

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	2
1.1	$\delta \perp xyz$ の導出	3
1.1.1	$p \mid x$ のとき	5
1.1.2	$p \perp x$ のとき ($p \mid yz$ 条件は省略)	6
1.2	解の条件 (Solution conditions)	7
1.3	$(x^{p-1})^2 \equiv y^{p-1}z^{p-1} \pmod{\delta}$ のとき	10
1.4	同値変換 (Equivalence transformation)	11
1.5	一般的解の条件 (General solution conditions)	11
1.5.1	$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1}$ のとき	11
1.5.2	Common to $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2}$	12
1.5.3	$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2}$ のとき	14
1.5.4	$-y \equiv z \equiv x \pmod{\theta_3}$ のとき	14
1.5.5	Common to $-y \not\equiv z \not\equiv x \pmod{\theta_4}$	15
1.5.6	まとめ	17
1.6	$-x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \pmod{\delta}$ のとき	18
1.6.1	Common to $-x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \pmod{\delta}$	18
1.6.2	$-x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \pmod{\delta}$ のとき	19
1.6.3	Common to $-l_2^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv m_2^{-1}z^{p-1} \pmod{\delta}$	22
1.6.4	$-l_2^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv m_2^{-1}z^{p-1} \pmod{\delta}$ のとき	23
1.6.5	Common to $-m_3^{-1}x^{p-1} \not\equiv l_3^{-1}y^{p-1} \not\equiv z^{p-1} \pmod{\delta}$	26
1.6.6	$-m_3^{-1}x^{p-1} \not\equiv l_3^{-1}y^{p-1} \not\equiv z^{p-1} \pmod{\delta}$ のとき	27
1.6.7	Cycle	30
1.6.8	A splice	31
1.6.9	$p = 6n + 1$ のとき	37
1.6.10	$p = 6n + 3$ のとき	38
1.7	$-x^{p-1} \equiv l_1^{-1}y^{p-1} \equiv m_1^{-1}z^{p-1} \pmod{\delta}$ のとき	39
1.7.1	Common to $x^{p-1} \not\equiv q_1^{-1}y^{p-1} \not\equiv r_1^{-1}z^{p-1} \pmod{\delta}$	39
1.7.2	$x^{p-1} \not\equiv q_1^{-1}y^{p-1} \not\equiv r_1^{-1}z^{p-1} \pmod{\delta}$ のとき	40

1.7.3	Common to $q_2^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv r_2^{-1}z^{p-1} \pmod{\delta}$	43
1.7.4	$q_2^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv r_2^{-1}z^{p-1} \pmod{\delta}$ のとき	44
1.7.5	Common to $q_3^{-1}x^{p-1} \not\equiv r_3^{-1}y^{p-1} \not\equiv z^{p-1} \pmod{\delta}$	46
1.7.6	$z^{p-1} \not\equiv q_3^{-1}x^{p-1} \not\equiv r_3^{-1}y^{p-1} \pmod{\delta}$ のとき	47
1.7.7	A splice	49
1.7.8	$p = 6n + 1$ のとき	55
1.7.9	$p = 6n + 3$ のとき	56
1.7.10	Complement 1(補足 1)	56
1.7.11	Complement 2(補足 2)	57
1.8	$\delta = 2$ のとき	59
1.8.1	$2 \mid x$, $2 \perp yz$	59
1.9	$\delta' \perp xyz$ の導出	60
1.9.1	$p \mid z$ のとき (諸条件は省略)	60
1.9.2	Common to $x^{p-1} \not\equiv l_1'^{-1}y^{p-1} \not\equiv -m_1'^{-1}z^{p-1} \pmod{\delta'}$	61
1.9.3	$x^{p-1} \not\equiv l_1'^{-1}y^{p-1} \not\equiv -m_1'^{-1}z^{p-1} \pmod{\delta'}$ のとき	62
1.9.4	Common to $l_2'^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv -m_2'^{-1}z^{p-1} \pmod{\delta'}$	65
1.9.5	$l_2'^{-1}x^{p-1} \not\equiv y^{p-1} \not\equiv -m_2'^{-1}z^{p-1} \pmod{\delta'}$ のとき	66
1.9.6	Common to $m_3'^{-1}x^{p-1} \not\equiv l_3'^{-1}y^{p-1} \not\equiv -z^{p-1} \pmod{\delta'}$	69
1.9.7	$m_3'^{-1}x^{p-1} \not\equiv l_3'^{-1}y^{p-1} \not\equiv -z^{p-1} \pmod{\delta'}$ のとき	70
1.9.8	A splice	73
1.9.9	$p = 6n + 1$ のとき	79
1.9.10	$p = 6n + 3$ のとき	80
1.10	$\delta' = 2$ のとき	81
1.10.1	$2 \mid z$, $2 \perp xy$	81

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)

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

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

$$p \mid x, p \nmid yz \Rightarrow p^n \mid x \ (n \geq 2), p^{n^{p-1}} \mid z - y$$

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

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

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

一般的に

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

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

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

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

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

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

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。

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

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

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

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

よって、少なくとも

$$p^2 \mid x$$

$x = p^2a\alpha$ 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

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

□

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

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

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

Proof 6

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

$\delta \mid S$ 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 $\delta \mid x + z$

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

$z^p - x^p = y^p \equiv 0 \pmod{\delta}$ なので

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

よって

$$\delta \perp \beta$$

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

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

よって

$$\delta \perp \gamma$$

□

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

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

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

Proof 8

$$\begin{aligned} x + z - y &= a'\alpha' + a'^p \\ &= a'(\alpha' + a'^{p-1}) \\ p \perp x, (3) \text{ より } p \perp S' , p \perp \delta \\ \alpha'^p &= R = py^{p-1} + (z - y)(\dots) \\ R &\equiv py^{p-1} \pmod{a'} \\ py^{p-1} &\perp a' \\ \alpha' &\perp a' \end{aligned}$$

$\delta \mid S'$ 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 $\delta \mid x + z$

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

$z^p - x^p = y^p \equiv 0 \pmod{\delta}$ なので

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

よって $\delta \perp \beta'$
 $\delta \mid \gamma'$, $\delta \mid x - y$ ならば同様に

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

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

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

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。

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

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

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

$$yz \equiv UT \pmod{\theta}$$

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

同様に

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

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

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

$\theta \perp xyzU'T'$ 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。

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

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

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

$$xz \equiv U'T' \pmod{\theta}$$

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

同様に

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

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

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

$\theta \perp xyzU''T'''$ 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。

$$\begin{aligned}
-U''y^{p-1} - T'''x^{p-1} &\equiv z^p \pmod{\theta} \\
-U''y^{p-1} - T'''x^{p-1} &\equiv x^p + y^p \pmod{\theta} \\
-x^p - T'''x^{p-1} &\equiv U''y^{p-1} + y^p \pmod{\theta} \\
-x^{p-1}(x + T''') &\equiv y^{p-1}(U'' + y) \pmod{\theta} \\
-x^{p-1}(xy + T'''y) &\equiv y \cdot y^{p-1}(U'' + y) \pmod{\theta} \\
-U''y^{p-1} \cdot -T'''x^{p-1} &\equiv x^p y^p \pmod{\theta} \text{ ならば} \\
xy &\equiv U''T''' \pmod{\theta}
\end{aligned} \tag{8}$$

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

同様に

$$\begin{aligned}
-x \cdot x^{p-1}(x + T''') &\equiv y^{p-1}(xU'' + xy) \pmod{\theta} \\
-x^p(x + T''') &\equiv y^{p-1}(xU'' + U''T''') \pmod{\theta} \\
x^p(x + T''') &\equiv -U''y^{p-1}(x + T''') \pmod{\theta}
\end{aligned}$$

よって合同式 (8) および $-U''y^{p-1} \cdot -T'''x^{p-1} \equiv x^p y^p \pmod{\theta}$ を満たすとき解の候補は 3 通りである。

$$\begin{aligned}
-U''y^{p-1} &\equiv x^p \pmod{\theta} \\
-T'''x^{p-1} &\equiv y^p \pmod{\theta} \\
&\text{or , and} \\
-U''y^{p-1} &\equiv y^p \pmod{\theta} \\
-T'''x^{p-1} &\equiv x^p \pmod{\theta}
\end{aligned} \tag{9}$$

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

(4),(6),(8) から

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

【Solution conditions】

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

1.3 $(x^{p-1})^2 \equiv y^{p-1}z^{p-1} \pmod{\delta}$ のとき

$x - y \equiv -z \pmod{\delta}$ より

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

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

ならば

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

であるから自動的に

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

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

Definition 9 $y \equiv rz \pmod{\delta}$, $z \equiv qy \pmod{\delta}$, $qr \perp \delta$

$$x + qy \equiv rz \pmod{\delta}$$

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

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

ならば

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

であるから自動的に

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

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

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

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

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

1.4 同値変換 (Equivalence transformation)

s, t, u を変数とおく。

$\theta \perp stxyz$ 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】

$$s_1 x^{p-1} + t_1 y^{p-1} \equiv u_1 z^{p-1} \pmod{\theta}$$

$$s_2 z^{p-1} + t_2 x^{p-1} \equiv u_2 y^{p-1} \pmod{\theta}$$

$$s_3 y^{p-1} + t_3 z^{p-1} \equiv u_3 x^{p-1} \pmod{\theta}$$

このとき以下を同値変換の成立条件と呼び、以降 [] で示す。

$$[s_1 \equiv u_3 - t_2 \pmod{\theta}]$$

$$[t_1 \equiv u_2 - s_3 \pmod{\theta}]$$

$$[u_1 \equiv s_2 + t_3 \pmod{\theta}]$$

1.5 一般解の条件 (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。

$$s_1 x^{p-1} + t_2 x^{p-1} \equiv u_3 x^{p-1} \pmod{\theta}$$

$$s_3 y^{p-1} + t_1 y^{p-1} \equiv u_2 y^{p-1} \pmod{\theta}$$

$$s_2 z^{p-1} + t_3 z^{p-1} \equiv u_1 z^{p-1} \pmod{\theta}$$

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

$$s_1 x^{p-1} - t_2 y^{p-1} \equiv -u_3 z^{p-1} \pmod{\theta_1}$$

$$-s_3 x^{p-1} + t_1 y^{p-1} \equiv u_2 z^{p-1} \pmod{\theta_1}$$

$$-s_2 x^{p-1} + t_3 y^{p-1} \equiv u_1 z^{p-1} \pmod{\theta_1}$$

$\pmod{\theta_1}$ として

$$s_1 \equiv x, \quad t_1 \equiv y, \quad u_1 \equiv z$$

$$s_2 \equiv -x, \quad t_2 \equiv -y, \quad u_2 \equiv z$$

$$s_3 \equiv -x, \quad t_3 \equiv y, \quad u_3 \equiv -z$$

$$[x + z - y \equiv 0 \pmod{\delta}]$$

【General solution conditions】

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

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

(5)、(10)、(11) より

$$\begin{aligned}
Uz^{p-1} &\equiv -yx^{p-1} \pmod{\delta} \\
Ty^{p-1} &\equiv -zx^{p-1} \pmod{\delta} \\
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
x^p - yx^{p-1} &\equiv -zx^{p-1} \pmod{\theta_1} \\
x^p + zx^{p-1} &\equiv yx^{p-1} \pmod{\theta_2} \\
-yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \pmod{\delta} \\
(x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta}
\end{aligned} \tag{12}$$

