p \mod \theta_1 \\ q_1^{2p} + q_1^p r_1^p + r_1^{2p} &\equiv 0 \mod \theta_1 \end{aligned}$$

$r_1^p - q_1^p \not\equiv 0 \mod \theta_1$ なので $r_1 \equiv -1 \mod \theta_1$ , $q_1 \equiv -1 \mod \theta_1$ のとき
$x^p + y^p \not\equiv z^p \mod \theta_1$

$$\begin{aligned} q_1^p + r_1^p &\equiv -1 \mod \theta_1 \\ q_1^{2p} + q_1^p r_1^p &\equiv -q_1^p \mod \theta_1 \\ q_1^{2p} + q_1^p + 1 &\equiv 0 \mod \theta_1 \end{aligned}$$

$q_1^p r_1^p \equiv 1 \mod \theta_1$ なので

$$q_1^p \equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \tag{69}$$

$$r_1^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \tag{70}$$

$x + k_2 - y \equiv -z + k_2 \mod \delta$ より

$x + k_2 \equiv l_2 x \mod \delta$ , $-z + k_2 \equiv -m_2 z \mod \delta$

$$\begin{aligned} l_2 x \quad -y \quad &\equiv -m_2 z \mod \delta \\ \\ -l_2 x y^{p-1} \quad +y^p \quad &\equiv m_2 z y^{p-1} \mod \delta \\ -z^p \quad +y^p \quad &\equiv -x^p \mod \theta_4 \\ -(x+k_2) y^{p-1} \quad +y^p \quad &\equiv (z-k_2) y^{p-1} \mod \theta_4 \\ \\ x^p \quad +y^p \quad &\equiv z^p \mod \theta_4 \\ (-z+k_2) y^{p-1} \quad +y^p \quad &\equiv (x+k_2) y^{p-1} \mod \theta_4 \\ -m_2 z y^{p-1} \quad +y^p \quad &\equiv l_2 x y^{p-1} \mod \theta_4 \\ m_2 z \quad -y \quad &\equiv -l_2 x \mod \theta_4 \end{aligned}$$

**Definition 17** $-z + k_2 \equiv q_2 x \mod \delta$ , $x + k_2 \equiv r_2 z \mod \delta$ , $q_2 r_2 \perp \delta$

$$\begin{aligned} -m_2 z \quad &\equiv q_2 x \mod \delta \\ l_2 x \quad &\equiv r_2 z \mod \delta \end{aligned}$$

$$q_2 x + y \equiv r_2 z \mod \delta$$

$$\begin{aligned} x^p \quad +q_2^{-1} y x^{p-1} \quad &\equiv q_2^{-1} r_2 z x^{p-1} \mod \delta \\ q_2 x y^{p-1} \quad +y^p \quad &\equiv r_2 z y^{p-1} \mod \delta \\ q_2 r_2^{-1} x z^{p-1} \quad +r_2^{-1} y z^{p-1} \quad &\equiv z^p \mod \delta \end{aligned} \tag{71}$$

### 1.7.3 Common to $q_2^{-1} x^{p-1} \not\equiv y^{p-1} \not\equiv r_2^{-1} z^{p-1} \mod \delta$

(71) より

$$\begin{aligned} q_2^{-1} y x^{p-1} \cdot q_2^{-1} r_2 z x^{p-1} \quad &\equiv y^p z^p \mod \delta \\ q_2^{-2} r_2 \left(x^{p-1}\right)^2 \quad &\equiv y^{p-1} z^{p-1} \mod \delta \\ \left(q_2^{-1} x^{p-1}\right)^2 \quad &\equiv r_2^{-1} y^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{72}$$

$$\begin{aligned} q_2 x y^{p-1} \cdot r_2 y^{p-1} z \quad &\equiv x^p z^p \mod \delta \\ q_2 r_2 \left(y^{p-1}\right)^2 \quad &\equiv x^{p-1} z^{p-1} \mod \delta \\ \left(y^{p-1}\right)^2 \quad &\equiv q_2^{-1} r_2^{-1} x^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{73}$$

$$\begin{aligned} q_2 r_2^{-1} x z^{p-1} \cdot r_2^{-1} y z^{p-1} \quad &\equiv x^p y^p \mod \delta \\ q_2 r_2^{-2} \left(z^{p-1}\right)^2 \quad &\equiv x^{p-1} y^{p-1} \mod \delta \\ \left(r_2^{-1} z^{p-1}\right)^2 \quad &\equiv q_2^{-1} x^{p-1} y^{p-1} \mod \delta \end{aligned} \tag{74}$$

(72)(73)(74) より

$$\left(q_2^{-1}x^{p-1}\right)^3 \equiv \left(y^{p-1}\right)^3 \equiv \left(r_2^{-1}z^{p-1}\right)^3 \mod \delta$$

$$\left(y^{p-1}\right)^3-\left(r_2^{-1}z^{p-1}\right)^3 \equiv (y^{p-1}-r_2^{-1}z^{p-1})((y^{p-1})^2+r_2^{-1}y^{p-1}z^{p-1}+(r_2^{-1}z^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(q_2^{-1}x^{p-1}\right)^3-\left(y^{p-1}\right)^3 \equiv (q_2^{-1}x^{p-1}-y^{p-1})((q_2^{-1}x^{p-1})^2+q_2^{-1}x^{p-1}y^{p-1}+(y^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(q_2^{-1}x^{p-1}\right)^3-\left(r_2^{-1}z^{p-1}\right)^3 \equiv (q_2^{-1}x^{p-1}-r_2^{-1}z^{p-1})((q_2^{-1}x^{p-1})^2+q_2^{-1}r_2^{-1}x^{p-1}z^{p-1}+(r_2^{-1}z^{p-1})^2) \equiv 0 \mod \delta$$

### 1.7.4 $q_2^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv r_2^{-1}z^{p-1} \mod \delta$ のとき

(72)(74) より

$$\begin{aligned}
(r_2^{-1}z^{p-1})^2 + (y^{p-1})^2 + (q_2^{-1}x^{p-1})^2 &\equiv 0 \mod \theta_1 \\
q_2^{-1}x^{p-1}y^{p-1} + (y^{p-1})^2 + r_2^{-1}y^{p-1}z^{p-1} &\equiv 0 \mod \theta_1 \\
q_2^{-1}x^{p-1} + y^{p-1} + r_2^{-1}z^{p-1} &\equiv 0 \mod \theta_1 \\
q_2^{-1}x^{p-1} + y^{p-1} &\equiv -r_2^{-1}z^{p-1} \mod \theta_1
\end{aligned}$$

【General solution conditions】

$$\begin{array}{rrl}
x^p & +q_2y^{p-1}x & \equiv -q_2r_2^{-1}z^{p-1}x \mod \theta_1 \\
q_2^{-1}x^{p-1}y & +y^p & \equiv -r_2^{-1}z^{p-1}y \mod \theta_1 \\
-q_2^{-1}r_2x^{p-1}z & -r_2y^{p-1}z & \equiv z^p \mod \theta_1
\end{array} \tag{75}$$

(75) より

$$\begin{aligned}
q_2y^{p-1}x \cdot -q_2r_2^{-1}z^{p-1}x &\equiv y^pz^p \mod \theta_1 \\
x^2 &\equiv -q_2^{-2}r_2yz \mod \theta_1
\end{aligned} \tag{76}$$

$$\begin{aligned}
q_2^{-1}x^{p-1}y \cdot -r_2^{-1}z^{p-1}y &\equiv x^pz^p \mod \theta_1 \\
y^2 &\equiv -q_2r_2xz \mod \theta_1
\end{aligned} \tag{77}$$

$$\begin{aligned}
-q_2^{-1}r_2x^{p-1}z \cdot -r_2y^{p-1}z &\equiv x^py^p \mod \theta_1 \\
z^2 &\equiv q_2r_2^{-2}xy \mod \theta_1
\end{aligned} \tag{78}$$

$$
\begin{aligned}
\text{(72) より } \left(x^{p-1}\right)^2 &\equiv q_2^2 r_2^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
\left(x^2\right)^{p-1} &\equiv q_2^2 r_2^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
\text{(76) より } \left(-q_2^{-2} r_2 yz\right)^{p-1} &\equiv q_2^2 r_2^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
q_2^{-2p+2} r_2^{p-1} y^{p-1} z^{p-1} &\equiv q_2^2 r_2^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
q_2^{-2p} r_2^p &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
\text{(73) より } \left(y^{p-1}\right)^2 &\equiv q_2^{-1} r_2^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
\left(y^2\right)^{p-1} &\equiv q_2^{-1} r_2^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
\text{(77) より } \left(-q_2 r_2 xz\right)^{p-1} &\equiv q_2^{-1} r_2^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
q_2^{p-1} r_2^{p-1} x^{p-1} z^{p-1} &\equiv q_2^{-1} r_2^{-1} x^{p-1} z^{p-1} \mod \theta_1 \\
q_2^p r_2^p &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
\text{(74) より } \left(z^{p-1}\right)^2 &\equiv q_2^{-1} r_2^2 x^{p-1} y^{p-1} \mod \theta_1 \\
\left(z^2\right)^{p-1} &\equiv q_2^{-1} r_2^2 x^{p-1} y^{p-1} \mod \theta_1 \\
\text{(78) より } \left(q_2 r_2^{-2} xy\right)^{p-1} &\equiv q_2^{-1} r_2^2 x^{p-1} y^{p-1} \mod \theta_1 \\
q_2^{p-1} r_2^{-2p+2} x^{p-1} y^{p-1} &\equiv q_2^{-1} r_2^2 x^{p-1} y^{p-1} \mod \theta_1 \\
q_2^p r_2^{-2p} &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
q_2^p r_2^p &\equiv 1 \mod \theta_1 \\
q_2^{-2p} r_2^p &\equiv 1 \mod \theta_1 \\
q_2^p r_2^{-2p} &\equiv 1 \mod \theta_1
\end{aligned}
$$

(71)(60) より

$$
\begin{aligned}
q_2^{-1} y x^{p-1} &\equiv q_1 y x^{p-1} \mod \delta \\
q_2^{-1} &\equiv q_1 \mod \delta \\
1 &\equiv q_1^p q_2^p \mod \delta
\end{aligned} \tag{79}
$$

であるから (69) より

$$
q_2^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \tag{80}
$$

$$
r_2^p \equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \tag{81}
$$

$x - k_3 - y + k_3 \equiv -z \mod \delta$ より

$x - k_3 \equiv m_3 x \mod \delta$ , $-y + k_3 \equiv -l_3 y \mod \delta$

$$m_3 x \quad -l_3 y \quad \equiv -z \mod \delta$$

$$\begin{aligned} -m_3 x z^{p-1} \quad +l_3 y z^{p-1} \quad &\equiv z^p \mod \delta \\ y^p \quad +x^p \quad &\equiv z^p \mod \theta_4 \\ (-x + k_3) z^{p-1} \quad +(y - k_3) z^{p-1} \quad &\equiv z^p \mod \theta_4 \end{aligned}$$

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \theta_4 \\ (y - k_3) z^{p-1} \quad +(-x + k_3) z^{p-1} \quad &\equiv z^p \mod \theta_4 \\ +l_3 y z^{p-1} \quad -m_3 x z^{p-1} \quad &\equiv z^p \mod \theta_4 \\ -l_3 y \quad +m_3 x \quad &\equiv -z \mod \theta_4 \end{aligned}$$

**Definition 18** $y - k_3 \equiv q_3 x \mod \delta$ , $-x + k_3 \equiv r_3 y \mod \delta$ , $q_3 r_3 \perp \delta$

$$\begin{aligned} l_3 y \quad &\equiv q_3 x \mod \delta \\ -m_3 x \quad &\equiv r_3 y \mod \delta \end{aligned}$$

$$q_3 x + r_3 y \equiv z \mod \delta$$

$$\begin{aligned} x^p \quad +q_3^{-1} r_3 y x^{p-1} \quad &\equiv q_3^{-1} z x^{p-1} \mod \delta \\ q_3 r_3^{-1} x y^{p-1} \quad +y^p \quad &\equiv r_3^{-1} z y^{p-1} \mod \delta \\ q_3 x z^{p-1} \quad +r_3 y z^{p-1} \quad &\equiv z^p \mod \delta \end{aligned} \tag{82}$$