(7)、(10)、(11) より

$$\begin{aligned}
-U'z^{p-1} &\equiv -xy^{p-1} \pmod{\delta} \\
-T'x^{p-1} &\equiv zy^{p-1} \pmod{\delta} \\
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
-xy^{p-1} + y^p &\equiv zy^{p-1} \pmod{\theta_1} \\
-zy^{p-1} + y^p &\equiv xy^{p-1} \pmod{\theta_2} \\
-xy^{p-1} \cdot zy^{p-1} &\equiv x^p z^p \pmod{\delta} \\
(y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta}
\end{aligned} \tag{13}$$

(9)、(10)、(11) より

$$\begin{aligned}
-U''y^{p-1} &\equiv -xz^{p-1} \pmod{\delta} \\
-T''x^{p-1} &\equiv yz^{p-1} \pmod{\delta} \\
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
-xz^{p-1} + yz^{p-1} &\equiv z^p \pmod{\theta_1} \\
yz^{p-1} - xz^{p-1} &\equiv z^p \pmod{\theta_2} \\
-xz^{p-1} \cdot yz^{p-1} &\equiv x^p y^p \pmod{\delta} \\
(z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta}
\end{aligned} \tag{14}$$

(12)(13)(14) より

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

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

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

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

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

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

$\delta \nmid 3AB$ なので

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

2つの因数のうち、一方は δ と互いに素である。 (15)

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

(13)(14) より

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

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。

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

$\theta_2 = \theta_3$ or θ_4 とする。

1.5.4 $-y \equiv z \equiv x \pmod{\theta_3}$ のとき

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

$\pmod{\theta_3}$ として

$$\begin{aligned}s_1'' &\equiv x^{p-1} \quad , \quad t_1'' \equiv y^{p-1} \quad , \quad u_1'' \equiv z^{p-1} \\ s_2'' &\equiv x^{p-1} \quad , \quad t_2'' \equiv -y^{p-1} \quad , \quad u_2'' \equiv -z^{p-1} \\ s_3'' &\equiv -x^{p-1} \quad , \quad t_3'' \equiv -y^{p-1} \quad , \quad u_3'' \equiv z^{p-1} \\ [x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_2}]\end{aligned}$$

【General solution conditions】

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

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

1.5.5 Common to $-y \not\equiv z \not\equiv x \pmod{\theta_4}$

(16)(17) より

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

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

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

(18)(19)(20) より

$$-y^3 \equiv z^3 \equiv x^3 \pmod{\theta_2}$$

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

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

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

$\theta_4 = \delta$ 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

$$x + z - y \not\equiv 0 \pmod{\theta_4}$$

$$\begin{aligned}
(12) \text{ より } (x^{p-1})^2 &\equiv y^{p-1}z^{p-1} \pmod{\theta_4} \\
(x^2)^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\theta_4} \\
(18) \text{ より } (-yz)^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\theta_4} \\
y^{p-1}z^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\theta_4}
\end{aligned}$$

$$\begin{aligned}
(13) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1}z^{p-1} \pmod{\theta_4} \\
(y^2)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\theta_4} \\
(19) \text{ より } (xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\theta_4} \\
x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\theta_4}
\end{aligned}$$

δ の定義に反する。

$$\begin{aligned}
(14) \text{ より } (z^{p-1})^2 &\equiv -x^{p-1}y^{p-1} \pmod{\theta_4} \\
(z^2)^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\theta_4} \\
(20) \text{ より } (-xy)^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\theta_4} \\
x^{p-1}y^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\theta_4}
\end{aligned}$$

δ の定義に反するので $\theta_4 \neq \delta$

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

1.5.6 まとめ

【General solution conditions】

$$\begin{aligned}
x^p + y^p &\equiv z^p \pmod{\theta_1} \\
&\Leftrightarrow \\
\begin{aligned}
x^p - yx^{p-1} &\equiv -zx^{p-1} \pmod{\theta_1} \\
-xy^{p-1} + y^p &\equiv zy^{p-1} \pmod{\theta_1} \\
-xz^{p-1} + yz^{p-1} &\equiv z^p \pmod{\theta_1}
\end{aligned} \\
x^p + y^p &\equiv z^p \pmod{\theta_4} \\
&\Leftrightarrow \\
\begin{aligned}
x^p + zx^{p-1} &\equiv yx^{p-1} \pmod{\theta_4} \\
-zzy^{p-1} + y^p &\equiv xy^{p-1} \pmod{\theta_4} \\
yz^{p-1} - xz^{p-1} &\equiv z^p \pmod{\theta_4}
\end{aligned}
\end{aligned} \tag{21}$$

$$\begin{aligned}
x^p + y^p &\equiv z^p \pmod{\theta_3} \\
&\Leftrightarrow \\
\begin{aligned}
x^p - y^{p-1}x &\equiv z^{p-1}x \pmod{\theta_3} \\
-x^{p-1}y + y^p &\equiv -z^{p-1}y \pmod{\theta_3} \\
x^{p-1}z - y^{p-1}z &\equiv z^p \pmod{\theta_3}
\end{aligned} \\
x^p + y^p &\equiv z^p \pmod{\theta_4} \\
&\Leftrightarrow \\
\begin{aligned}
x^p - z^{p-1}x &\equiv y^{p-1}x \pmod{\theta_4} \\
z^{p-1}y + y^p &\equiv x^{p-1}y \pmod{\theta_4} \\
-y^{p-1}z + x^{p-1}z &\equiv z^p \pmod{\theta_4}
\end{aligned}
\end{aligned} \tag{22}$$

【Equivalence transformation】

$$\begin{aligned}
-x^{p-1} &\equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1} \\
xx^{p-1} + yy^{p-1} &\equiv zz^{p-1} \pmod{\theta_1} \\
-xx^{p-1} - yx^{p-1} &\equiv zy^{p-1} \pmod{\theta_1} \\
-xy^{p-1} + yz^{p-1} &\equiv -zx^{p-1} \pmod{\theta_1} \\
&\text{or} \\
x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_4} \\
xx^{p-1} + yy^{p-1} &\equiv zz^{p-1} \pmod{\theta_4} \\
yz^{p-1} + zx^{p-1} &\equiv xy^{p-1} \pmod{\theta_4} \\
-zy^{p-1} - xz^{p-1} &\equiv yx^{p-1} \pmod{\theta_4}
\end{aligned}$$

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

$x - y + k_1 \equiv -z + k_1 \pmod{\delta}$ より

Definition 13 $-y + k_1 \equiv -l_1y \pmod{\delta}$, $-z + k_1 \equiv -m_1z \pmod{\delta}$, $l_1m_1 \perp \delta$

$$-l_1yx^{p-1} \cdot -m_1zx^{p-1} \equiv y^p z^p \pmod{\delta}$$

$x - l_1y \equiv -m_1z \pmod{\delta}$ より

$$\begin{aligned} x^p - l_1yx^{p-1} &\equiv -m_1zx^{p-1} \pmod{\delta} \\ -l_1^{-1}xy^{p-1} + y^p &\equiv l_1^{-1}m_1zy^{p-1} \pmod{\delta} \\ -m_1^{-1}xz^{p-1} + l_1m_1^{-1}yz^{p-1} &\equiv z^p \pmod{\delta} \end{aligned} \quad (23)$$

ここで

$$\begin{aligned} -l_1yx^{p-1} \equiv y^p \pmod{\delta} &\Rightarrow -m_1zx^{p-1} \equiv z^p \pmod{\delta} \\ -x^{p-1} \equiv l_1^{-1}y^{p-1} \pmod{\delta} &\Rightarrow -x^{p-1} \equiv m_1^{-1}z^{p-1} \pmod{\delta} \end{aligned}$$

であるから自動的に

$$\begin{aligned} -l_1^{-1}xy^{p-1} \equiv x^p \pmod{\delta} , \quad l_1^{-1}m_1zy^{p-1} &\equiv z^p \pmod{\delta} \\ -m_1^{-1}xz^{p-1} \equiv x^p \pmod{\delta} , \quad l_1m_1^{-1}yz^{p-1} &\equiv y^p \pmod{\delta} \end{aligned}$$

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

$$\begin{aligned} -x^{p-1} \equiv l_1^{-1}y^{p-1} \equiv m_1^{-1}z^{p-1} \pmod{\delta} \\ \text{or} \\ -x^{p-1} \not\equiv l_1^{-1}y^{p-1} \not\equiv m_1^{-1}z^{p-1} \pmod{\delta} \end{aligned}$$

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

(23) より

$$\begin{aligned} -l_1yx^{p-1} \cdot -m_1zx^{p-1} &\equiv y^p z^p \pmod{\delta} \\ l_1m_1 (x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ (x^{p-1})^2 &\equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \quad (24)$$

$$\begin{aligned} -l_1^{-1}xy^{p-1} \cdot l_1^{-1}m_1zy^{p-1} &\equiv x^p z^p \pmod{\delta} \\ l_1^{-2}m_1 (y^{p-1})^2 &\equiv -x^{p-1}z^{p-1} \pmod{\delta} \\ (l_1^{-1}y^{p-1})^2 &\equiv -m_1^{-1}x^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \quad (25)$$

$$\begin{aligned} -m_1^{-1}xz^{p-1} \cdot l_1m_1^{-1}yz^{p-1} &\equiv x^p y^p \pmod{\delta} \\ l_1m_1^{-2} (z^{p-1})^2 &\equiv -x^{p-1}y^{p-1} \pmod{\delta} \\ (m_1^{-1}z^{p-1})^2 &\equiv -l_1^{-1}x^{p-1}y^{p-1} \pmod{\delta} \end{aligned} \quad (26)$$

(24)(25)(26) より

$$\begin{aligned}
-(x^{p-1})^3 &\equiv (l_1^{-1}y^{p-1})^3 \equiv (m_1^{-1}z^{p-1})^3 \pmod{\delta} \\
(m_1^{-1}z^{p-1})^3 - (l_1^{-1}y^{p-1})^3 &\equiv (m_1^{-1}z^{p-1} - l_1^{-1}y^{p-1})((m_1^{-1}z^{p-1})^2 + l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} + (l_1^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta} \\
(x^{p-1})^3 + (m_1^{-1}z^{p-1})^3 &\equiv (x^{p-1} + m_1^{-1}z^{p-1})((x^{p-1})^2 - m_1^{-1}x^{p-1}z^{p-1} + (m_1^{-1}z^{p-1})^2) \equiv 0 \pmod{\delta} \\
(x^{p-1})^3 + (l_1^{-1}y^{p-1})^3 &\equiv (x^{p-1} + l_1^{-1}y^{p-1})((x^{p-1})^2 - l_1^{-1}x^{p-1}y^{p-1} + (l_1^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta}
\end{aligned}$$

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

(25)(26) より

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

【General solution conditions】

$$\begin{aligned}
x^p - l_1^{-1}y^{p-1}x &\equiv m_1^{-1}z^{p-1}x \pmod{\theta_4} \\
-l_1x^{p-1}y + y^p &\equiv -l_1m_1^{-1}z^{p-1}y \pmod{\theta_4} \\
m_1x^{p-1}z - l_1^{-1}m_1y^{p-1}z &\equiv z^p \pmod{\theta_4}
\end{aligned} \tag{27}$$

(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。

$$\begin{aligned}
-l_1^{-1}y^{p-1}x \cdot m_1^{-1}z^{p-1}x &\equiv y^p z^p \pmod{\theta_4} \\
x^2 &\equiv -l_1m_1yz \pmod{\theta_4}
\end{aligned} \tag{28}$$

$$\begin{aligned}
-l_1x^{p-1}y \cdot -l_1m_1^{-1}z^{p-1}y &\equiv x^p z^p \pmod{\theta_4} \\
y^2 &\equiv l_1^{-2}m_1xz \pmod{\theta_4}
\end{aligned} \tag{29}$$

$$\begin{aligned}
m_1x^{p-1}z \cdot -l_1^{-1}m_1y^{p-1}z &\equiv x^p y^p \pmod{\theta_4} \\
z^2 &\equiv -l_1m_1^{-2}xy \pmod{\theta_4}
\end{aligned} \tag{30}$$

(28)(29)(30) より

$$-l_1^3y^3 \equiv m_1^3z^3 \equiv x^3 \pmod{\theta_4}$$

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

(15) より二つの因数の一方が解となる。

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

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

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

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

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

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

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

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

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

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

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

$l_1^p m_1^p \equiv 1 \pmod{\theta_4}$ なので

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

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

$$x + k_2 - y \equiv -z + k_2 \pmod{\delta} \text{ より}$$

Definition 14 $x + k_2 \equiv l_2 x \pmod{\delta}$, $-z + k_2 \equiv -m_2 z \pmod{\delta}$, $l_2 m_2 \perp \delta$

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

$$l_2 x - y \equiv -m_2 z \pmod{\delta} \text{ より}$$

$$\begin{aligned} x^p - l_2^{-1} y x^{p-1} &\equiv -l_2^{-1} m_2 z x^{p-1} \pmod{\delta} \\ -l_2 x y^{p-1} + y^p &\equiv m_2 z y^{p-1} \pmod{\delta} \\ -l_2 m_2^{-1} x z^{p-1} + m_2^{-1} y z^{p-1} &\equiv z^p \pmod{\delta} \end{aligned} \quad (34)$$

ここで

$$\begin{aligned} -l_2 x y^{p-1} \equiv x^p \pmod{\delta} &\Rightarrow m_2 z y^{p-1} \equiv z^p \pmod{\delta} \\ -l_2 y^{p-1} \equiv x^{p-1} \pmod{\delta} &\Rightarrow m_2 y^{p-1} \equiv z^{p-1} \pmod{\delta} \end{aligned}$$

であるから自動的に

$$\begin{aligned} -l_2^{-1} y x^{p-1} \equiv y^p \pmod{\delta} \text{ , } -l_2^{-1} m_2 z x^{p-1} &\equiv z^p \pmod{\delta} \\ -l_2 m_2^{-1} x z^{p-1} \equiv x^p \pmod{\delta} \text{ , } m_2^{-1} y z^{p-1} &\equiv y^p \pmod{\delta} \end{aligned}$$

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

$$\begin{aligned} -l_2^{-1} x^{p-1} \equiv y^{p-1} \equiv m_2^{-1} z^{p-1} \pmod{\delta} \\ \text{or} \\ -l_2^{-1} x^{p-1} \not\equiv y^{p-1} \not\equiv m_2^{-1} z^{p-1} \pmod{\delta} \end{aligned}$$

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

(34) より

$$\begin{aligned} -l_2^{-1} y x^{p-1} \cdot -l_2^{-1} m_2 z x^{p-1} &\equiv y^p z^p \pmod{\delta} \\ l_2^{-2} m_2 (x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ (l_2^{-1} x^{p-1})^2 &\equiv m_2^{-1} y^{p-1} z^{p-1} \pmod{\delta} \end{aligned} \quad (35)$$

$$\begin{aligned} -l_2 x y^{p-1} \cdot m_2 z y^{p-1} &\equiv x^p z^p \pmod{\delta} \\ l_2 m_2 (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \\ (y^{p-1})^2 &\equiv -l_2^{-1} m_2^{-1} x^{p-1} z^{p-1} \pmod{\delta} \end{aligned} \quad (36)$$

$$\begin{aligned} -l_2 m_2^{-1} x z^{p-1} \cdot m_2^{-1} y z^{p-1} &\equiv x^p y^p \pmod{\delta} \\ l_2 m_2^{-2} (z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \\ (m_2^{-1} z^{p-1})^2 &\equiv -l_2^{-1} x^{p-1} y^{p-1} \pmod{\delta} \end{aligned} \quad (37)$$

(35)(36)(37) より

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

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

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

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

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

(35)(37) より

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

【General solution conditions】

$$\begin{aligned} x^p - l_2y^{p-1}x &\equiv l_2m_2^{-1}z^{p-1}x \pmod{\theta_4} \\ -l_2^{-1}x^{p-1}y + y^p &\equiv -m_2^{-1}z^{p-1}y \pmod{\theta_4} \\ l_2^{-1}m_2x^{p-1}z - m_2y^{p-1}z &\equiv z^p \pmod{\theta_4} \end{aligned} \quad (38)$$

(38) より

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

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

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

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

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

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

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

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

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

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

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

よって $m_2^p + l_2^p \not\equiv 0 \pmod{\theta_4}$

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

(23)(34) より

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

$l_2^p m_2^p \equiv -1 \pmod{\theta_4}$ なので

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

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

$$x - k_3 - y + k_3 \equiv -z \pmod{\delta} \text{ より}$$

Definition 15 $x - k_3 \equiv m_3 x \pmod{\delta}$, $-y + k_3 \equiv -l_3 y \pmod{\delta}$, $l_3 m_3 \perp \delta$

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

$$m_3 x - l_3 y \equiv -z \pmod{\delta} \text{ より}$$

$$\begin{aligned} x^p - l_3 m_3^{-1} y x^{p-1} &\equiv -m_3^{-1} z x^{p-1} \pmod{\delta} \\ -l_3^{-1} m_3 x y^{p-1} + y^p &\equiv l_3^{-1} z y^{p-1} \pmod{\delta} \\ -m_3 x z^{p-1} + l_3 y z^{p-1} &\equiv z^p \pmod{\delta} \end{aligned} \quad (45)$$

ここで

$$\begin{aligned} -m_3 x z^{p-1} \equiv x^p \pmod{\delta} &\Rightarrow l_3 y z^{p-1} \equiv y^p \pmod{\delta} \\ -m_3 z^{p-1} \equiv x^{p-1} \pmod{\delta} &\Rightarrow l_3 z^{p-1} \equiv y^{p-1} \pmod{\delta} \end{aligned}$$

であるから自動的に

$$\begin{aligned} -l_3 m_3^{-1} y x^{p-1} &\equiv y^p \pmod{\delta} , \quad -m_3^{-1} z x^{p-1} \equiv z^p \pmod{\delta} \\ -l_3^{-1} m_3 x y^{p-1} &\equiv x^p \pmod{\delta} , \quad l_3^{-1} z y^{p-1} \equiv z^p \pmod{\delta} \end{aligned}$$

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

$$\begin{aligned} -m_3^{-1} x^{p-1} &\equiv l_3^{-1} y^{p-1} \equiv z^{p-1} \pmod{\delta} \\ \text{or} \\ -m_3^{-1} x^{p-1} &\not\equiv l_3^{-1} y^{p-1} \not\equiv z^{p-1} \pmod{\delta} \end{aligned}$$