### 1.7.5 Common to $q_3^{-1} x^{p-1} \not\equiv r_3^{-1} y^{p-1} \not\equiv z^{p-1} \mod \delta$

(82) より

$$\begin{aligned} q_3^{-1} r_3 y x^{p-1} \cdot q_3^{-1} z x^{p-1} \quad &\equiv y^p z^p \mod \delta \\ q_3^{-2} r_3 \left(x^{p-1}\right)^2 \quad &\equiv y^{p-1} z^{p-1} \mod \delta \\ \left(q_3^{-1} x^{p-1}\right)^2 \quad &\equiv r_3^{-1} y^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{83}$$

$$\begin{aligned} q_3 r_3^{-1} x y^{p-1} \cdot r_3^{-1} z y^{p-1} \quad &\equiv x^p z^p \mod \delta \\ q_3 r_3^{-2} \left(y^{p-1}\right)^2 \quad &\equiv x^{p-1} z^{p-1} \mod \delta \\ \left(r_3^{-1} y^{p-1}\right)^2 \quad &\equiv q_3^{-1} x^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{84}$$

$$\begin{aligned} q_3 x z^{p-1} \cdot r_3 y z^{p-1} \quad &\equiv x^p y^p \mod \delta \\ q_3 r_3 \left(z^{p-1}\right)^2 \quad &\equiv x^{p-1} y^{p-1} \mod \delta \\ \left(z^{p-1}\right)^2 \quad &\equiv q_3^{-1} r_3^{-1} x^{p-1} y^{p-1} \mod \delta \end{aligned} \tag{85}$$

(83)(84)(85) より

$$\left(q_3^{-1}x^{p-1}\right)^3 \equiv \left(r_3^{-1}y^{p-1}\right)^3 \equiv \left(z^{p-1}\right)^3 \mod \delta$$

$$\left(z^{p-1}\right)^3-\left(r_3^{-1}y^{p-1}\right)^3 \equiv (z^{p-1}-r_3^{-1}y^{p-1})((z^{p-1})^2+r_3^{-1}y^{p-1}z^{p-1}+(r_3^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(q_3^{-1}x^{p-1}\right)^3-\left(z^{p-1}\right)^3 \equiv (q_3^{-1}x^{p-1}-z^{p-1})((q_3^{-1}x^{p-1})^2+q_3^{-1}x^{p-1}z^{p-1}+(z^{p-1})^2) \equiv 0 \mod \delta$$

$$\left(q_3^{-1}x^{p-1}\right)^3-\left(r_3^{-1}y^{p-1}\right)^3 \equiv (q_3^{-1}x^{p-1}-r_3^{-1}y^{p-1})((q_3^{-1}x^{p-1})^2+q_3^{-1}r_3^{-1}x^{p-1}y^{p-1}+(r_3^{-1}y^{p-1})^2) \equiv 0 \mod \delta$$

### 1.7.6 $z^{p-1} \not\equiv q_3^{-1}x^{p-1} \not\equiv r_3^{-1}y^{p-1} \mod \delta$ のとき

(83)(84) より

$$\begin{aligned}
(r_3^{-1}y^{p-1})^2 + (q_3^{-1}x^{p-1})^2 + (z^{p-1})^2 &\equiv 0 \mod \theta_1 \\
q_3^{-1}x^{p-1}z^{p-1} + r_3^{-1}y^{p-1}z^{p-1} + (z^{p-1})^2 &\equiv 0 \mod \theta_1 \\
q_3^{-1}x^{p-1} + r_3^{-1}y^{p-1} + z^{p-1} &\equiv 0 \mod \theta_1 \\
q_3^{-1}x^{p-1} + r_3^{-1}y^{p-1} &\equiv -z^{p-1} \mod \theta_1
\end{aligned}$$

【General solution conditions】

$$\begin{array}{rcl}
x^p \quad +q_3r_3^{-1}y^{p-1}x & \equiv -q_3z^{p-1}x \mod \theta_1 \\
q_3^{-1}r_3x^{p-1}y \quad +y^p & \equiv -r_3z^{p-1}y \mod \theta_1 \\
-q_3^{-1}x^{p-1}z \quad -r_3^{-1}y^{p-1}z & \equiv z^p \mod \theta_1
\end{array} \tag{86}$$

(86) より

$$\begin{aligned}
q_3r_3^{-1}y^{p-1}x \cdot -q_3z^{p-1}x &\equiv y^pz^p \mod \theta_1 \\
x^2 &\equiv -q_3^{-2}r_3yz \mod \theta_1
\end{aligned} \tag{87}$$

$$\begin{aligned}
q_3^{-1}r_3x^{p-1}y \cdot -r_3z^{p-1}y &\equiv x^pz^p \mod \theta_1 \\
y^2 &\equiv -q_3r_3^{-2}xz \mod \theta_1
\end{aligned} \tag{88}$$

$$\begin{aligned}
-q_3^{-1}x^{p-1}z \cdot -r_3^{-1}y^{p-1}z &\equiv x^py^p \mod \theta_1 \\
z^2 &\equiv q_3r_3xy \mod \theta_1
\end{aligned} \tag{89}$$

$$
\begin{aligned}
\text{(83) より } \left(x^{p-1}\right)^2 &\equiv q_3^2 r_3^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
\left(x^2\right)^{p-1} &\equiv q_3^2 r_3^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
\text{(87) より } \left(-q_3^{-2} r_3 yz\right)^{p-1} &\equiv q_3^2 r_3^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
q_3^{-2p+2} r_3^{p-1} y^{p-1} z^{p-1} &\equiv q_3^2 r_3^{-1} y^{p-1} z^{p-1} \mod \theta_1 \\
q_3^{-2p} r_3^p &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
\text{(84) より } \left(y^{p-1}\right)^2 &\equiv q_3^{-1} r_3^2 x^{p-1} z^{p-1} \mod \theta_1 \\
\left(y^2\right)^{p-1} &\equiv q_3^{-1} r_3^2 x^{p-1} z^{p-1} \mod \theta_1 \\
\text{(88) より } \left(-q_3 r_3^{-2} xz\right)^{p-1} &\equiv q_3^{-1} r_3^2 x^{p-1} z^{p-1} \mod \theta_1 \\
q_3^{p-1} r_3^{-2p+2} x^{p-1} z^{p-1} &\equiv q_3^{-1} r_3^2 x^{p-1} z^{p-1} \mod \theta_1 \\
q_3^p r_3^{-2p} &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
\text{(85) より } \left(z^{p-1}\right)^2 &\equiv q_3^{-1} r_3^{-1} x^{p-1} y^{p-1} \mod \theta_1 \\
\left(z^2\right)^{p-1} &\equiv q_3^{-1} r_3^{-1} x^{p-1} y^{p-1} \mod \theta_1 \\
\text{(89) より } (q_3 r_3 xy)^{p-1} &\equiv q_3^{-1} r_3^{-1} x^{p-1} y^{p-1} \mod \theta_1 \\
q_3^{p-1} r_3^{p-1} x^{p-1} y^{p-1} &\equiv q_3^{-1} r_3^{-1} x^{p-1} y^{p-1} \mod \theta_1 \\
q_3^p r_3^p &\equiv 1 \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
q_3^p r_3^p &\equiv 1 \mod \theta_1 \\
q_3^{-2p} r_3^p &\equiv 1 \mod \theta_1 \\
q_3^p r_3^{-2p} &\equiv 1 \mod \theta_1
\end{aligned}
$$

(60)(71)(82) より

$$
\begin{aligned}
r_1^{-1} xz^{p-1} &\equiv q_3 xz^{p-1} \mod \delta \\
r_1^{-1} &\equiv q_3 \mod \delta \\
1 &\equiv q_3^p r_1^p \mod \delta
\end{aligned} \tag{90}
$$

$$
\begin{aligned}
r_3^{-1} zy^{p-1} &\equiv r_2 zy^{p-1} \mod \delta \\
r_3^{-1} &\equiv r_2 \mod \delta
\end{aligned} \tag{91}
$$

(70) より

$$
q_3^p \equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \tag{92}
$$

$$
r_3^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \tag{93}
$$

### 1.7.7 A splice

(65) より

$$\begin{aligned} x^2 &\equiv -q_1 r_1 yz \mod \theta_1 \\ -x^2 &\equiv q_1 y \cdot r_1 z \mod \theta_1 \\ -x^2 &\equiv (z-k_1)(y-k_1) \mod \theta_1 \\ -x^2 &\equiv yz-(y+z)k_1+k_1^2 \mod \theta_1 \\ 0 &\equiv k_1^2-(y+z)k_1+yz+x^2 \mod \theta_1 \end{aligned}$$

$$\begin{aligned} k_1 &\equiv \frac{y+z\pm\sqrt{(y+z)^2-4(yz+x^2)}}{2} \mod \theta_1 \\ k_1 &\equiv \frac{y+z\pm\sqrt{(y-z)^2-4x^2}}{2} \mod \theta_1 \\ k_1 &\equiv \frac{y+z\pm\sqrt{x^2-4x^2}}{2} \mod \theta_1 \\ k_1 &\equiv \frac{y+z\pm\sqrt{-3x^2}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -y+k_1 &\equiv \frac{-y+z\pm\sqrt{-3x^2}}{2} \mod \theta_1 \\ -z+k_1 &\equiv \frac{y-z\pm\sqrt{-3x^2}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -r_1 z &\equiv x\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_1 \\ -q_1 y &\equiv x\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -r_1 z x^{p-1} &\equiv x^p\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_1 \\ -q_1 y x^{p-1} &\equiv x^p\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} y^p &\equiv x^p\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_1 \\ z^p &\equiv x^p\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{aligned} \tag{94}$$

$$
\begin{aligned}
-z &\equiv xr_1^{-1} \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
-y &\equiv xq_1^{-1} \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

(90)(79) より

$$
\begin{aligned}
-z &\equiv xq_3 \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
-y &\equiv xq_2 \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
-z^p &\equiv x^p q_3^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1 \\
-y^p &\equiv x^p q_2^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1
\end{aligned}
$$

(94) より

$$
\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv q_3^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1 \\
\frac{1 \mp \sqrt{-3}}{2} &\equiv q_2^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1
\end{aligned}
$$

(92)(80) より

$$
\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \pm \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_1 \\
\frac{1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \mp \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_1
\end{aligned}
$$

$q_1^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1$ のとき

$$
\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \mp \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_1 \\
\frac{1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \pm \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_1
\end{aligned}
$$

(77) より

$$\begin{aligned} y^2 &\equiv -q_2 r_2 xz \mod \theta_1 \\ -y^2 &\equiv q_2 x \cdot r_2 z \mod \theta_1 \\ -y^2 &\equiv (-z+k_2)(x+k_2) \mod \theta_1 \\ -y^2 &\equiv -xz + (x-z)k_2 + k_2^2 \mod \theta_1 \\ 0 &\equiv k_2^2 + (x-z)k_2 - xz + y^2 \mod \theta_1 \end{aligned}$$

$$\begin{aligned} k_2 &\equiv \frac{z-x \pm \sqrt{(x-z)^2 - 4(-xz+y^2)}}{2} \mod \theta_1 \\ k_2 &\equiv \frac{z-x \pm \sqrt{(x+z)^2 - 4y^2}}{2} \mod \theta_1 \\ k_2 &\equiv \frac{z-x \pm \sqrt{y^2 - 4y^2}}{2} \mod \theta_1 \\ k_2 &\equiv \frac{z-x \pm \sqrt{-3y^2}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} x+k_2 &\equiv \frac{z+x \pm \sqrt{-3y^2}}{2} \mod \theta_1 \\ -z+k_2 &\equiv \frac{-z-x \pm \sqrt{-3y^2}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} r_2 z &\equiv y \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1 \\ q_2 x &\equiv y \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} r_2 z y^{p-1} &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1 \\ q_2 x y^{p-1} &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -x^p &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1 \\ -z^p &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \end{aligned} \tag{95}$$

$$
\begin{aligned}
z &\equiv yr_2^{-1} \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
x &\equiv yq_2^{-1} \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