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

(45) より

$$\begin{aligned} -l_3 m_3^{-1} y x^{p-1} \cdot -m_3^{-1} z x^{p-1} &\equiv y^p z^p \pmod{\delta} \\ l_3 m_3^{-2} (x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ (m_3^{-1} x^{p-1})^2 &\equiv l_3^{-1} y^{p-1} z^{p-1} \pmod{\delta} \end{aligned} \quad (46)$$

$$\begin{aligned} -l_3^{-1} m_3 x y^{p-1} \cdot l_3^{-1} z y^{p-1} &\equiv x^p z^p \pmod{\delta} \\ l_3^{-2} m_3 (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \\ (l_3^{-1} y^{p-1})^2 &\equiv -m_3^{-1} x^{p-1} z^{p-1} \pmod{\delta} \end{aligned} \quad (47)$$

$$\begin{aligned} -m_3 x z^{p-1} \cdot l_3 y z^{p-1} &\equiv x^p y^p \pmod{\delta} \\ l_3 m_3 (z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \\ (z^{p-1})^2 &\equiv -l_3^{-1} m_3^{-1} x^{p-1} y^{p-1} \pmod{\delta} \end{aligned} \quad (48)$$

(46)(47)(48) より

$$\begin{aligned}
-(m_3^{-1}x^{p-1})^3 &\equiv (l_3^{-1}y^{p-1})^3 \equiv (z^{p-1})^3 \pmod{\delta} \\
(z^{p-1})^3 - (l_3^{-1}y^{p-1})^3 &\equiv (z^{p-1} - l_3^{-1}y^{p-1})((z^{p-1})^2 + l_3^{-1}y^{p-1}z^{p-1} + (l_3^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta} \\
(m_3^{-1}x^{p-1})^3 + (z^{p-1})^3 &\equiv (m_3^{-1}x^{p-1} + z^{p-1})((m_3^{-1}x^{p-1})^2 - m_3^{-1}x^{p-1}z^{p-1} + (z^{p-1})^2) \equiv 0 \pmod{\delta} \\
(m_3^{-1}x^{p-1})^3 + (l_3^{-1}y^{p-1})^3 &\equiv (m_3^{-1}x^{p-1} + l_3^{-1}y^{p-1})((m_3^{-1}x^{p-1})^2 - l_3^{-1}m_3^{-1}x^{p-1}y^{p-1} + (l_3^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta}
\end{aligned}$$

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

(46)(47) より

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

【General solution conditions】

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

(49) より

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

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

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

$$\begin{aligned}
(46) \text{ より } (x^{p-1})^2 &\equiv l_3^{-1} m_3^2 y^{p-1} z^{p-1} \pmod{\theta_4} \\
(x^2)^{p-1} &\equiv l_3^{-1} m_3^2 y^{p-1} z^{p-1} \pmod{\theta_4} \\
(50) \text{ より } (-l_3 m_3^{-2} y z)^{p-1} &\equiv l_3^{-1} m_3^2 y^{p-1} z^{p-1} \pmod{\theta_4} \\
l_3^{p-1} m_3^{-2p+2} y^{p-1} z^{p-1} &\equiv l_3^{-1} m_3^2 y^{p-1} z^{p-1} \pmod{\theta_4} \\
l_3^p m_3^{-2p} &\equiv 1 \pmod{\theta_4}
\end{aligned}$$

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

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

$$\begin{aligned}
l_3^p m_3^p &\equiv -1 \pmod{\theta_4} \\
l_3^{-2p} m_3^p &\equiv -1 \pmod{\theta_4} \\
l_3^p m_3^{-2p} &\equiv 1 \pmod{\theta_4}
\end{aligned}$$

$$\begin{aligned}
-m_3^{3p} &\equiv l_3^{3p} \pmod{\theta_4} \\
m_3^{3p} + l_3^{3p} &\equiv (m_3^p + l_3^p)(m_3^{2p} - l_3^p m_3^p + l_3^{2p}) \pmod{\theta_4}
\end{aligned}$$

$$\begin{aligned}
-m_3^p &\equiv l_3^{2p} \pmod{\theta_4} \\
l_3^p &\equiv m_3^{2p} \pmod{\theta_4}
\end{aligned}$$

$$\begin{aligned}
-l_3^p - m_3^p &\equiv l_3^{2p} - m_3^{2p} \pmod{\theta_4} \\
-(l_3^p + m_3^p) &\equiv (l_3^p + m_3^p)(l_3^p - m_3^p) \pmod{\theta_4} \\
-1 &\equiv l_3^p - m_3^p \pmod{\theta_4}
\end{aligned}$$

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

よって $m_3^p + l_3^p \not\equiv 0 \pmod{\theta_4}$

$$\begin{aligned}
l_3^p - m_3^p &\equiv -1 \pmod{\theta_4} \\
l_3^{2p} - l_3^p m_3^p &\equiv -l_3^p \pmod{\theta_4} \\
l_3^{2p} + l_3^p + 1 &\equiv 0 \pmod{\theta_4}
\end{aligned}$$

(23)(34)(45) より

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

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

$l_3^p m_3^p \equiv -1 \pmod{\theta_4}$ なので

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

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

1.6.7 Cycle

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

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

1.6.8 A splice

(28) より

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

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

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

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

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

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

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

(42)(53) より

$$\begin{aligned}
-y &\equiv xl_2 \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_4} \\
-z &\equiv xm_3 \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_4} \\
-y^p &\equiv x^p l_2^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta_4} \\
-z^p &\equiv x^p m_3^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta_4}
\end{aligned}$$

(57) より

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

(43)(56) より

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

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

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

(40) より

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

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

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

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

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

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

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

(42)(54) より

$$\begin{aligned}
x &\equiv yl_1 \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_4} \\
-z &\equiv yl_3 \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_4} \\
x^p &\equiv y^p l_1^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta_4} \\
-z^p &\equiv y^p l_3^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta_4}
\end{aligned}$$

(58) より

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

(32)(55) より

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

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

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

(52) より

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

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

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

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

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

(57) より $\pm$ の調整

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

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

(54)(53) より

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

(59) より

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

(44)(33) より

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

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

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

1.6.9 $p = 6n + 1$ のとき

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

(28)(40)(52) より

$$\begin{aligned}
x^2 &\equiv -l_1 m_1 y z \pmod{\theta_4} \\
x^2 &\equiv -y z \pmod{\theta_4}
\end{aligned}$$

$$\begin{aligned}
y^2 &\equiv l_2 m_2 x z \pmod{\theta_4} \\
y^2 &\equiv -x z \pmod{\theta_4}
\end{aligned}$$

$$\begin{aligned}
z^2 &\equiv -l_3 m_3 x y \pmod{\theta_4} \\
z^2 &\equiv x y \pmod{\theta_4}
\end{aligned}$$

$$-z^3 \equiv x^3 \equiv y^3 \pmod{\theta_4}$$

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

$x + z - y \equiv 0 \pmod{\theta_4}$ ないので

$$x + z \not\equiv 0 \pmod{\theta_4}$$

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

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 $n = 0$, $p = 3$ 、 $x^3 + y^3 \equiv z^3 \pmod{\theta_4}$

$$(x + z - y)^3 \equiv x^3 + z^3 - y^3 - 3x^2y + 3x^2z + 3xy^2 + 3xz^2 + 3y^2z - 3yz^2 - 6xyz \pmod{\theta_4}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(-x^2y + x^2z + xy^2 + xz^2 + y^2z - yz^2 - 2xyz) \pmod{\theta_4}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(-y(x^2 + 2xz + z^2) + (x + z)xz + (x + z)y^2) \pmod{\theta_4}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(-y(x + z)^2 + (x + z)xz + (x + z)y^2) \pmod{\theta_4}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(x + z)(-xy - yz + xz + y^2) \pmod{\theta_4}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(x + z)(-x(y - z) + y(y - z)) \pmod{\theta_4}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(x + z)(y - z)(y - x) \pmod{\theta_4}$$

$$0 \equiv 2x^3 + 3yxz \pmod{\theta_4}$$

$$-2x^2 \equiv 3yz \pmod{\theta_4}$$

(28) より

$$2l_1m_1yz \equiv 3yz \pmod{\theta_4}$$

$$2l_1m_1 \equiv 3 \pmod{\theta_4}$$

$$2^p l_1^p m_1^p \equiv 3^p \pmod{\theta_4}$$

(31) より

$$2^3 \equiv 3^3 \pmod{\theta_4}$$

$$8 \equiv 27 \pmod{\theta_4}$$

$$0 \equiv 19 \pmod{\theta_4}$$

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

$x - y + k_1 \equiv -z + k_1 \pmod{\delta}$ より

$$-y + k_1 \equiv -l_1y \pmod{\delta}, \quad -z + k_1 \equiv -m_1z \pmod{\delta}$$

$$\begin{aligned} x & -l_1y & \equiv -m_1z & \pmod{\delta} \\ x^p & -l_1yx^{p-1} & \equiv -m_1zx^{p-1} & \pmod{\delta} \\ x^p & -z^p & \equiv -y^p & \pmod{\theta_4} \\ x^p & +(-y + k_1)x^{p-1} & \equiv (-z + k_1)x^{p-1} & \pmod{\theta_4} \end{aligned}$$

$$\begin{aligned} x^p & +y^p & \equiv z^p & \pmod{\theta_4} \\ x^p & +(z - k_1)x^{p-1} & \equiv (y - k_1)x^{p-1} & \pmod{\theta_4} \\ x^p & +m_1zx^{p-1} & \equiv l_1yx^{p-1} & \pmod{\theta_4} \\ x & +m_1z & \equiv l_1y & \pmod{\theta_4} \end{aligned}$$

Definition 16 $z - k_1 \equiv q_1y \pmod{\delta}$, $y - k_1 \equiv r_1z \pmod{\delta}$, $q_1r_1 \perp \delta$

$$\begin{aligned} m_1z & \equiv q_1y \pmod{\delta} \\ l_1y & \equiv r_1z \pmod{\delta} \\ x + q_1y & \equiv r_1z \pmod{\delta} \end{aligned}$$

$$\begin{aligned} x^p & +q_1yx^{p-1} & \equiv r_1zx^{p-1} & \pmod{\delta} \\ q_1^{-1}xy^{p-1} & +y^p & \equiv q_1^{-1}r_1zy^{p-1} & \pmod{\delta} \\ r_1^{-1}xz^{p-1} & +q_1r_1^{-1}yz^{p-1} & \equiv z^p & \pmod{\delta} \end{aligned} \tag{60}$$