(91)(79) より

$$
\begin{aligned}
z &\equiv yr_3 \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
x &\equiv yq_1 \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
z^p &\equiv y^p r_3^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1 \\
x^p &\equiv y^p q_1^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1
\end{aligned}
$$

(95) より

$$
\begin{aligned}
\frac{1 \mp \sqrt{-3}}{2} &\equiv r_3^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1 \\
\frac{-1 \mp \sqrt{-3}}{2} &\equiv q_1^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_1
\end{aligned}
$$

(93)(69) より

$$
\begin{aligned}
\frac{1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{-1 \mp \sqrt{-3}}{2}\right) \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_1 \\
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{-1 \pm \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_1
\end{aligned}
$$

$q_1^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1$ のとき

$$
\begin{aligned}
\frac{1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{-1 \pm \sqrt{-3}}{2}\right) \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_1 \\
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{-1 \mp \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_1
\end{aligned}
$$

(89) より

$$\begin{aligned} z^2 &\equiv q_3 r_3 xy \mod \theta_1 \\ -z^2 &\equiv -q_3 x \cdot r_3 y \mod \theta_1 \\ -z^2 &\equiv (-y+k_3)(-x+k_3) \mod \theta_1 \\ -z^2 &\equiv xy-(x+y)k_3+k_3^2 \mod \theta_1 \\ 0 &\equiv k_3^2-(x+y)k_3+xy+z^2 \mod \theta_1 \end{aligned}$$

$$\begin{aligned} k_3 &\equiv \frac{x+y\pm\sqrt{(x+y)^2-4(xy+z^2)}}{2} \mod \theta_1 \\ k_3 &\equiv \frac{x+y\pm\sqrt{(x-y)^2-4z^2}}{2} \mod \theta_1 \\ k_3 &\equiv \frac{x+y\pm\sqrt{z^2-4z^2}}{2} \mod \theta_1 \\ k_3 &\equiv \frac{x+y\pm\sqrt{-3z^2}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -y+k_3 &\equiv \frac{-y+x\pm\sqrt{-3z^2}}{2} \mod \theta_1 \\ -x+k_3 &\equiv \frac{y-x\pm\sqrt{-3z^2}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -q_3 x &\equiv z\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_1 \\ r_3 y &\equiv z\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{aligned}$$

$$\begin{aligned} -q_3 x z^{p-1} &\equiv z^p\cdot\frac{-1\pm\sqrt{-3}}{2} \mod \theta_1 \\ r_3 y z^{p-1} &\equiv z^p\cdot\frac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{aligned}$$

(94) より $\pm$ の調整

$$\begin{aligned} -y^p &\equiv z^p\cdot\frac{-1\mp\sqrt{-3}}{2} \mod \theta_1 \\ x^p &\equiv z^p\cdot\frac{1\mp\sqrt{-3}}{2} \mod \theta_1 \end{aligned} \tag{96}$$

$$
\begin{aligned}
-x &\equiv q_3^{-1} z \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \\
y &\equiv r_3^{-1} z \cdot \frac{1 \mp \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

(90)(91) より

$$
\begin{aligned}
-x &\equiv r_1 z \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \\
y &\equiv r_2 z \cdot \frac{1 \mp \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
-x^p &\equiv z^p r_1^p \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^p \mod \theta_1 \\
y^p &\equiv z^p r_2^p \cdot \left( \frac{1 \mp \sqrt{-3}}{2} \right)^p \mod \theta_1
\end{aligned}
$$

(96) より

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv r_1^p \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^p \mod \theta_1 \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv r_2^p \cdot \left( \frac{1 \mp \sqrt{-3}}{2} \right)^p \mod \theta_1
\end{aligned}
$$

(70)(81) より

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{-1 \mp \sqrt{-3}}{2} \right) \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^{6n+1} \mod \theta_1 \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{-1 \pm \sqrt{-3}}{2} \right) \cdot \left( \frac{1 \mp \sqrt{-3}}{2} \right)^{6n+1} \mod \theta_1
\end{aligned}
$$

$q_1^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1$ のとき

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{-1 \pm \sqrt{-3}}{2} \right) \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^{6n+3} \mod \theta_1 \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{-1 \mp \sqrt{-3}}{2} \right) \cdot \left( \frac{1 \mp \sqrt{-3}}{2} \right)^{6n+3} \mod \theta_1
\end{aligned}
$$

### 1.7.8 $p = 6n + 1$ のとき

$$
\begin{aligned}
q_1^p \equiv q_1 &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
r_1^p \equiv r_1 &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \\
q_2^p \equiv q_2 &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1 \\
r_2^p \equiv r_2 &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
q_3^p \equiv q_3 &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_1 \\
r_3^p \equiv r_3 &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_1
\end{aligned}
$$

(65)(77)(89) より

$$
\begin{aligned}
x^2 &\equiv -q_1 r_1 yz \mod \theta_1 \\
x^2 &\equiv -yz \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
y^2 &\equiv -q_2 r_2 xz \mod \theta_1 \\
y^2 &\equiv -xz \mod \theta_1
\end{aligned}
$$

$$
\begin{aligned}
z^2 &\equiv q_3 r_3 xy \mod \theta_1 \\
z^2 &\equiv xy \mod \theta_1
\end{aligned}
$$

$$
-z^3 \equiv x^3 \equiv y^3 \mod \theta_1
$$

$$
\begin{aligned}
z^3 + y^3 &\equiv (z+y)(z^2 - yz + y^2) \equiv 0 \mod \theta_1 \\
x^3 + z^3 &\equiv (x+z)(x^2 - xz + z^2) \equiv 0 \mod \theta_1 \\
x^3 - y^3 &\equiv (x-y)(x^2 + xy + y^2) \equiv 0 \mod \theta_1
\end{aligned}
$$

$x + z - y \equiv 0 \mod \theta_1$ なので

$$
x + z \not\equiv 0 \mod \theta_1
$$

$$
\begin{aligned}
x^2 - xz + z^2 &\equiv 0 \mod \theta_1 \\
x^2 - xz + xy &\equiv 0 \mod \theta_1 \\
x - z + y &\not\equiv 0 \mod \theta_1
\end{aligned}
$$

よって $p = 6n + 1$ は満たさない。

### 1.7.9 $p = 6n + 3$ のとき

$p$ は素数なので $n = 0$ ， $p = 3$、$x^3 + y^3 \equiv z^3 \mod \theta_1$

$$
\begin{aligned}
(x + z - y)^3 &\equiv x^3 + z^3 - y^3 - 3x^2y + 3x^2z + 3xy^2 + 3xz^2 + 3y^2z - 3yz^2 - 6xyz \mod \theta_1 \\
(x + z - y)^3 &\equiv 2x^3 + 3(-x^2y + x^2z + xy^2 + xz^2 + y^2z - yz^2 - 2xyz) \mod \theta_1 \\
(x + z - y)^3 &\equiv 2x^3 + 3(-y(x^2 + 2xz + z^2) + (x + z)xz + (x + z)y^2) \mod \theta_1 \\
(x + z - y)^3 &\equiv 2x^3 + 3(-y(x + z)^2 + (x + z)xz + (x + z)y^2) \mod \theta_1 \\
(x + z - y)^3 &\equiv 2x^3 + 3(x + z)(-xy - yz + xz + y^2) \mod \theta_1 \\
(x + z - y)^3 &\equiv 2x^3 + 3(x + z)(-x(y - z) + y(y - z)) \mod \theta_1 \\
(x + z - y)^3 &\equiv 2x^3 + 3(x + z)(y - z)(y - x) \mod \theta_1 \\
0 &\equiv 2x^3 + 3yxz \mod \theta_1 \\
-2x^2 &\equiv 3yz \mod \theta_1
\end{aligned}
$$

(65) より

$$
\begin{aligned}
2q_1r_1yz &\equiv 3yz \mod \theta_1 \\
2q_1r_1 &\equiv 3 \mod \theta_1 \\
2^p q_1^p r_1^p &\equiv 3^p \mod \theta_1
\end{aligned}
$$

(68) より

$$
\begin{aligned}
2^3 &\equiv 3^3 \mod \theta_1 \\
8 &\equiv 27 \mod \theta_1 \\
0 &\equiv 19 \mod \theta_1
\end{aligned}
$$

これは $0 \equiv 19 \mod \theta_4$ ともに成り立つと (15) に矛盾する。ともに成り立たない場合もまた矛盾する。

### 1.7.10 Complement 1(補足 1)

Fermat's little theorem より

$$
\begin{aligned}
1 &\equiv 2^{19-1} \mod 19 \\
2^{-1} &\equiv 2^{19-2} \mod 19 \\
2^{-1} &\equiv 2^{17} \mod 19 \\
2^{-1} &\equiv 10
\end{aligned}
$$

$$
\begin{aligned}
\sqrt{-3} &\equiv \sqrt{19 - 3} \mod 19 \\
\sqrt{-3} &\equiv \sqrt{16} \mod 19 \\
\sqrt{-3} &\equiv 4 \mod 19
\end{aligned}
$$

### 1.7.11 Complement 2(補足 2)

**Proposition 19** $\left(x^{p-1}\right)^2 \equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_4 \Rightarrow$
$\left(l_1^{-1}y^{p-1}\right)^2 \equiv -m_1^{-1}x^{p-1}z^{p-1} \mod \theta_4$ , $\left(m_1^{-1}z^{p-1}\right)^2 \equiv -l_1^{-1}x^{p-1}y^{p-1} \mod \theta_4$

**Proof 20** $q_1$ , $r_1$ が合同式を満たす変数とするとき、(97)(98) の各項は同値な仮定ができる。

$$\begin{array}{rrrl} x^p & +m_1zx^{p-1} & \equiv l_1yx^{p-1} & \mod \theta_1 \\ -l_1^{-1}m_1zy^{p-1} & +y^p & \equiv l_1^{-1}xy^{p-1} & \mod \theta_1 \\ l_1m_1^{-1}yz^{p-1} & -m_1^{-1}xz^{p-1} & \equiv z^p & \mod \theta_1 \end{array} \tag{97}$$

$$\begin{array}{rrrl} x^p & +q_1yx^{p-1} & \equiv r_1zx^{p-1} & \mod \theta_1 \\ q_1^{-1}xy^{p-1} & +y^p & \equiv q_1^{-1}r_1zy^{p-1} & \mod \theta_1 \\ r_1^{-1}xz^{p-1} & +q_1r_1^{-1}yz^{p-1} & \equiv z^p & \mod \theta_1 \end{array} \tag{98}$$

よって $\left(x^{p-1}\right)^2 \equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_1 \Rightarrow$
$\left(l_1^{-1}y^{p-1}\right)^2 \equiv -m_1^{-1}x^{p-1}z^{p-1} \mod \theta_1$ , $\left(m_1^{-1}z^{p-1}\right)^2 \equiv -l_1^{-1}x^{p-1}y^{p-1} \mod \theta_1$

であるから (62)(63) および (94) を導出できる。(95)(96) もまた同様である。
ただし $x^p, y^p, z^p, \theta_1$ は共通なので符号の整合性がなければならない。

$$\begin{array}{rcl} x+q_1y & \equiv & r_1z \mod \theta_1 \\ x+x\cdot\dfrac{-1\mp\sqrt{-3}}{2} & \equiv & x\cdot\dfrac{1\mp\sqrt{-3}}{2} \mod \theta_1 \end{array} \tag{99}$$

$$\begin{array}{rcl} q_2x+y & \equiv & r_2z \mod \theta_1 \\ y\cdot\dfrac{-1\pm\sqrt{-3}}{2}+y & \equiv & y\cdot\dfrac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{array} \tag{100}$$

(99) の両辺に $x^{-1}y\cdot\frac{-1\pm\sqrt{-3}}{2}$ をかけると

$$\begin{array}{rcl} q_1^{-1}x+y & \equiv & q_1^{-1}r_1z \mod \theta_1 \\ y\cdot\dfrac{-1\pm\sqrt{-3}}{2}+y & \equiv & y\cdot\dfrac{1\pm\sqrt{-3}}{2} \mod \theta_1 \end{array} \tag{101}$$

(99) の両辺に $x^{-1}z\cdot\frac{1\pm\sqrt{-3}}{2}$ をかけると

$$\begin{array}{rcl} r_1^{-1}x+q_1r_1^{-1}y & \equiv & z \mod \theta_1 \\ z\cdot\dfrac{1\pm\sqrt{-3}}{2}+z\cdot\dfrac{1\mp\sqrt{-3}}{2} & \equiv & z \mod \theta_1 \end{array} \tag{102}$$

(100) の両辺に $y^{-1}z\cdot\frac{1\mp\sqrt{-3}}{2}$ をかけると

$$\begin{array}{rcl} q_2r_2^{-1}x+r_2^{-1}y & \equiv & z \mod \theta_1 \\ z\cdot\dfrac{1\pm\sqrt{-3}}{2}+z\cdot\dfrac{1\mp\sqrt{-3}}{2} & \equiv & z \mod \theta_1 \end{array} \tag{103}$$

以下の式は $\pm$ の調整している。

$$\begin{aligned} q_3x + r_3y &\equiv z \mod \theta_1 \\ z \cdot \frac{1 \pm \sqrt{-3}}{2} + z \cdot \frac{1 \mp \sqrt{-3}}{2} &\equiv z \mod \theta_1 \end{aligned} \tag{104}$$

(100)(101) より

$$q_1^{-1}x \equiv q_2x \mod \theta_1$$

(102)(104) より

$$r_1^{-1}x \equiv q_3x \mod \theta_1$$

(103)(104) より

$$r_2^{-1}y \equiv r_3y \mod \theta_1$$

よって以下の式の各項は (98) と同値であることが示された。

$$\begin{aligned} x^p &+q_1yx^{p-1} &&\equiv r_1zx^{p-1} \mod \theta_1 \\ q_2xy^{p-1} &+y^p &&\equiv r_2zy^{p-1} \mod \theta_1 \\ q_3xz^{p-1} &+r_3yz^{p-1} &&\equiv z^p \mod \theta_1 \end{aligned}$$

また $q_1$ ， $q_2$ は $\theta_1$ と $\theta_4$ の共通の代数である。

$$\begin{aligned} q_1 &\equiv m_1zy^{-1} \mod \theta_1 \\ q_1 &\equiv m_1zy^{-1} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} q_2 &\equiv -m_2zx^{-1} \mod \theta_1 \\ q_2 &\equiv -m_2zx^{-1} \mod \theta_4 \end{aligned}$$

$$\begin{aligned} q_2xy^{p-1} &\equiv q_1^{-1}xy^{p-1} \mod \theta_1 \\ &\Rightarrow \\ q_2xy^{p-1} &\equiv q_1^{-1}xy^{p-1} \mod \theta_4 \end{aligned}$$

以上より

$\left(x^{p-1}\right)^2 \equiv q_1^{-1}r_1^{-1}y^{p-1}z^{p-1} \mod \theta_4 \Rightarrow x^{p-1} \equiv q_1^{-1}y^{p-1} \equiv r_1^{-1}z^{p-1} \mod \theta_4$
なので

$\left(q_1^{-1}y^{p-1}\right)^2 \equiv r_1^{-1}x^{p-1}z^{p-1} \mod \theta_4$ ， $\left(r_1^{-1}z^{p-1}\right)^2 \equiv q_1^{-1}x^{p-1}y^{p-1} \mod \theta_4$
ゆえに

$\left(x^{p-1}\right)^2 \equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \mod \theta_4 \Rightarrow$
$\left(l_1^{-1}y^{p-1}\right)^2 \equiv -m_1^{-1}x^{p-1}z^{p-1} \mod \theta_4$ ， $\left(m_1^{-1}z^{p-1}\right)^2 \equiv -l_1^{-1}x^{p-1}y^{p-1} \mod \theta_4$

□

## 1.8 $\delta = 2$ のとき

### 1.8.1 $2 \mid x$ , $2 \perp yz$

$S = 2^k$ のとき

$$x + z - y = p^n a 2^k$$

$$x^p = z^p - y^p = (z - y)(py^{p-1} + (z - y)(\ldots))$$

$$\begin{aligned} 2 \mid L &= p^{np-1} a^p \\ 2 \mid a & \end{aligned}$$

$$\begin{aligned} 2 \perp R &= p\alpha^p \\ 2 \perp \alpha & \end{aligned}$$

$$\begin{aligned} x + z - y &= p^n a(\alpha + p^{(p-1)n-1} a^{p-1}) \\ 2^k &= \alpha + p^{(p-1)n-1} a^{p-1} = odd \\ 2^0 &= 1 \end{aligned}$$

しかし、$\alpha + p^{(p-1)n-1} a^{p-1} > 1$ なので矛盾する。

$S' = 2^k$ のとき

$$x + z - y = a' 2^k$$

$$x^p = z^p - y^p = (z - y)(py^{p-1} + (z - y)(\ldots))$$

$$\begin{aligned} 2 \mid L &= a'^p \\ 2 \mid a' & \end{aligned}$$

$$\begin{aligned} 2 \perp R &= \alpha'^p \\ 2 \perp \alpha' & \end{aligned}$$

$$\begin{aligned} x + z - y &= a'(\alpha' + a'^{p-1}) \\ 2^k &= \alpha' + a'^{p-1} = odd \\ 2^0 &= 1 \end{aligned}$$

しかし、$\alpha' + a'^{p-1} > 1$ なので矛盾する。

よって $2 \mid x$ のとき成り立たない。

## 1.9 $\delta' \perp xyz$ の導出

### 1.9.1 $p \mid z$ のとき ( 諸条件は省略 )

$$x = a\alpha \qquad y = b\beta \qquad z = p^n c\gamma$$
$$z - y = a^p \qquad z - x = b^p \qquad x + y = p^{np-1}c^p$$
$$p \perp xyc\gamma \qquad \delta' = \text{奇素数 (definition)}$$

**Proposition 21** $z + x + y = p^n cS$" , $\delta' \mid S$" $\Rightarrow$ $\delta' \perp xyz$

**Proof 22**

$$\begin{aligned} z + x + y &= p^n c\gamma + p^{np-1}c^p \\ &= p^n c(\gamma + p^{(p-1)n-1}c^{p-1}) \\ p \perp S" \quad &, \quad p \perp \delta' \\ p\gamma^p = R &= py^{p-1} + (x+y)(\ldots) \\ R &\equiv py^{p-1} \mod c \\ py^{p-1} &\perp c \\ \gamma &\perp c \end{aligned}$$

$\delta' \mid S$" のとき $\delta' \mid c$ または $\delta' \mid \gamma$ ならば上記と矛盾するので

$$\delta' \perp z$$

$$\begin{aligned} 2z &= -(x+y-z) + (z+x+y) \\ ab &\mid x+y-z \\ z &\perp ab \end{aligned}$$

$\delta' \mid ab$ ならば $\delta' \mid 2z$ でなければならず矛盾するので

$$\delta' \perp ab$$

$\delta' \mid \beta$ ならば $\delta' \mid z + x$

$$\begin{aligned} z &\equiv -x \mod \delta' \\ z^p &\equiv -x^p \mod \delta' \\ z^p + x^p &\equiv 0 \mod \delta' \end{aligned}$$

$z^p - x^p = y^p \equiv 0 \mod \delta'$ なので

$$\begin{aligned} z^p + x^p + (z^p - x^p) &\equiv 0 \mod \delta' \\ 2z^p &\not\equiv 0 \mod \delta' \end{aligned}$$

よって $\delta' \perp \beta$

$\delta' \mid \alpha$ , $\delta' \mid z + y$ ならば同様に

$$\begin{aligned} z^p + y^p + (z^p - y^p) &\equiv 0 \mod \delta' \\ 2z^p &\not\equiv 0 \mod \delta' \end{aligned}$$

よって $\delta' \perp \alpha$ □

$x+y+k_1' \equiv -z+k_1' \mod \delta'$ より

**Definition 23** $y+k_1' \equiv l_1' y \mod \delta' \quad , \ -z+k_1' \equiv -m_1' z \mod \delta' \quad , \ l_1' m_1' \perp \delta'$

$$l_1' y x^{p-1} \cdot -m_1' z x^{p-1} \equiv y^p z^p \mod \delta'$$

$x+l_1' y \equiv -m_1' z \mod \delta'$ より

$$\begin{array}{ccc} x^p & +l_1' y x^{p-1} & \equiv -m_1' z x^{p-1} \mod \delta' \\ l_1'^{-1} x y^{p-1} & +y^p & \equiv -l_1'^{-1} m_1' z y^{p-1} \mod \delta' \\ -m_1'^{-1} x z^{p-1} & -l_1' m_1'^{-1} y z^{p-1} & \equiv z^p \mod \delta' \end{array} \tag{105}$$

ここで

$$l_1' y x^{p-1} \equiv y^p \mod \delta' \Rightarrow -m_1' z x^{p-1} \equiv z^p \mod \delta'$$
$$x^{p-1} \equiv l_1'^{-1} y^{p-1} \mod \delta' \Rightarrow x^{p-1} \equiv -m_1'^{-1} z^{p-1} \mod \delta'$$

であるから自動的に

$$l_1'^{-1} x y^{p-1} \equiv x^p \mod \delta' \quad , \ -l_1'^{-1} m_1' z y^{p-1} \equiv z^p \mod \delta'$$
$$-m_1'^{-1} x z^{p-1} \equiv x^p \mod \delta' \quad , \ -l_1' m_1'^{-1} y z^{p-1} \equiv y^p \mod \delta'$$

よって $x^p+y^p \equiv z^p \mod \delta'$ が成り立つ条件は

$$\begin{array}{c} x^{p-1} \equiv l_1'^{-1} y^{p-1} \equiv -m_1'^{-1} z^{p-1} \mod \delta' \\ or \\ x^{p-1} \not\equiv l_1'^{-1} y^{p-1} \not\equiv -m_1'^{-1} z^{p-1} \mod \delta' \end{array}$$

### 1.9.2 Common to $x^{p-1} \not\equiv l_1'^{-1} y^{p-1} \not\equiv -m_1'^{-1} z^{p-1} \mod \delta'$

(105) より

$$\begin{array}{cc} l_1' y x^{p-1} \cdot -m_1' z x^{p-1} & \equiv y^p z^p \mod \delta' \\ l_1' m_1' \left(x^{p-1}\right)^2 & \equiv -y^{p-1} z^{p-1} \mod \delta' \\ \left(x^{p-1}\right)^2 & \equiv -l_1'^{-1} m_1'^{-1} y^{p-1} z^{p-1} \mod \delta' \end{array} \tag{106}$$

$$\begin{array}{cc} l_1'^{-1} x y^{p-1} \cdot -l_1'^{-1} m_1' z y^{p-1} & \equiv x^p z^p \mod \delta' \\ l_1'^{-2} m_1' \left(y^{p-1}\right)^2 & \equiv -x^{p-1} z^{p-1} \mod \delta' \\ \left(l_1'^{-1} y^{p-1}\right)^2 & \equiv -m_1'^{-1} x^{p-1} z^{p-1} \mod \delta' \end{array} \tag{107}$$

$$\begin{array}{cc} -m_1'^{-1} x z^{p-1} \cdot -l_1' m_1'^{-1} y z^{p-1} & \equiv x^p y^p \mod \delta' \\ l_1' m_1'^{-2} \left(z^{p-1}\right)^2 & \equiv x^{p-1} y^{p-1} \mod \delta' \\ \left(m_1'^{-1} z^{p-1}\right)^2 & \equiv l_1'^{-1} x^{p-1} y^{p-1} \mod \delta' \end{array} \tag{108}$$