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

(60) より

$$\begin{aligned} q_1yx^{p-1} \cdot r_1zx^{p-1} & \equiv y^p z^p \pmod{\delta} \\ q_1r_1(x^{p-1})^2 & \equiv y^{p-1}z^{p-1} \pmod{\delta} \\ (x^{p-1})^2 & \equiv q_1^{-1}r_1^{-1}y^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \tag{61}$$

$$\begin{aligned} q_1^{-1}xy^{p-1} \cdot q_1^{-1}r_1zy^{p-1} & \equiv x^p z^p \pmod{\delta} \\ q_1^{-2}r_1(y^{p-1})^2 & \equiv x^{p-1}z^{p-1} \pmod{\delta} \\ (q_1^{-1}y^{p-1})^2 & \equiv r_1^{-1}x^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \tag{62}$$

$$\begin{aligned} r_1^{-1}xz^{p-1} \cdot q_1r_1^{-1}yz^{p-1} & \equiv x^p y^p \pmod{\delta} \\ q_1r_1^{-2}(z^{p-1})^2 & \equiv x^{p-1}y^{p-1} \pmod{\delta} \\ (r_1^{-1}z^{p-1})^2 & \equiv q_1^{-1}x^{p-1}y^{p-1} \pmod{\delta} \end{aligned} \tag{63}$$

(61)(62)(63) より

$$\begin{aligned}
(x^{p-1})^3 &\equiv (q_1^{-1}y^{p-1})^3 \equiv (r_1^{-1}z^{p-1})^3 \pmod{\delta} \\
(r_1^{-1}z^{p-1})^3 - (q_1^{-1}y^{p-1})^3 &\equiv (r_1^{-1}z^{p-1} - q_1^{-1}y^{p-1})((r_1^{-1}z^{p-1})^2 + q_1^{-1}r_1^{-1}y^{p-1}z^{p-1} + (q_1^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta} \\
(x^{p-1})^3 - (r_1^{-1}z^{p-1})^3 &\equiv (x^{p-1} - r_1^{-1}z^{p-1})((x^{p-1})^2 + r_1^{-1}x^{p-1}z^{p-1} + (r_1^{-1}z^{p-1})^2) \equiv 0 \pmod{\delta} \\
(x^{p-1})^3 - (q_1^{-1}y^{p-1})^3 &\equiv (x^{p-1} - q_1^{-1}y^{p-1})((x^{p-1})^2 + q_1^{-1}x^{p-1}y^{p-1} + (q_1^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta}
\end{aligned}$$

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

(62)(63) より

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

【General solution conditions】

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

(64) より

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

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

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

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

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

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

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

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

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

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

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

$r_1^p - q_1^p \not\equiv 0 \pmod{\theta_1}$ ないので $r_1 \equiv -1 \pmod{\theta_1}$, $q_1 \equiv -1 \pmod{\theta_1}$ のとき
 $x^p + y^p \not\equiv z^p \pmod{\theta_1}$

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

$q_1^p r_1^p \equiv 1 \pmod{\theta_1}$ ないので

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

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

$$x + k_2 - y \equiv -z + k_2 \pmod{\delta} \text{ より}$$

$$x + k_2 \equiv l_2 x \pmod{\delta}, \quad -z + k_2 \equiv -m_2 z \pmod{\delta}$$

$$l_2 x - y \equiv -m_2 z \pmod{\delta}$$

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

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

Definition 17 $-z + k_2 \equiv q_2 x \pmod{\delta}$, $x + k_2 \equiv r_2 z \pmod{\delta}$, $q_2 r_2 \perp \delta$

$$-m_2 z \equiv q_2 x \pmod{\delta}$$

$$l_2 x \equiv r_2 z \pmod{\delta}$$

$$q_2 x + y \equiv r_2 z \pmod{\delta}$$

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

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

(71) より

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

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

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

(72)(73)(74) より

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

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

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

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

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

(72)(74) より

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

【General solution conditions】

$$\begin{aligned} x^p + q_2y^{p-1}x &\equiv -q_2r_2^{-1}z^{p-1}x \pmod{\theta_1} \\ q_2^{-1}x^{p-1}y + y^p &\equiv -r_2^{-1}z^{p-1}y \pmod{\theta_1} \\ -q_2^{-1}r_2x^{p-1}z - r_2y^{p-1}z &\equiv z^p \pmod{\theta_1} \end{aligned} \quad (75)$$

(75) より

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

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

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

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

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

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

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

(71)(60) より

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

であるから (69) より

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

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

$$x - k_3 - y + k_3 \equiv -z \pmod{\delta} \text{ より}$$

$$x - k_3 \equiv m_3x \pmod{\delta}, \quad -y + k_3 \equiv -l_3y \pmod{\delta}$$

$$m_3x \quad -l_3y \quad \equiv -z \pmod{\delta}$$

$$\begin{aligned} -m_3xz^{p-1} \quad +l_3yz^{p-1} &\equiv z^p \pmod{\delta} \\ y^p \quad +x^p &\equiv z^p \pmod{\theta_4} \\ (-x+k_3)z^{p-1} \quad +(y-k_3)z^{p-1} &\equiv z^p \pmod{\theta_4} \end{aligned}$$

$$\begin{aligned} x^p \quad +y^p &\equiv z^p \pmod{\theta_4} \\ (y-k_3)z^{p-1} \quad +(-x+k_3)z^{p-1} &\equiv z^p \pmod{\theta_4} \\ +l_3yz^{p-1} \quad -m_3xz^{p-1} &\equiv z^p \pmod{\theta_4} \\ -l_3y \quad +m_3x &\equiv -z \pmod{\theta_4} \end{aligned}$$

Definition 18 $y - k_3 \equiv q_3x \pmod{\delta}$, $-x + k_3 \equiv r_3y \pmod{\delta}$, $q_3r_3 \perp \delta$

$$l_3y \equiv q_3x \pmod{\delta}$$

$$-m_3x \equiv r_3y \pmod{\delta}$$

$$q_3x + r_3y \equiv z \pmod{\delta}$$

$$\begin{aligned} x^p \quad +q_3^{-1}r_3yx^{p-1} &\equiv q_3^{-1}zx^{p-1} \pmod{\delta} \\ q_3r_3^{-1}xy^{p-1} \quad +y^p &\equiv r_3^{-1}zy^{p-1} \pmod{\delta} \\ q_3xz^{p-1} \quad +r_3yz^{p-1} &\equiv z^p \pmod{\delta} \end{aligned} \tag{82}$$

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

(82) より

$$\begin{aligned} q_3^{-1}r_3yx^{p-1} \cdot q_3^{-1}zx^{p-1} &\equiv y^pz^p \pmod{\delta} \\ q_3^{-2}r_3(x^{p-1})^2 &\equiv y^{p-1}z^{p-1} \pmod{\delta} \\ (q_3^{-1}x^{p-1})^2 &\equiv r_3^{-1}y^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \tag{83}$$

$$\begin{aligned} q_3r_3^{-1}xy^{p-1} \cdot r_3^{-1}zy^{p-1} &\equiv x^pz^p \pmod{\delta} \\ q_3r_3^{-2}(y^{p-1})^2 &\equiv x^{p-1}z^{p-1} \pmod{\delta} \\ (r_3^{-1}y^{p-1})^2 &\equiv q_3^{-1}x^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \tag{84}$$

$$\begin{aligned} q_3xz^{p-1} \cdot r_3yz^{p-1} &\equiv x^py^p \pmod{\delta} \\ q_3r_3(z^{p-1})^2 &\equiv x^{p-1}y^{p-1} \pmod{\delta} \\ (z^{p-1})^2 &\equiv q_3^{-1}r_3^{-1}x^{p-1}y^{p-1} \pmod{\delta} \end{aligned} \tag{85}$$

(83)(84)(85) より

$$\begin{aligned}
(q_3^{-1}x^{p-1})^3 &\equiv (r_3^{-1}y^{p-1})^3 \equiv (z^{p-1})^3 \pmod{\delta} \\
(z^{p-1})^3 - (r_3^{-1}y^{p-1})^3 &\equiv (z^{p-1} - r_3^{-1}y^{p-1})((z^{p-1})^2 + r_3^{-1}y^{p-1}z^{p-1} + (r_3^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta} \\
(q_3^{-1}x^{p-1})^3 - (z^{p-1})^3 &\equiv (q_3^{-1}x^{p-1} - z^{p-1})((q_3^{-1}x^{p-1})^2 + q_3^{-1}x^{p-1}z^{p-1} + (z^{p-1})^2) \equiv 0 \pmod{\delta} \\
(q_3^{-1}x^{p-1})^3 - (r_3^{-1}y^{p-1})^3 &\equiv (q_3^{-1}x^{p-1} - r_3^{-1}y^{p-1})((q_3^{-1}x^{p-1})^2 + q_3^{-1}r_3^{-1}x^{p-1}y^{p-1} + (r_3^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta}
\end{aligned}$$

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

(83)(84) より

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

【General solution conditions】

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

(86) より

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

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

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

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

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

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

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

(60)(71)(82) より

$$\begin{aligned}
r_1^{-1} x z^{p-1} &\equiv q_3 x z^{p-1} \pmod{\delta} \\
r_1^{-1} &\equiv q_3 \pmod{\delta} \\
1 &\equiv q_3^p r_1^p \pmod{\delta}
\end{aligned} \tag{90}$$

$$\begin{aligned}
r_3^{-1} z y^{p-1} &\equiv r_2 z y^{p-1} \pmod{\delta} \\
r_3^{-1} &\equiv r_2 \pmod{\delta}
\end{aligned} \tag{91}$$