(106)(107)(108) より

$$\left(x^{p-1}\right)^3 \equiv \left(l_1'^{-1}y^{p-1}\right)^3 \equiv -\left(m_1'^{-1}z^{p-1}\right)^3 \mod \delta'$$

$\left(m_1'^{-1}z^{p-1}\right)^3+\left(l_1'^{-1}y^{p-1}\right)^3 \equiv (m_1'^{-1}z^{p-1}+l_1'^{-1}y^{p-1})((m_1'^{-1}z^{p-1})^2-l_1'^{-1}m_1'^{-1}y^{p-1}z^{p-1}+(l_1'^{-1}y^{p-1})^2) \equiv 0 \mod$

$\left(x^{p-1}\right)^3+\left(m_1'^{-1}z^{p-1}\right)^3 \equiv (x^{p-1}+m_1'^{-1}z^{p-1})((x^{p-1})^2-m_1'^{-1}x^{p-1}z^{p-1}+(m_1'^{-1}z^{p-1})^2) \equiv 0 \mod \delta'$

$\left(x^{p-1}\right)^3-\left(l_1'^{-1}y^{p-1}\right)^3 \equiv (x^{p-1}-l_1'^{-1}y^{p-1})((x^{p-1})^2+l_1'^{-1}x^{p-1}y^{p-1}+(l_1'^{-1}y^{p-1})^2) \equiv 0 \mod \delta'$

### 1.9.3 $x^{p-1} \not\equiv l_1'^{-1}y^{p-1} \not\equiv -m_1'^{-1}z^{p-1} \mod \delta'$ のとき

(107)(108) より

$$\begin{aligned}
(x^{p-1})^2 + (m_1'^{-1}z^{p-1})^2 + (l_1'^{-1}y^{p-1})^2 &\equiv 0 \mod \theta_4' \\
(x^{p-1})^2 + l_1'^{-1}x^{p-1}y^{p-1} - m_1'^{-1}x^{p-1}z^{p-1} &\equiv 0 \mod \theta_4' \\
x^{p-1} + l_1'^{-1}y^{p-1} - m_1'^{-1}z^{p-1} &\equiv 0 \mod \theta_4' \\
x^{p-1} + l_1'^{-1}y^{p-1} &\equiv m_1'^{-1}z^{p-1} \mod \theta_4'
\end{aligned}$$

【General solution conditions】

$$\begin{array}{rrl}
x^p & +l_1'^{-1}y^{p-1}x & \equiv m_1'^{-1}z^{p-1}x \mod \theta_4' \\
l_1'x^{p-1}y & +y^p & \equiv l_1'm_1'^{-1}z^{p-1}y \mod \theta_4' \\
m_1'x^{p-1}z & +l_1'^{-1}m_1'y^{p-1}z & \equiv z^p \mod \theta_4'
\end{array} \tag{109}$$

(109) より

$$\begin{aligned}
l_1'^{-1}y^{p-1}x \cdot m_1'^{-1}z^{p-1}x &\equiv y^pz^p \mod \theta_4' \\
x^2 &\equiv l_1'm_1'yz \mod \theta_4'
\end{aligned} \tag{110}$$

$$\begin{aligned}
l_1'x^{p-1}y \cdot l_1'm_1'^{-1}z^{p-1}y &\equiv x^pz^p \mod \theta_4' \\
y^2 &\equiv l_1'^{-2}m_1'xz \mod \theta_4'
\end{aligned} \tag{111}$$

$$\begin{aligned}
m_1'x^{p-1}z \cdot l_1'^{-1}m_1'y^{p-1}z &\equiv x^py^p \mod \theta_4' \\
z^2 &\equiv l_1'm_1'^{-2}xy \mod \theta_4'
\end{aligned} \tag{112}$$

$$
\begin{aligned}
\text{(106) より } \left(x^{p-1}\right)^2 &\equiv -l_1'^{-1}m_1'^{-1}y^{p-1}z^{p-1} \mod \theta_4' \\
\left(x^2\right)^{p-1} &\equiv -l_1'^{-1}m_1'^{-1}y^{p-1}z^{p-1} \mod \theta_4' \\
\text{(110) より } \left(l_1'm_1'yz\right)^{p-1} &\equiv -l_1'^{-1}m_1'^{-1}y^{p-1}z^{p-1} \mod \theta_4' \\
l_1'^{p-1}m_1'^{p-1}y^{p-1}z^{p-1} &\equiv -l_1'^{-1}m_1'^{-1}y^{p-1}z^{p-1} \mod \theta_4' \\
l_1'^{p}m_1'^{p}y^{p-1}z^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta_4' \\
l_1'^{p}m_1'^{p} &\equiv -1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
\text{(107) より } \left(y^{p-1}\right)^2 &\equiv -l_1'^{2}m_1'^{-1}x^{p-1}z^{p-1} \mod \theta_4' \\
\left(y^2\right)^{p-1} &\equiv -l_1'^{2}m_1'^{-1}x^{p-1}z^{p-1} \mod \theta_4' \\
\text{(111) より } \left(l_1'^{-2}m_1'xz\right)^{p-1} &\equiv -l_1'^{2}m_1'^{-1}x^{p-1}z^{p-1} \mod \theta_4' \\
l_1'^{-2p+2}m_1'^{p-1}x^{p-1}z^{p-1} &\equiv -l_1'^{2}m_1'^{-1}x^{p-1}z^{p-1} \mod \theta_4' \\
l_1'^{-2p}m_1'^{p}x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_4' \\
l_1'^{-2p}m_1'^{p} &\equiv -1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
\text{(108) より } \left(z^{p-1}\right)^2 &\equiv l_1'^{-1}m_1'^{2}x^{p-1}y^{p-1} \mod \theta_4' \\
\left(z^2\right)^{p-1} &\equiv l_1'^{-1}m_1'^{2}x^{p-1}y^{p-1} \mod \theta_4' \\
\text{(112) より } \left(l_1'm_1'^{-2}xy\right)^{p-1} &\equiv l_1'^{-1}m_1'^{2}x^{p-1}y^{p-1} \mod \theta_4' \\
l_1'^{p-1}m_1'^{-2p+2}x^{p-1}y^{p-1} &\equiv l_1'^{-1}m_1'^{2}x^{p-1}y^{p-1} \mod \theta_4' \\
l_1'^{p}m_1'^{-2p}x^{p-1}y^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta_4' \\
l_1'^{p}m_1'^{-2p} &\equiv 1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
l_1'^p m_1'^p &\equiv -1 \mod \theta_4' \\
l_1'^{-2p} m_1'^p &\equiv -1 \mod \theta_4' \\
l_1'^p m_1'^{-2p} &\equiv 1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
-m_1'^{3p} &\equiv l_1'^{3p} \mod \theta_4' \\
m_1'^{3p} + l_1'^{3p} &\equiv (m_1'^p + l_1'^p)(m_1'^{2p} - l_1'^p m_1'^p + l_1'^{2p}) \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
-m_1'^p &\equiv l_1'^{2p} \mod \theta_4' \\
l_1'^p &\equiv m_1'^{2p} \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
l_1'^p + m_1'^p &\equiv m_1'^{2p} - l_1'^{2p} \mod \theta_4' \\
l_1'^p + m_1'^p &\equiv (m_1'^p + l_1'^p)(m_1'^p - l_1'^p) \mod \theta_4' \\
1 &\equiv m_1'^p - l_1'^p \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
(m_1'^p - l_1'^p)^2 &\equiv 1^2 \mod \theta_4' \\
l_1'^{2p} - 2l_1'^p m_1'^p + m_1'^{2p} &\equiv 1 \mod \theta_4' \\
l_1'^{2p} - 2l_1'^p m_1'^p + m_1'^{2p} &\equiv -l_1'^p m_1'^p \mod \theta_4' \\
l_1'^{2p} - l_1'^p m_1'^p + m_1'^{2p} &\equiv 0 \mod \theta_4'
\end{aligned}
$$

よって $m_1'^p + l_1'^p \not\equiv 0 \mod \theta_4'$

$$
\begin{aligned}
m_1'^p - l_1'^p &\equiv 1 \mod \theta_4' \\
l_1'^{2p} - l_1'^p m_1'^p &\equiv -l_1'^p \mod \theta_4' \\
l_1'^{2p} + l_1'^p + 1 &\equiv 0 \mod \theta_4'
\end{aligned}
$$

$l_1'^p m_1'^p \equiv -1 \mod \theta_4'$ なので

$$
l_1'^p \equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4' \tag{113}
$$

$$
m_1'^p \equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4' \tag{114}
$$

$x + k_2' + y \equiv -z + k_2' \mod \delta'$ より

**Definition 24** $x+k_2' \equiv l_2' x \mod \delta'$ , $-z+k_2' \equiv -m_2' z \mod \delta'$ , $l_2' m_2' \perp \delta'$

$$l_2' x y^{p-1} \cdot -m_2' z y^{p-1} \equiv x^p z^p \mod \delta'$$

$l_2' x + y \equiv -m_2' z \mod \delta'$ より

$$\begin{array}{rrl} x^p & +l_2'^{-1} y x^{p-1} & \equiv -l_2'^{-1} m_2' z x^{p-1} \mod \delta' \\ l_2' x y^{p-1} & +y^p & \equiv -m_2' z y^{p-1} \mod \delta' \\ -l_2' m_2'^{-1} x z^{p-1} & -m_2'^{-1} y z^{p-1} & \equiv z^p \mod \delta' \end{array} \tag{115}$$

ここで

$$l_2' x y^{p-1} \equiv x^p \mod \delta' \Rightarrow -m_2' z y^{p-1} \equiv z^p \mod \delta'$$
$$l_2' y^{p-1} \equiv x^{p-1} \mod \delta' \Rightarrow -m_2' y^{p-1} \equiv z^{p-1} \mod \delta'$$

であるから自動的に

$$l_2'^{-1} y x^{p-1} \equiv y^p \mod \delta' \quad , \quad -l_2'^{-1} m_2' z x^{p-1} \equiv z^p \mod \delta'$$
$$-l_2' m_2'^{-1} x z^{p-1} \equiv x^p \mod \delta' \quad , \quad -m_2'^{-1} y z^{p-1} \equiv y^p \mod \delta'$$

よって $x^p + y^p \equiv z^p \mod \delta'$ が成り立つ条件は

$$\begin{array}{c} l_2'^{-1} x^{p-1} \equiv y^{p-1} \equiv -m_2'^{-1} z^{p-1} \mod \delta' \\ or \\ l_2'^{-1} x^{p-1} \not\equiv y^{p-1} \not\equiv -m_2'^{-1} z^{p-1} \mod \delta' \end{array}$$

### 1.9.4 Common to $l_2'^{-1} x^{p-1} \not\equiv y^{p-1} \not\equiv -m_2'^{-1} z^{p-1} \mod \delta'$

(115) より

$$\begin{array}{rl} l_2'^{-1} y x^{p-1} \cdot -l_2'^{-1} m_2' z x^{p-1} & \equiv y^p z^p \mod \delta' \\ l_2'^{-2} m_2' \left(x^{p-1}\right)^2 & \equiv -y^{p-1} z^{p-1} \mod \delta' \\ \left(l_2'^{-1} x^{p-1}\right)^2 & \equiv -m_2'^{-1} y^{p-1} z^{p-1} \mod \delta' \end{array} \tag{116}$$

$$\begin{array}{rl} l_2' x y^{p-1} \cdot -m_2' z y^{p-1} & \equiv x^p z^p \mod \delta' \\ l_2' m_2' \left(y^{p-1}\right)^2 & \equiv -x^{p-1} z^{p-1} \mod \delta' \\ \left(y^{p-1}\right)^2 & \equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \mod \delta' \end{array} \tag{117}$$

$$\begin{array}{rl} -l_2' m_2'^{-1} x z^{p-1} \cdot -m_2'^{-1} y z^{p-1} & \equiv x^p y^p \mod \delta' \\ l_2' m_2'^{-2} \left(z^{p-1}\right)^2 & \equiv x^{p-1} y^{p-1} \mod \delta' \\ \left(m_2'^{-1} z^{p-1}\right)^2 & \equiv l_2'^{-1} x^{p-1} y^{p-1} \mod \delta' \end{array} \tag{118}$$

(116)(117)(118) より

$$\left(l_2'^{-1}x^{p-1}\right)^3 \equiv \left(y^{p-1}\right)^3 \equiv -\left(m_2'^{-1}z^{p-1}\right)^3 \mod \delta'$$

$$\left(y^{p-1}\right)^3+\left(m_2'^{-1}z^{p-1}\right)^3 \equiv (y^{p-1}+m_2'^{-1}z^{p-1})((y^{p-1})^2-m_2'^{-1}y^{p-1}z^{p-1}+(m_2'^{-1}z^{p-1})^2) \equiv 0 \mod \delta'$$

$$\left(l_2'^{-1}x^{p-1}\right)^3-\left(y^{p-1}\right)^3 \equiv (l_2'^{-1}x^{p-1}-y^{p-1})((l_2'^{-1}x^{p-1})^2+l_2'^{-1}x^{p-1}y^{p-1}+(y^{p-1})^2) \equiv 0 \mod \delta'$$

$$\left(l_2'^{-1}x^{p-1}\right)^3+\left(m_2'^{-1}z^{p-1}\right)^3 \equiv (l_2'^{-1}x^{p-1}+m_2'^{-1}z^{p-1})((l_2'^{-1}x^{p-1})^2-l_2'^{-1}m_2'^{-1}x^{p-1}z^{p-1}+(m_2'^{-1}z^{p-1})^2) \equiv 0 \quad \mathrm{m}$$

### 1.9.5 $l_2'^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv -m_2'^{-1}z^{p-1} \mod \delta'$ のとき

(116)(118) より

$$\begin{aligned}
(m_2'^{-1}z^{p-1})^2 + (y^{p-1})^2 + (l_2'^{-1}x^{p-1})^2 &\equiv 0 \mod \theta_4' \\
l_2'^{-1}x^{p-1}y^{p-1} + (y^{p-1})^2 - m_2'^{-1}y^{p-1}z^{p-1} &\equiv 0 \mod \theta_4' \\
l_2'^{-1}x^{p-1} + y^{p-1} - m_2'^{-1}z^{p-1} &\equiv 0 \mod \theta_4' \\
l_2'^{-1}x^{p-1} + y^{p-1} &\equiv m_2'^{-1}z^{p-1} \mod \theta_4'
\end{aligned}$$

【General solution conditions】

$$\begin{aligned}
x^p \quad +l_2'y^{p-1}x \quad &\equiv l_2'm_2'^{-1}z^{p-1}x \mod \theta_4' \\
l_2'^{-1}x^{p-1}y \quad +y^p \quad &\equiv m_2'^{-1}z^{p-1}y \mod \theta_4' \\
l_2'^{-1}m_2'x^{p-1}z \quad +m_2'y^{p-1}z \quad &\equiv z^p \mod \theta_4'
\end{aligned} \tag{119}$$

(119) より

$$\begin{aligned}
l_2'y^{p-1}x \cdot l_2'm_2'^{-1}z^{p-1}x &\equiv y^pz^p \mod \theta_4' \\
x^2 &\equiv l_2'^{-2}m_2'yz \mod \theta_4'
\end{aligned} \tag{120}$$

$$\begin{aligned}
l_2'^{-1}x^{p-1}y \cdot m_2'^{-1}z^{p-1}y &\equiv x^pz^p \mod \theta_4' \\
y^2 &\equiv l_2'm_2'xz \mod \theta_4'
\end{aligned} \tag{121}$$

$$\begin{aligned}
l_2'^{-1}m_2'x^{p-1}z \cdot m_2'y^{p-1}z &\equiv x^py^p \mod \theta_4' \\
z^2 &\equiv l_2'm_2'^{-2}xy \mod \theta_4'
\end{aligned} \tag{122}$$

$$
\begin{aligned}
\text{(116) より } \left(x^{p-1}\right)^2 &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \mod \theta_4' \\
\left(x^2\right)^{p-1} &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \mod \theta_4' \\
\text{(120) より } \left(l_2'^{-2} m_2' yz\right)^{p-1} &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \mod \theta_4' \\
l_2'^{-2p+2} m_2'^{p-1} y^{p-1} z^{p-1} &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \mod \theta_4' \\
l_2'^{-2p} m_2'^{p} &\equiv -1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
\text{(117) より } \left(y^{p-1}\right)^2 &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \mod \theta_4' \\
\left(y^2\right)^{p-1} &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \mod \theta_4' \\
\text{(121) より } \left(l_2' m_2' xz\right)^{p-1} &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \mod \theta_4' \\
l_2'^{p-1} m_2'^{p-1} x^{p-1} z^{p-1} &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \mod \theta_4' \\
l_2'^{p} m_2'^{p} &\equiv -1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
\text{(118) より } \left(z^{p-1}\right)^2 &\equiv l_2'^{-1} m_2'^{2} x^{p-1} y^{p-1} \mod \theta_4' \\
\left(z^2\right)^{p-1} &\equiv l_2'^{-1} m_2'^{2} x^{p-1} y^{p-1} \mod \theta_4' \\
\text{(122) より } \left(l_2' m_2'^{-2} xy\right)^{p-1} &\equiv l_2'^{-1} m_2'^{2} x^{p-1} y^{p-1} \mod \theta_4' \\
l_2'^{p-1} m_2'^{-2p+2} x^{p-1} y^{p-1} &\equiv l_2'^{-1} m_2'^{2} x^{p-1} y^{p-1} \mod \theta_4' \\
l_2'^{p} m_2'^{-2p} &\equiv 1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
l_2'^p m_2'^p &\equiv -1 \mod \theta_4' \\
l_2'^{-2p} m_2'^p &\equiv -1 \mod \theta_4' \\
l_2'^p m_2'^{-2p} &\equiv 1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
-m_2'^{3p} &\equiv l_2'^{3p} \mod \theta_4' \\
m_2'^{3p} + l_2'^{3p} &\equiv (m_2'^p + l_2'^p)(m_2'^{2p} - l_2'^p m_2'^p + l_2'^{2p}) \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
m_2'^p &\equiv -l_2'^{2p} \mod \theta_4' \\
l_2'^p &\equiv m_2'^{2p} \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
m_2'^p + l_2'^p &\equiv m_2'^{2p} - l_2'^{2p} \mod \theta_4' \\
m_2'^p + l_2'^p &\equiv (m_2'^p + l_2'^p)(m_2'^p - l_2'^p) \mod \theta_4' \\
1 &\equiv m_2'^p - l_2'^p \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
(m_2'^p - l_2'^p)^2 &\equiv 1^2 \mod \theta_4' \\
m_2'^{2p} - 2l_2'^p m_2'^p + l_2'^{2p} &\equiv 1 \mod \theta_4' \\
m_2'^{2p} - 2l_2'^p m_2'^p + l_2'^{2p} &\equiv -l_2'^p m_2'^p \mod \theta_4' \\
m_2'^{2p} - l_2'^p m_2'^p + l_2'^{2p} &\equiv 0 \mod \theta_4'
\end{aligned}
$$

よって $m_2'^p + l_2'^p \not\equiv 0 \mod \theta_4$

$$
\begin{aligned}
m_2'^p - l_2'^p &\equiv 1 \mod \theta_4' \\
-l_2'^p m_2'^p + l_2'^{2p} &\equiv -l_2'^p \mod \theta_4' \\
l_2'^{2p} + l_2'^p + 1 &\equiv 0 \mod \theta_4'
\end{aligned}
$$

(105)(115) より

$$
\begin{aligned}
l_2'^{-1} y x^{p-1} &\equiv l_1' y x^{p-1} \mod \delta' \\
l_2'^{-1} &\equiv l_1' \mod \delta' \\
1 &\equiv l_1' l_2'^p \mod \delta'
\end{aligned} \tag{123}
$$

$l_2'^p m_2'^p \equiv -1 \mod \theta_4'$ なので

$$
l_2'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4' \tag{124}
$$

$$
m_2'^p \equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4' \tag{125}
$$

$x - k'_3 + y + k'_3 \equiv -z \mod \delta'$ より

**Definition 25** $x - k'_3 \equiv m'_3 x \mod \delta'$ , $y + k'_3 \equiv l'_3 y \mod \delta'$ , $l'_3 m'_3 \perp \delta'$

$$-m'_3 x z^{p-1} \cdot -l'_3 y z^{p-1} \equiv x^p y^p \mod \delta'$$

$m'_3 x + l'_3 y \equiv -z \mod \delta'$ より

$$\begin{array}{ccc} x^p & +l'_3 m'^{-1}_3 y x^{p-1} & \equiv -m'^{-1}_3 z x^{p-1} \mod \delta' \\ l'^{-1}_3 m'_3 x y^{p-1} & +y^p & \equiv -l'^{-1}_3 z y^{p-1} \mod \delta' \\ -m'_3 x z^{p-1} & -l'_3 y z^{p-1} & \equiv z^p \mod \delta' \end{array} \tag{126}$$

ここで

$$-m'_3 x z^{p-1} \equiv x^p \mod \delta' \Rightarrow -l'_3 y z^{p-1} \equiv y^p \mod \delta'$$
$$-m'_3 z^{p-1} \equiv x^{p-1} \mod \delta' \Rightarrow -l'_3 z^{p-1} \equiv y^{p-1} \mod \delta'$$

であるから自動的に

$$l'_3 m'^{-1}_3 y x^{p-1} \equiv y^p \mod \delta' \quad , \quad -m'^{-1}_3 z x^{p-1} \equiv z^p \mod \delta'$$
$$l'^{-1}_3 m'_3 x y^{p-1} \equiv x^p \mod \delta' \quad , \quad -l'^{-1}_3 z y^{p-1} \equiv z^p \mod \delta'$$

よって $x^p + y^p \equiv z^p \mod \delta'$ が成り立つ条件は

$$\begin{gathered} m'^{-1}_3 x^{p-1} \equiv l'^{-1}_3 y^{p-1} \equiv -z^{p-1} \mod \delta' \\ or \\ m'^{-1}_3 x^{p-1} \not\equiv l'^{-1}_3 y^{p-1} \not\equiv -z^{p-1} \mod \delta' \end{gathered}$$

### 1.9.6 Common to $m'^{-1}_3 x^{p-1} \not\equiv l'^{-1}_3 y^{p-1} \not\equiv -z^{p-1} \mod \delta'$

(126) より

$$\begin{array}{cc} l'_3 m'^{-1}_3 y x^{p-1} \cdot -m'^{-1}_3 z x^{p-1} & \equiv y^p z^p \mod \delta' \\ l'_3 m'^{-2}_3 \left(x^{p-1}\right)^2 & \equiv -y^{p-1} z^{p-1} \mod \delta' \\ \left(m'^{-1}_3 x^{p-1}\right)^2 & \equiv -l'^{-1}_3 y^{p-1} z^{p-1} \mod \delta' \end{array} \tag{127}$$

$$\begin{array}{cc} l'^{-1}_3 m'_3 x y^{p-1} \cdot -l'^{-1}_3 z y^{p-1} & \equiv x^p z^p \mod \delta' \\ l'^{-2}_3 m'_3 \left(y^{p-1}\right)^2 & \equiv -x^{p-1} z^{p-1} \mod \delta' \\ \left(l'^{-1}_3 y^{p-1}\right)^2 & \equiv -m'^{-1}_3 x^{p-1} z^{p-1} \mod \delta' \end{array} \tag{128}$$

$$\begin{array}{cc} -m'_3 x z^{p-1} \cdot -l'_3 y z^{p-1} & \equiv x^p y^p \mod \delta' \\ l'_3 m'_3 \left(z^{p-1}\right)^2 & \equiv x^{p-1} y^{p-1} \mod \delta' \\ \left(z^{p-1}\right)^2 & \equiv l'^{-1}_3 m'^{-1}_3 x^{p-1} y^{p-1} \mod \delta' \end{array} \tag{129}$$