(70) より

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

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

1.7.7 A splice

(65) より

$$\begin{aligned}
x^2 &\equiv -q_1 r_1 y z \pmod{\theta_1} \\
-x^2 &\equiv q_1 y \cdot r_1 z \pmod{\theta_1} \\
-x^2 &\equiv (z - k_1)(y - k_1) \pmod{\theta_1} \\
-x^2 &\equiv yz - (y + z)k_1 + k_1^2 \pmod{\theta_1} \\
0 &\equiv k_1^2 - (y + z)k_1 + yz + x^2 \pmod{\theta_1} \\
\\
k_1 &\equiv \frac{y + z \pm \sqrt{(y + z)^2 - 4(yz + x^2)}}{2} \pmod{\theta_1} \\
k_1 &\equiv \frac{y + z \pm \sqrt{(y - z)^2 - 4x^2}}{2} \pmod{\theta_1} \\
k_1 &\equiv \frac{y + z \pm \sqrt{x^2 - 4x^2}}{2} \pmod{\theta_1} \\
k_1 &\equiv \frac{y + z \pm \sqrt{-3x^2}}{2} \pmod{\theta_1} \\
\\
-y + k_1 &\equiv \frac{-y + z \pm \sqrt{-3x^2}}{2} \pmod{\theta_1} \\
-z + k_1 &\equiv \frac{y - z \pm \sqrt{-3x^2}}{2} \pmod{\theta_1} \\
\\
-r_1 z &\equiv x \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
-q_1 y &\equiv x \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
\\
-r_1 z x^{p-1} &\equiv x^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
-q_1 y x^{p-1} &\equiv x^p \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
\\
y^p &\equiv x^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
z^p &\equiv x^p \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1}
\end{aligned} \tag{94}$$

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

(90)(79) より

$$\begin{aligned}
-z &\equiv xq_3 \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
-y &\equiv xq_2 \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
-z^p &\equiv x^p q_3^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta_1} \\
-y^p &\equiv x^p q_2^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta_1}
\end{aligned}$$

(94) より

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

(92)(80) より

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

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

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

(77) より

$$\begin{aligned}
y^2 &\equiv -q_2 r_2 x z \pmod{\theta_1} \\
-y^2 &\equiv q_2 x \cdot r_2 z \pmod{\theta_1} \\
-y^2 &\equiv (-z + k_2)(x + k_2) \pmod{\theta_1} \\
-y^2 &\equiv -xz + (x - z)k_2 + k_2^2 \pmod{\theta_1} \\
0 &\equiv k_2^2 + (x - z)k_2 - xz + y^2 \pmod{\theta_1} \\
\\
k_2 &\equiv \frac{z - x \pm \sqrt{(x - z)^2 - 4(-xz + y^2)}}{2} \pmod{\theta_1} \\
k_2 &\equiv \frac{z - x \pm \sqrt{(x + z)^2 - 4y^2}}{2} \pmod{\theta_1} \\
k_2 &\equiv \frac{z - x \pm \sqrt{y^2 - 4y^2}}{2} \pmod{\theta_1} \\
k_2 &\equiv \frac{z - x \pm \sqrt{-3y^2}}{2} \pmod{\theta_1} \\
\\
x + k_2 &\equiv \frac{z + x \pm \sqrt{-3y^2}}{2} \pmod{\theta_1} \\
-z + k_2 &\equiv \frac{-z - x \pm \sqrt{-3y^2}}{2} \pmod{\theta_1} \\
\\
r_2 z &\equiv y \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
q_2 x &\equiv y \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
\\
r_2 z y^{p-1} &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
q_2 x y^{p-1} &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
\\
-x^p &\equiv y^p \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta_1} \\
-z^p &\equiv y^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta_1}
\end{aligned} \tag{95}$$

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

(91)(79) より

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

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

(95) より

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

(93)(69) より

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

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

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

(89) より

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

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

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

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

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

(94) より $\pm$ の調整

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

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

(90)(91) より

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

(96) より

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

(70)(81) より

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

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

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

1.7.8 $p = 6n + 1$ のとき

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

(65)(77)(89) より

$$\begin{aligned}
x^2 &\equiv -q_1 r_1 y z \pmod{\theta_1} \\
x^2 &\equiv -y z \pmod{\theta_1}
\end{aligned}$$

$$\begin{aligned}
y^2 &\equiv -q_2 r_2 x z \pmod{\theta_1} \\
y^2 &\equiv -x z \pmod{\theta_1}
\end{aligned}$$

$$\begin{aligned}
z^2 &\equiv q_3 r_3 x y \pmod{\theta_1} \\
z^2 &\equiv x y \pmod{\theta_1}
\end{aligned}$$

$$-z^3 \equiv x^3 \equiv y^3 \pmod{\theta_1}$$

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

$x + z - y \equiv 0 \pmod{\theta_1}$ ないので

$$x + z \not\equiv 0 \pmod{\theta_1}$$

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

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 $n = 0$, $p = 3$ 、 $x^3 + y^3 \equiv z^3 \pmod{\theta_1}$

$$(x + z - y)^3 \equiv x^3 + z^3 - y^3 - 3x^2y + 3x^2z + 3xy^2 + 3xz^2 + 3y^2z - 3yz^2 - 6xyz \pmod{\theta_1}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(-x^2y + x^2z + xy^2 + xz^2 + y^2z - yz^2 - 2xyz) \pmod{\theta_1}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(-y(x^2 + 2xz + z^2) + (x + z)xz + (x + z)y^2) \pmod{\theta_1}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(-y(x + z)^2 + (x + z)xz + (x + z)y^2) \pmod{\theta_1}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(x + z)(-xy - yz + xz + y^2) \pmod{\theta_1}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(x + z)(-x(y - z) + y(y - z)) \pmod{\theta_1}$$

$$(x + z - y)^3 \equiv 2x^3 + 3(x + z)(y - z)(y - x) \pmod{\theta_1}$$

$$0 \equiv 2x^3 + 3yxz \pmod{\theta_1}$$

$$-2x^2 \equiv 3yz \pmod{\theta_1}$$

(65) より

$$2q_1r_1yz \equiv 3yz \pmod{\theta_1}$$

$$2q_1r_1 \equiv 3 \pmod{\theta_1}$$

$$2^p q_1^p r_1^p \equiv 3^p \pmod{\theta_1}$$

(68) より

$$2^3 \equiv 3^3 \pmod{\theta_1}$$

$$8 \equiv 27 \pmod{\theta_1}$$

$$0 \equiv 19 \pmod{\theta_1}$$

これは $0 \equiv 19 \pmod{\theta_4}$ とともに成り立つと (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

$$1 \equiv 2^{19-1} \pmod{19}$$

$$2^{-1} \equiv 2^{19-2} \pmod{19}$$

$$2^{-1} \equiv 2^{17} \pmod{19}$$

$$2^{-1} \equiv 10$$

$$\sqrt{-3} \equiv \sqrt{19-3} \pmod{19}$$

$$\sqrt{-3} \equiv \sqrt{16} \pmod{19}$$

$$\sqrt{-3} \equiv 4 \pmod{19}$$

1.7.11 Complement 2(補足 2)

Proposition 19 $(x^{p-1})^2 \equiv l_1^{-1}m_1^{-1}y^{p-1}z^{p-1} \pmod{\theta_4} \Rightarrow$
 $(l_1^{-1}y^{p-1})^2 \equiv -m_1^{-1}x^{p-1}z^{p-1} \pmod{\theta_4} \quad , \quad (m_1^{-1}z^{p-1})^2 \equiv -l_1^{-1}x^{p-1}y^{p-1} \pmod{\theta_4}$

Proof 20 (60) より

$$\begin{array}{rcl} x^p & +q_1yx^{p-1} & \equiv r_1zx^{p-1} \pmod{\delta} \\ q_1^{-1}xy^{p-1} & +y^p & \equiv q_1^{-1}r_1zy^{p-1} \pmod{\delta} \\ r_1^{-1}xz^{p-1} & +q_1r_1^{-1}yz^{p-1} & \equiv z^p \pmod{\delta} \end{array} \quad (97)$$

ここで

$$\begin{aligned} q_1yx^{p-1} &\equiv y^p \pmod{\theta_4} \Rightarrow r_1zx^{p-1} \equiv z^p \pmod{\theta_4} \\ x^{p-1} &\equiv q_1^{-1}y^{p-1} \pmod{\theta_4} \Rightarrow x^{p-1} \equiv r_1^{-1}z^{p-1} \pmod{\theta_4} \end{aligned}$$

であるから自動的に

$$\begin{aligned} q_1^{-1}xy^{p-1} &\equiv x^p \pmod{\theta_4} \quad , \quad q_1^{-1}r_1zy^{p-1} \equiv z^p \pmod{\theta_4} \\ r_1^{-1}xz^{p-1} &\equiv x^p \pmod{\theta_4} \quad , \quad q_1r_1^{-1}yz^{p-1} \equiv y^p \pmod{\theta_4} \end{aligned}$$

(71) より

$$\begin{array}{rcl} x^p & +q_2^{-1}yx^{p-1} & \equiv q_2^{-1}r_2zx^{p-1} \pmod{\delta} \\ q_2xy^{p-1} & +y^p & \equiv r_2zy^{p-1} \pmod{\delta} \\ q_2r_2^{-1}xz^{p-1} & +r_2^{-1}yz^{p-1} & \equiv z^p \pmod{\delta} \end{array} \quad (98)$$

ここで

$$\begin{aligned} q_2xy^{p-1} &\equiv x^p \pmod{\theta_4} \Rightarrow r_2zy^{p-1} \equiv z^p \pmod{\theta_4} \\ y^{p-1} &\equiv q_2^{-1}x^{p-1} \pmod{\theta_4} \Rightarrow y^{p-1} \equiv r_2^{-1}z^{p-1} \pmod{\theta_4} \end{aligned}$$

であるから自動的に

$$\begin{aligned} q_2^{-1}yx^{p-1} &\equiv y^p \pmod{\theta_4} \quad , \quad q_2^{-1}r_2zx^{p-1} \equiv z^p \pmod{\theta_4} \\ q_2r_2^{-1}xz^{p-1} &\equiv x^p \pmod{\theta_4} \quad , \quad r_2^{-1}yz^{p-1} \equiv y^p \pmod{\theta_4} \end{aligned}$$