(127)(128)(129) より

$$\left(m_3'^{-1}x^{p-1}\right)^3 \equiv \left(l_3'^{-1}y^{p-1}\right)^3 \equiv -\left(z^{p-1}\right)^3 \mod \delta'$$

$$\left(z^{p-1}\right)^3+\left(l_3'^{-1}y^{p-1}\right)^3 \equiv (z^{p-1}+l_3'^{-1}y^{p-1})((z^{p-1})^2-l_3'^{-1}y^{p-1}z^{p-1}+(l_3'^{-1}y^{p-1})^2) \equiv 0 \mod \delta'$$

$$\left(m_3'^{-1}x^{p-1}\right)^3+\left(z^{p-1}\right)^3 \equiv (m_3'^{-1}x^{p-1}+z^{p-1})((m_3'^{-1}x^{p-1})^2-m_3'^{-1}x^{p-1}z^{p-1}+(z^{p-1})^2) \equiv 0 \mod \delta'$$

$$\left(m_3'^{-1}x^{p-1}\right)^3-\left(l_3'^{-1}y^{p-1}\right)^3 \equiv (m_3'^{-1}x^{p-1}-l_3'^{-1}y^{p-1})((m_3'^{-1}x^{p-1})^2+l_3'^{-1}m_3'^{-1}x^{p-1}y^{p-1}+(l_3'^{-1}y^{p-1})^2) \equiv 0 \quad \mathrm{m}$$

### 1.9.7 $m_3'^{-1}x^{p-1} \not\equiv l_3'^{-1}y^{p-1} \not\equiv -z^{p-1} \mod \delta'$ のとき

(127)(128) より

$$\begin{aligned}
(l_3'^{-1}y^{p-1})^2 + (m_3'^{-1}x^{p-1})^2 + (z^{p-1})^2 &\equiv 0 \mod \theta_4' \\
-m_3'^{-1}x^{p-1}z^{p-1} - l_3'^{-1}y^{p-1}z^{p-1} + (z^{p-1})^2 &\equiv 0 \mod \theta_4' \\
m_3'^{-1}x^{p-1} + l_3'^{-1}y^{p-1} - z^{p-1} &\equiv 0 \mod \theta_4' \\
m_3'^{-1}x^{p-1} + l_3'^{-1}y^{p-1} &\equiv z^{p-1} \mod \theta_4'
\end{aligned}$$

【General solution conditions】

$$\begin{array}{rcl}
x^p \quad +l_3'^{-1}m_3'y^{p-1}x & \equiv m_3'z^{p-1}x \mod \theta_4' \\
l_3'm_3'^{-1}x^{p-1}y \quad +y^p & \equiv l_3'z^{p-1}y \mod \theta_4' \\
m_3'^{-1}x^{p-1}z \quad +l_3'^{-1}y^{p-1}z & \equiv z^p \mod \theta_4'
\end{array} \tag{130}$$

(130) より

$$\begin{aligned}
l_3'^{-1}m_3'y^{p-1}x \cdot m_3'z^{p-1}x &\equiv y^pz^p \mod \theta_4' \\
x^2 &\equiv l_3'm_3'^{-2}yz \mod \theta_4'
\end{aligned} \tag{131}$$

$$\begin{aligned}
l_3'm_3'^{-1}x^{p-1}y \cdot l_3'z^{p-1}y &\equiv x^pz^p \mod \theta_4' \\
y^2 &\equiv l_3'^{-2}m_3'xz \mod \theta_4'
\end{aligned} \tag{132}$$

$$\begin{aligned}
m_3'^{-1}x^{p-1}z \cdot l_3'^{-1}y^{p-1}z &\equiv x^py^p \mod \theta_4' \\
z^2 &\equiv l_3'm_3'xy \mod \theta_4'
\end{aligned} \tag{133}$$

$$
\begin{aligned}
(127)\text{ より }\left(x^{p-1}\right)^2 &\equiv -l_3'^{-1}m_3'^2y^{p-1}z^{p-1} \mod \theta_4'\\
\left(x^2\right)^{p-1} &\equiv -l_3'^{-1}m_3'^2y^{p-1}z^{p-1} \mod \theta_4'\\
(131)\text{ より }\left(l_3'm_3'^{-2}yz\right)^{p-1} &\equiv -l_3'^{-1}m_3'^2y^{p-1}z^{p-1} \mod \theta_4'\\
l_3'^{p-1}m_3'^{-2p+2}y^{p-1}z^{p-1} &\equiv -l_3'^{-1}m_3'^2y^{p-1}z^{p-1} \mod \theta_4'\\
l_3'^pm_3'^{-2p} &\equiv -1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
(128)\text{ より }\left(y^{p-1}\right)^2 &\equiv -l_3'^2m_3'^{-1}x^{p-1}z^{p-1} \mod \theta_4'\\
\left(y^2\right)^{p-1} &\equiv -l_3'^2m_3'^{-1}x^{p-1}z^{p-1} \mod \theta_4'\\
(132)\text{ より }\left(l_3'^{-2}m_3'xz\right)^{p-1} &\equiv -l_3'^2m_3'^{-1}x^{p-1}z^{p-1} \mod \theta_4'\\
l_3'^{-2p+2}m_3'^{p-1}x^{p-1}z^{p-1} &\equiv -l_3'^2m_3'^{-1}x^{p-1}z^{p-1} \mod \theta_4'\\
l_3'^{-2p}m_3'^p &\equiv -1 \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
(129)\text{ より }\left(z^{p-1}\right)^2 &\equiv l_3'^{-1}m_3'^{-1}x^{p-1}y^{p-1} \mod \theta_4'\\
\left(z^2\right)^{p-1} &\equiv l_3'^{-1}m_3'^{-1}x^{p-1}y^{p-1} \mod \theta_4'\\
(133)\text{ より }\left(l_3'm_3'xy\right)^{p-1} &\equiv l_3'^{-1}m_3'^{-1}x^{p-1}y^{p-1} \mod \theta_4'\\
l_3'^{p-1}m_3'^{p-1}x^{p-1}y^{p-1} &\equiv l_3'^{-1}m_3'^{-1}x^{p-1}y^{p-1} \mod \theta_4'\\
l_3'^pm_3'^p &\equiv 1 \mod \theta_4'
\end{aligned}
$$

$$\begin{aligned} l_3'^p m_3'^p &\equiv 1 \mod \theta_4' \\ l_3'^{-2p} m_3'^p &\equiv -1 \mod \theta_4' \\ l_3'^p m_3'^{-2p} &\equiv -1 \mod \theta_4' \end{aligned} \tag{134}$$

$$m_3'^{3p} \equiv l_3'^{3p} \mod \theta_4'$$
$$m_3'^{3p} - l_3'^{3p} \equiv (m_3'^p - l_3'^p)(m_3'^{2p} + l_3'^p m_3'^p + l_3'^{2p}) \mod \theta_4'$$

$$-m_3'^p \equiv l_3'^{2p} \mod \theta_4'$$
$$l_3'^p \equiv -m_3'^{2p} \mod \theta_4'$$

$$l_3'^p - m_3'^p \equiv l_3'^{2p} - m_3'^{2p} \mod \theta_4'$$
$$l_3'^p - m_3'^p \equiv (l_3'^p + m_3'^p)(l_3'^p - m_3'^p) \mod \theta_4'$$
$$1 \equiv l_3'^p + m_3'^p \mod \theta_4'$$

$$(l_3'^p + m_3'^p)^2 \equiv 1^2 \mod \theta_4'$$
$$l_3'^{2p} + 2l_3'^p m_3'^p + m_3'^{2p} \equiv 1 \mod \theta_4'$$
$$l_3'^{2p} + 2l_3'^p m_3'^p + m_3'^{2p} \equiv l_3'^p m_3'^p \mod \theta_4'$$
$$l_3'^{2p} + l_3'^p m_3'^p + m_3'^{2p} \equiv 0 \mod \theta_4'$$

$m_3'^p - l_3'^p \not\equiv 0 \mod \theta_4'$ なので $m_3' \equiv 1 \mod \theta_4'$ , $l_3' \equiv 1 \mod \theta_4'$ のとき
$x^p + y^p \not\equiv z^p \mod \theta_4'$

$$l_3'^p + m_3'^p \equiv 1 \mod \theta_4'$$
$$l_3'^{2p} + l_3'^p m_3'^p \equiv l_3'^p \mod \theta_4'$$
$$l_3'^{2p} - l_3'^p + 1 \equiv 0 \mod \theta_4'$$

(105)(115)(126) より

$$\begin{aligned} -m_1'^{-1} x z^{p-1} &\equiv -m_3' x z^{p-1} \mod \delta' \\ m_1'^{-1} &\equiv m_3' \mod \delta' \\ 1 &\equiv m_1^p m_3'^p \mod \delta' \end{aligned} \tag{135}$$

$$\begin{aligned} -l_3'^{-1} z y^{p-1} &\equiv -m_2' z y^{p-1} \mod \delta' \\ l_3'^{-1} &\equiv m_2' \mod \delta' \end{aligned} \tag{136}$$

$l_3'^p m_3'^p \equiv 1 \mod \theta_4'$ なので

$$l_3'^p \equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4' \tag{137}$$

$$m_3'^p \equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4' \tag{138}$$

### 1.9.8 A splice

(110) より

$$\begin{aligned} x^2 &\equiv l'_1 m'_1 yz \mod \theta'_4 \\ -x^2 &\equiv l'_1 y \cdot -m'_1 z \mod \theta'_4 \\ -x^2 &\equiv (y+k'_1)(-z+k'_1) \mod \theta'_4 \\ -x^2 &\equiv -yz + (y-z)k'_1 + k'^2_1 \mod \theta'_4 \\ 0 &\equiv k'^2_1 + (y-z)k'_1 - yz + x^2 \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} k'_1 &\equiv \frac{z-y \pm \sqrt{(y-z)^2 - 4(-yz+x^2)}}{2} \mod \theta'_4 \\ k'_1 &\equiv \frac{z-y \pm \sqrt{(y+z)^2 - 4x^2}}{2} \mod \theta'_4 \\ k'_1 &\equiv \frac{z-y \pm \sqrt{x^2 - 4x^2}}{2} \mod \theta'_4 \\ k'_1 &\equiv \frac{z-y \pm \sqrt{-3x^2}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} y + k'_1 &\equiv \frac{z+y \pm \sqrt{-3x^2}}{2} \mod \theta'_4 \\ -z + k'_1 &\equiv \frac{-z-y \pm \sqrt{-3x^2}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} l'_1 y &\equiv x \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -m'_1 z &\equiv x \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} l'_1 y x^{p-1} &\equiv x^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -m'_1 z x^{p-1} &\equiv x^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} -z^p &\equiv x^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -y^p &\equiv x^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned} \tag{139}$$

$$
\begin{aligned}
y &\equiv x l_1'^{-1} \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4' \\
-z &\equiv x m_1'^{-1} \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

(123)(135) より

$$
\begin{aligned}
y &\equiv x l_2' \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4' \\
-z &\equiv x m_3' \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
y^p &\equiv x^p l_2'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4' \\
-z^p &\equiv x^p m_3'^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4'
\end{aligned}
$$

(139) より

$$
\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv l_2'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4' \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv m_3'^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4'
\end{aligned}
$$

(124)(138) より

$$
\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \mp \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4' \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \mp \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4'
\end{aligned}
$$

$l_1'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4'$ のとき

$$
\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \pm \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4' \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \pm \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4'
\end{aligned}
$$