(82) より

$$\begin{array}{rcl} x^p & +q_3^{-1}r_3yx^{p-1} & \equiv q_3^{-1}zx^{p-1} \pmod{\delta} \\ q_3r_3^{-1}xy^{p-1} & +y^p & \equiv r_3^{-1}zy^{p-1} \pmod{\delta} \\ q_3xz^{p-1} & +r_3yz^{p-1} & \equiv z^p \pmod{\delta} \end{array} \quad (99)$$

ここで

$$\begin{aligned} q_3xz^{p-1} &\equiv x^p \pmod{\theta_4} \Rightarrow r_3yz^{p-1} \equiv y^p \pmod{\theta_4} \\ z^{p-1} &\equiv q_3^{-1}x^{p-1} \pmod{\theta_4} \Rightarrow z^{p-1} \equiv r_3^{-1}y^{p-1} \pmod{\theta_4} \end{aligned}$$

であるから自動的に

$$\begin{aligned} q_3^{-1}r_3yx^{p-1} &\equiv y^p \pmod{\theta_4} \quad , \quad q_3^{-1}zx^{p-1} \equiv z^p \pmod{\theta_4} \\ q_3r_3^{-1}xy^{p-1} &\equiv x^p \pmod{\theta_4} \quad , \quad r_3^{-1}zy^{p-1} \equiv z^p \pmod{\theta_4} \end{aligned}$$

よって (97)(98)(99) の各項は同値である。

$$\begin{aligned} x^p + q_1 y x^{p-1} &\equiv r_1 z x^{p-1} \pmod{\theta_4} \\ q_2 x y^{p-1} + y^p &\equiv r_2 z y^{p-1} \pmod{\theta_4} \\ q_3 x z^{p-1} + r_3 y z^{p-1} &\equiv z^p \pmod{\theta_4} \end{aligned}$$

またこれは Definition 16,17,18 から次のように表すことができる。

$$\begin{aligned} x^p + m_1 z x^{p-1} &\equiv l_1 y x^{p-1} \pmod{\theta_4} \\ -m_2 z y^{p-1} + y^p &\equiv l_2 x y^{p-1} \pmod{\theta_4} \\ l_3 y z^{p-1} - m_3 x z^{p-1} &\equiv z^p \pmod{\theta_4} \end{aligned}$$

ここで

$$m_1 z x^{p-1} \equiv y^p \pmod{\theta_4} \Rightarrow l_1 y x^{p-1} \equiv z^p \pmod{\theta_4}$$

ならば

$$\begin{aligned} -m_2 z y^{p-1} &\equiv x^p \pmod{\theta_4} \quad , \quad l_2 x y^{p-1} \equiv z^p \pmod{\theta_4} \\ l_3 y z^{p-1} &\equiv x^p \pmod{\theta_4} \quad , \quad -m_3 x z^{p-1} \equiv y^p \pmod{\theta_4} \end{aligned}$$

$\pmod{\theta_1}$ のときも (23)(34)(45) の各項は同値であり、それら 2 項入れ替えの式に対応した $\pmod{\theta_4}$ も同値である。

以上より

$$\begin{aligned} (x^{p-1})^2 &\equiv l_1^{-1} m_1^{-1} y^{p-1} z^{p-1} \pmod{\theta_4} \Rightarrow \\ (l_1^{-1} y^{p-1})^2 &\equiv -m_1^{-1} x^{p-1} z^{p-1} \pmod{\theta_4} \quad , \quad (m_1^{-1} z^{p-1})^2 \equiv -l_1^{-1} x^{p-1} y^{p-1} \pmod{\theta_4} \end{aligned}$$

□

1.8 $\delta = 2$ のとき

1.8.1 $2 \mid x$, $2 \nmid yz$

$S = 2^k$ のとき

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

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

$$2 \mid L = p^{n p^{p-1}} a^p$$

$$2 \mid a$$

$$2 \nmid R = p \alpha^p$$

$$2 \nmid \alpha$$

$$x + z - y = p^n a (\alpha + p^{(p-1)n-1} a^{p-1})$$

$$2^k = \alpha + p^{(p-1)n-1} a^{p-1} = \text{odd}$$

$$2^0 = 1$$

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

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

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

$$2 \mid L = a'^p$$

$$2 \mid a'$$

$$2 \nmid R = \alpha'^p$$

$$2 \nmid \alpha'$$

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

$$2^k = \alpha' + a'^{p-1} = \text{odd}$$

$$2^0 = 1$$

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)

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

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

Proof 22

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

$\delta' \mid S''$ 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 $\delta' \mid z+x$

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

$z^p - x^p = y^p \equiv 0 \pmod{\delta'}$ なので

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

よって

$$\delta' \perp \beta$$

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

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

よって

$$\delta' \perp \alpha$$

□

$$x + y + k'_1 \equiv -z + k'_1 \pmod{\delta'} \text{ より}$$

Definition 23 $y + k'_1 \equiv l'_1 y \pmod{\delta'}$, $-z + k'_1 \equiv -m'_1 z \pmod{\delta'}$, $l'_1 m'_1 \perp \delta'$

$$l'_1 y x^{p-1} \cdot -m'_1 z x^{p-1} \equiv y^p z^p \pmod{\delta'}$$

$$x + l'_1 y \equiv -m'_1 z \pmod{\delta'} \text{ より}$$

$$\begin{array}{rcl} x^p & + l'_1 y x^{p-1} & \equiv -m'_1 z x^{p-1} \pmod{\delta'} \\ l_1'^{-1} x y^{p-1} & + y^p & \equiv -l_1'^{-1} m'_1 z y^{p-1} \pmod{\delta'} \\ -m_1'^{-1} x z^{p-1} & - l_1' m_1'^{-1} y z^{p-1} & \equiv z^p \pmod{\delta'} \end{array} \quad (100)$$

ここで

$$\begin{aligned} l_1' y x^{p-1} &\equiv y^p \pmod{\delta'} \Rightarrow -m'_1 z x^{p-1} \equiv z^p \pmod{\delta'} \\ x^{p-1} &\equiv l_1'^{-1} y^{p-1} \pmod{\delta'} \Rightarrow x^{p-1} \equiv -m_1'^{-1} z^{p-1} \pmod{\delta'} \end{aligned}$$

であるから自動的に

$$\begin{aligned} l_1'^{-1} x y^{p-1} &\equiv x^p \pmod{\delta'} , \quad -l_1'^{-1} m'_1 z y^{p-1} \equiv z^p \pmod{\delta'} \\ -m_1'^{-1} x z^{p-1} &\equiv x^p \pmod{\delta'} , \quad -l_1' m_1'^{-1} y z^{p-1} \equiv y^p \pmod{\delta'} \end{aligned}$$

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

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

or

$$x^{p-1} \not\equiv l_1'^{-1} y^{p-1} \not\equiv -m_1'^{-1} z^{p-1} \pmod{\delta'}$$

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

(100) より

$$\begin{aligned} l_1' y x^{p-1} \cdot -m_1' z x^{p-1} &\equiv y^p z^p \pmod{\delta'} \\ l_1' m_1' (x^{p-1})^2 &\equiv -y^{p-1} z^{p-1} \pmod{\delta'} \\ (x^{p-1})^2 &\equiv -l_1'^{-1} m_1'^{-1} y^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (101)$$

$$\begin{aligned} l_1'^{-1} x y^{p-1} \cdot -l_1'^{-1} m_1' z y^{p-1} &\equiv x^p z^p \pmod{\delta'} \\ l_1'^{-2} m_1' (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta'} \\ (l_1'^{-1} y^{p-1})^2 &\equiv -m_1'^{-1} x^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (102)$$

$$\begin{aligned} -m_1'^{-1} x z^{p-1} \cdot -l_1' m_1'^{-1} y z^{p-1} &\equiv x^p y^p \pmod{\delta'} \\ l_1' m_1'^{-2} (z^{p-1})^2 &\equiv x^{p-1} y^{p-1} \pmod{\delta'} \\ (m_1'^{-1} z^{p-1})^2 &\equiv l_1'^{-1} x^{p-1} y^{p-1} \pmod{\delta'} \end{aligned} \quad (103)$$

(101)(102)(103) より

$$\begin{aligned}
(x^{p-1})^3 &\equiv (l_1'^{-1}y^{p-1})^3 \equiv -(m_1'^{-1}z^{p-1})^3 \pmod{\delta'} \\
(m_1'^{-1}z^{p-1})^3 + (l_1'^{-1}y^{p-1})^3 &\equiv (m_1'^{-1}z^{p-1} + l_1'^{-1}y^{p-1})((m_1'^{-1}z^{p-1})^2 - l_1'^{-1}m_1'^{-1}y^{p-1}z^{p-1} + (l_1'^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta'} \\
(x^{p-1})^3 + (m_1'^{-1}z^{p-1})^3 &\equiv (x^{p-1} + m_1'^{-1}z^{p-1})((x^{p-1})^2 - m_1'^{-1}x^{p-1}z^{p-1} + (m_1'^{-1}z^{p-1})^2) \equiv 0 \pmod{\delta'} \\
(x^{p-1})^3 - (l_1'^{-1}y^{p-1})^3 &\equiv (x^{p-1} - l_1'^{-1}y^{p-1})((x^{p-1})^2 + l_1'^{-1}x^{p-1}y^{p-1} + (l_1'^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta'}
\end{aligned}$$

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

(102)(103) より

$$\begin{aligned}
(x^{p-1})^2 + (m_1'^{-1}z^{p-1})^2 + (l_1'^{-1}y^{p-1})^2 &\equiv 0 \pmod{\theta'_4} \\
(x^{p-1})^2 + l_1'^{-1}x^{p-1}y^{p-1} - m_1'^{-1}x^{p-1}z^{p-1} &\equiv 0 \pmod{\theta'_4} \\
x^{p-1} + l_1'^{-1}y^{p-1} - m_1'^{-1}z^{p-1} &\equiv 0 \pmod{\theta'_4} \\
x^{p-1} + l_1'^{-1}y^{p-1} &\equiv m_1'^{-1}z^{p-1} \pmod{\theta'_4}
\end{aligned}$$