(121) より

$$\begin{aligned} y^2 &\equiv l'_2 m'_2 xz \mod \theta'_4 \\ -y^2 &\equiv l'_2 x \cdot -m'_2 z \mod \theta'_4 \\ -y^2 &\equiv (x+k'_2)(-z+k'_2) \mod \theta'_4 \\ -y^2 &\equiv -xz + (x-z)k'_2 + k'^2_2 \mod \theta'_4 \\ 0 &\equiv k'^2_2 + (x-z)k'_2 - xz + y^2 \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} k'_2 &\equiv \frac{z-x \pm \sqrt{(x-z)^2 - 4(-xz+y^2)}}{2} \mod \theta'_4 \\ k'_2 &\equiv \frac{z-x \pm \sqrt{(x+z)^2 - 4y^2}}{2} \mod \theta'_4 \\ k'_2 &\equiv \frac{z-x \pm \sqrt{y^2 - 4y^2}}{2} \mod \theta'_4 \\ k'_2 &\equiv \frac{z-x \pm \sqrt{-3y^2}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} x + k'_2 &\equiv \frac{z+x \pm \sqrt{-3y^2}}{2} \mod \theta'_4 \\ -z + k'_2 &\equiv \frac{-z-x \pm \sqrt{-3y^2}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} l'_2 x &\equiv y \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -m'_2 z &\equiv y \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} l'_2 x y^{p-1} &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -m'_2 z y^{p-1} &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned}$$

(139) より ± の調整

$$\begin{aligned} -z^p &\equiv y^p \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta'_4 \\ -x^p &\equiv y^p \cdot \frac{1 \mp \sqrt{-3}}{2} \mod \theta'_4 \end{aligned} \tag{140}$$

$$
\begin{aligned}
x &\equiv y l_2'^{-1} \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
-z &\equiv y m_2'^{-1} \cdot \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

(123)(136) より

$$
\begin{aligned}
x &\equiv y l_1' \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
z &\equiv y l_3' \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
x^p &\equiv y^p l_1'^p \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^p \mod \theta_4' \\
z^p &\equiv y^p l_3'^p \cdot \left( \frac{-1 \pm \sqrt{-3}}{2} \right)^p \mod \theta_4'
\end{aligned}
$$

(140) より

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv l_1'^p \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^p \mod \theta_4' \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv l_3'^p \cdot \left( \frac{-1 \pm \sqrt{-3}}{2} \right)^p \mod \theta_4'
\end{aligned}
$$

(113)(137) より

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{-1 \pm \sqrt{-3}}{2} \right) \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^{6n+3} \mod \theta_4' \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{1 \pm \sqrt{-3}}{2} \right) \cdot \left( \frac{-1 \pm \sqrt{-3}}{2} \right)^{6n+3} \mod \theta_4'
\end{aligned}
$$

$l_1'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4'$ のとき

$$
\begin{aligned}
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{-1 \mp \sqrt{-3}}{2} \right) \cdot \left( \frac{-1 \mp \sqrt{-3}}{2} \right)^{6n+1} \mod \theta_4' \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv \left( \frac{1 \mp \sqrt{-3}}{2} \right) \cdot \left( \frac{-1 \pm \sqrt{-3}}{2} \right)^{6n+1} \mod \theta_4'
\end{aligned}
$$

(133) より

$$\begin{aligned} z^2 &\equiv l'_3 m'_3 xy \mod \theta'_4 \\ -z^2 &\equiv -m'_3 x \cdot l'_3 y \mod \theta'_4 \\ -z^2 &\equiv (-x + k''_3)(y + k''_3) \mod \theta'_4 \\ -z^2 &\equiv -xy + (y-x)k''_3 + k''^2_3 \mod \theta'_4 \\ 0 &\equiv k''^2_3 + (y-x)k''_3 - xy + z^2 \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} k''_3 &\equiv \frac{x - y \pm \sqrt{(y-x)^2 - 4(-xy + z^2)}}{2} \mod \theta'_4 \\ k''_3 &\equiv \frac{x - y \pm \sqrt{(y+x)^2 - 4z^2}}{2} \mod \theta'_4 \\ k''_3 &\equiv \frac{x - y \pm \sqrt{z^2 - 4z^2}}{2} \mod \theta'_4 \\ k''_3 &\equiv \frac{x - y \pm \sqrt{-3z^2}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} y + k''_3 &\equiv \frac{x + y \pm \sqrt{-3z^2}}{2} \mod \theta'_4 \\ -x + k''_3 &\equiv \frac{-x - y \pm \sqrt{-3z^2}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} l'_3 y &\equiv z \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -m'_3 x &\equiv z \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned}$$

$$\begin{aligned} l'_3 y z^{p-1} &\equiv z^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta'_4 \\ -m'_3 x z^{p-1} &\equiv z^p \cdot \frac{1 \pm \sqrt{-3}}{2} \mod \theta'_4 \end{aligned}$$

(139) より ± の調整

$$\begin{aligned} -x^p &\equiv z^p \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta'_4 \\ y^p &\equiv z^p \cdot \frac{1 \mp \sqrt{-3}}{2} \mod \theta'_4 \end{aligned} \tag{141}$$

$$
\begin{aligned}
y &\equiv z l_3'^{-1} \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
-x &\equiv z m_3'^{-1} \cdot \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

(136)(135) より

$$
\begin{aligned}
y &\equiv z m_2' \cdot \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
x &\equiv z m_1' \cdot \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
y^p &\equiv z^p m_2'^p \cdot \left(\frac{-1 \mp \sqrt{-3}}{2}\right)^p \mod \theta_4' \\
x^p &\equiv z^p m_1'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4'
\end{aligned}
$$

(141) より

$$
\begin{aligned}
\frac{1 \mp \sqrt{-3}}{2} &\equiv m_2'^p \cdot \left(\frac{-1 \mp \sqrt{-3}}{2}\right)^p \mod \theta_4' \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv m_1'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^p \mod \theta_4'
\end{aligned}
$$

(125)(114) より

$$
\begin{aligned}
\frac{1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{1 \mp \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \mp \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4' \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv \left(\frac{1 \pm \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+3} \mod \theta_4'
\end{aligned}
$$

$l_1'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4'$ のとき

$$
\begin{aligned}
\frac{1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{1 \pm \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \mp \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4' \\
\frac{1 \pm \sqrt{-3}}{2} &\equiv \left(\frac{1 \mp \sqrt{-3}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{6n+1} \mod \theta_4'
\end{aligned}
$$

### 1.9.9 $p = 6n + 1$ のとき

$$
\begin{aligned}
l_1'^p \equiv l_1' &\equiv \frac{-1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
m_1'^p \equiv m_1' &\equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
l_2'^p \equiv l_2' &\equiv \frac{-1 \pm \sqrt{-3}}{2} \mod \theta_4' \\
m_2'^p \equiv m_2' &\equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4' \\
l_3'^p \equiv l_3' &\equiv \frac{1 \mp \sqrt{-3}}{2} \mod \theta_4' \\
m_3'^p \equiv m_3' &\equiv \frac{1 \pm \sqrt{-3}}{2} \mod \theta_4'
\end{aligned}
$$

(110)(121)(133) より

$$
\begin{aligned}
x^2 &\equiv l_1' m_1' yz \mod \theta_4' \\
x^2 &\equiv -yz \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
y^2 &\equiv l_2' m_2' xz \mod \theta_4' \\
y^2 &\equiv -xz \mod \theta_4'
\end{aligned}
$$

$$
\begin{aligned}
z^2 &\equiv l_3' m_3' xy \mod \theta_4' \\
z^2 &\equiv xy \mod \theta_4'
\end{aligned}
$$

$$
-z^3 \equiv x^3 \equiv y^3 \mod \theta_4'
$$

$$
\begin{aligned}
z^3 + y^3 &\equiv (z+y)(z^2 - yz + y^2) \equiv 0 \mod \theta_4' \\
x^3 + z^3 &\equiv (x+z)(x^2 - xz + z^2) \equiv 0 \mod \theta_4' \\
x^3 - y^3 &\equiv (x-y)(x^2 + xy + y^2) \equiv 0 \mod \theta_4'
\end{aligned}
$$

$x + z + y \equiv 0 \mod \theta_4'$ なので

$$
x + z \not\equiv 0 \mod \theta_4'
$$

$$
\begin{aligned}
x^2 - xz + z^2 &\equiv 0 \mod \theta_4' \\
x^2 - xz + xy &\equiv 0 \mod \theta_4' \\
x - z + y &\not\equiv 0 \mod \theta_4'
\end{aligned}
$$

よって $p = 6n + 1$ は満たさない。

### 1.9.10 $p = 6n + 3$ のとき

$p$ は素数なので $n = 0$ ， $p = 3$、$x^3 + y^3 \equiv z^3 \mod \theta_4'$

$$
\begin{aligned}
(x+z+y)^3 &\equiv x^3 + z^3 + y^3 + 3x^2y + 3x^2z + 3xy^2 + 3xz^2 + 3y^2z + 3yz^2 + 6xyz \mod \theta_4' \\
(x+z+y)^3 &\equiv 2z^3 + 3(x^2y + x^2z + xy^2 + xz^2 + y^2z + yz^2 + 2xyz) \mod \theta_4' \\
(x+z+y)^3 &\equiv 2z^3 + 3(y(x^2 + 2xz + z^2) + (x+z)xz + (x+z)y^2) \mod \theta_4' \\
(x+z+y)^3 &\equiv 2z^3 + 3(y(x+z)^2 + (x+z)xz + (x+z)y^2) \mod \theta_4' \\
(x+z+y)^3 &\equiv 2z^3 + 3(x+z)(xy + yz + xz + y^2) \mod \theta_4' \\
(x+z+y)^3 &\equiv 2z^3 + 3(x+z)(x(y+z) + y(y+z)) \mod \theta_4' \\
(x+z+y)^3 &\equiv 2z^3 + 3(x+z)(y+z)(y+x) \mod \theta_4' \\
0 &\equiv 2z^3 - 3yxz \mod \theta_4' \\
2z^2 &\equiv 3xy \mod \theta_4'
\end{aligned}
$$

(133) より

$$
\begin{aligned}
2l_3'm_3'xy &\equiv 3xy \mod \theta_4' \\
2l_3'm_3' &\equiv 3 \mod \theta_4' \\
2^p l_3'^p m_3'^p &\equiv 3^p \mod \theta_4'
\end{aligned}
$$

(134) より

$$
\begin{aligned}
2^3 &\equiv 3^3 \mod \theta_4' \\
8 &\equiv 27 \mod \theta_4' \\
0 &\equiv 19 \mod \theta_4'
\end{aligned}
$$

$$
x + z + y \equiv 0 \mod 19
$$

$x + z - y \equiv 0 \mod 19$ が成り立つと仮定すると $19 \mid y$ となり前提に反する。

## 1.10 $\delta' = 2$ のとき

### 1.10.1 $2 \mid z$ , $2 \perp xy$

$S" = 2^k$ のとき

$$z + x + y = p^n c 2^k$$

$$z^p = x^p + y^p = (x+y)(py^{p-1} + (x+y)(\ldots))$$

$$2 \mid L = p^{np-1} c^p$$
$$2 \mid c$$

$$2 \perp R = p\gamma^p$$
$$2 \perp \gamma$$

$$z + x + y = p^n c(\gamma + p^{(p-1)n-1} c^{p-1})$$
$$2^k = \gamma + p^{(p-1)n-1} c^{p-1} = odd$$
$$2^0 = 1$$

しかし、$\gamma + p^{(p-1)n-1} c^{p-1} > 1$ なので矛盾する。$p \perp z$ のときも同様である。

よって $2 \mid z$ のとき成り立たない。

$y + z - x$ は $x, y$ について $x + z - y$ と対称のため $2 \mid y$ のときも成り立たない。

以上より

$$x^p + y^p \neq z^p \quad (p \geqq 3)$$