【General solution conditions】

$$\begin{aligned}
x^p + l_1'^{-1}y^{p-1}x &\equiv m_1'^{-1}z^{p-1}x \pmod{\theta'_4} \\
l_1'x^{p-1}y + y^p &\equiv l_1'm_1'^{-1}z^{p-1}y \pmod{\theta'_4} \\
m_1'x^{p-1}z + l_1'^{-1}m_1'y^{p-1}z &\equiv z^p \pmod{\theta'_4}
\end{aligned} \tag{104}$$

(104) より

$$\begin{aligned}
l_1'^{-1}y^{p-1}x \cdot m_1'^{-1}z^{p-1}x &\equiv y^p z^p \pmod{\theta'_4} \\
x^2 &\equiv l_1'm_1'yz \pmod{\theta'_4}
\end{aligned} \tag{105}$$

$$\begin{aligned}
l_1'x^{p-1}y \cdot l_1'm_1'^{-1}z^{p-1}y &\equiv x^p z^p \pmod{\theta'_4} \\
y^2 &\equiv l_1'^{-2}m_1'xz \pmod{\theta'_4}
\end{aligned} \tag{106}$$

$$\begin{aligned}
m_1'x^{p-1}z \cdot l_1'^{-1}m_1'y^{p-1}z &\equiv x^p y^p \pmod{\theta'_4} \\
z^2 &\equiv l_1'm_1'^{-2}xy \pmod{\theta'_4}
\end{aligned} \tag{107}$$

$$\begin{aligned}
(101) \text{ より } (x^{p-1})^2 &\equiv -l_1'^{-1} m_1'^{-1} y^{p-1} z^{p-1} \pmod{\theta'_4} \\
(x^2)^{p-1} &\equiv -l_1'^{-1} m_1'^{-1} y^{p-1} z^{p-1} \pmod{\theta'_4} \\
(105) \text{ より } (l_1' m_1' y z)^{p-1} &\equiv -l_1'^{-1} m_1'^{-1} y^{p-1} z^{p-1} \pmod{\theta'_4} \\
l_1'^{p-1} m_1'^{p-1} y^{p-1} z^{p-1} &\equiv -l_1'^{-1} m_1'^{-1} y^{p-1} z^{p-1} \pmod{\theta'_4} \\
l_1'^p m_1'^p y^{p-1} z^{p-1} &\equiv -y^{p-1} z^{p-1} \pmod{\theta'_4} \\
l_1'^p m_1'^p &\equiv -1 \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
(102) \text{ より } (y^{p-1})^2 &\equiv -l_1'^2 m_1'^{-1} x^{p-1} z^{p-1} \pmod{\theta'_4} \\
(y^2)^{p-1} &\equiv -l_1'^2 m_1'^{-1} x^{p-1} z^{p-1} \pmod{\theta'_4} \\
(106) \text{ より } (l_1'^{-2} m_1' x z)^{p-1} &\equiv -l_1'^2 m_1'^{-1} x^{p-1} z^{p-1} \pmod{\theta'_4} \\
l_1'^{-2p+2} m_1'^{p-1} x^{p-1} z^{p-1} &\equiv -l_1'^2 m_1'^{-1} x^{p-1} z^{p-1} \pmod{\theta'_4} \\
l_1'^{-2p} m_1'^p x^{p-1} z^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\theta'_4} \\
l_1'^{-2p} m_1'^p &\equiv -1 \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
(103) \text{ より } (z^{p-1})^2 &\equiv l_1'^{-1} m_1'^2 x^{p-1} y^{p-1} \pmod{\theta'_4} \\
(z^2)^{p-1} &\equiv l_1'^{-1} m_1'^2 x^{p-1} y^{p-1} \pmod{\theta'_4} \\
(107) \text{ より } (l_1' m_1'^{-2} x y)^{p-1} &\equiv l_1'^{-1} m_1'^2 x^{p-1} y^{p-1} \pmod{\theta'_4} \\
l_1'^{p-1} m_1'^{-2p+2} x^{p-1} y^{p-1} &\equiv l_1'^{-1} m_1'^2 x^{p-1} y^{p-1} \pmod{\theta'_4} \\
l_1'^p m_1'^{-2p} x^{p-1} y^{p-1} &\equiv x^{p-1} y^{p-1} \pmod{\theta'_4} \\
l_1'^p m_1'^{-2p} &\equiv 1 \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
l_1^p m_1'^p &\equiv -1 \pmod{\theta'_4} \\
l_1'^{-2p} m_1'^p &\equiv -1 \pmod{\theta'_4} \\
l_1^p m_1'^{-2p} &\equiv 1 \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
-m_1'^{3p} &\equiv l_1'^{3p} \pmod{\theta'_4} \\
m_1'^{3p} + l_1'^{3p} &\equiv (m_1'^p + l_1'^p)(m_1'^{2p} - l_1'^p m_1'^p + l_1'^{2p}) \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
-m_1'^p &\equiv l_1'^{2p} \pmod{\theta'_4} \\
l_1'^p &\equiv m_1'^{2p} \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
l_1'^p + m_1'^p &\equiv m_1'^{2p} - l_1'^{2p} \pmod{\theta'_4} \\
l_1'^p + m_1'^p &\equiv (m_1'^p + l_1'^p)(m_1'^p - l_1'^p) \pmod{\theta'_4} \\
1 &\equiv m_1'^p - l_1'^p \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
(m_1'^p - l_1'^p)^2 &\equiv 1^2 \pmod{\theta'_4} \\
l_1'^{2p} - 2l_1'^p m_1'^p + m_1'^{2p} &\equiv 1 \pmod{\theta'_4} \\
l_1'^{2p} - 2l_1'^p m_1'^p + m_1'^{2p} &\equiv -l_1'^p m_1'^p \pmod{\theta'_4} \\
l_1'^{2p} - l_1'^p m_1'^p + m_1'^{2p} &\equiv 0 \pmod{\theta'_4}
\end{aligned}$$

よって $m_1'^p + l_1'^p \not\equiv 0 \pmod{\theta'_4}$

$$\begin{aligned}
m_1'^p - l_1'^p &\equiv 1 \pmod{\theta'_4} \\
l_1'^{2p} - l_1'^p m_1'^p &\equiv -l_1'^p \pmod{\theta'_4} \\
l_1'^{2p} + l_1'^p + 1 &\equiv 0 \pmod{\theta'_4}
\end{aligned}$$

$l_1^p m_1'^p \equiv -1 \pmod{\theta'_4}$ なるので

$$l_1'^p \equiv \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \quad (108)$$

$$m_1'^p \equiv \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \quad (109)$$

$$x + k'_2 + y \equiv -z + k'_2 \pmod{\delta'} \text{ より}$$

Definition 24 $x + k'_2 \equiv l'_2 x \pmod{\delta'}$, $-z + k'_2 \equiv -m'_2 z \pmod{\delta'}$, $l'_2 m'_2 \perp \delta'$

$$l'_2 x y^{p-1} \cdot -m'_2 z y^{p-1} \equiv x^p z^p \pmod{\delta'}$$

$$l'_2 x + y \equiv -m'_2 z \pmod{\delta'} \text{ より}$$

$$\begin{aligned} x^p + l'^{-1}_2 y x^{p-1} &\equiv -l'^{-1}_2 m'_2 z x^{p-1} \pmod{\delta'} \\ l'_2 x y^{p-1} + y^p &\equiv -m'_2 z y^{p-1} \pmod{\delta'} \\ -l'_2 m'^{-1}_2 x z^{p-1} - m'^{-1}_2 y z^{p-1} &\equiv z^p \pmod{\delta'} \end{aligned} \quad (110)$$

ここで

$$\begin{aligned} l'_2 x y^{p-1} \equiv x^p \pmod{\delta'} &\Rightarrow -m'_2 z y^{p-1} \equiv z^p \pmod{\delta'} \\ l'_2 y^{p-1} \equiv x^{p-1} \pmod{\delta'} &\Rightarrow -m'_2 y^{p-1} \equiv z^{p-1} \pmod{\delta'} \end{aligned}$$

であるから自動的に

$$\begin{aligned} l'^{-1}_2 y x^{p-1} \equiv y^p \pmod{\delta'} , \quad -l'^{-1}_2 m'_2 z x^{p-1} &\equiv z^p \pmod{\delta'} \\ -l'_2 m'^{-1}_2 x z^{p-1} \equiv x^p \pmod{\delta'} , \quad -m'^{-1}_2 y z^{p-1} &\equiv y^p \pmod{\delta'} \end{aligned}$$

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

$$\begin{aligned} l'^{-1}_2 x^{p-1} \equiv y^{p-1} &\equiv -m'^{-1}_2 z^{p-1} \pmod{\delta'} \\ \text{or} \\ l'^{-1}_2 x^{p-1} \not\equiv y^{p-1} &\not\equiv -m'^{-1}_2 z^{p-1} \pmod{\delta'} \end{aligned}$$

1.9.4 Common to $l'^{-1}_2 x^{p-1} \not\equiv y^{p-1} \not\equiv -m'^{-1}_2 z^{p-1} \pmod{\delta'}$

(110) より

$$\begin{aligned} l'^{-1}_2 y x^{p-1} \cdot -l'^{-1}_2 m'_2 z x^{p-1} &\equiv y^p z^p \pmod{\delta'} \\ l'^{-2}_2 m'_2 (x^{p-1})^2 &\equiv -y^{p-1} z^{p-1} \pmod{\delta'} \\ (l'^{-1}_2 x^{p-1})^2 &\equiv -m'^{-1}_2 y^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (111)$$

$$\begin{aligned} l'_2 x y^{p-1} \cdot -m'_2 z y^{p-1} &\equiv x^p z^p \pmod{\delta'} \\ l'_2 m'_2 (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta'} \\ (y^{p-1})^2 &\equiv -l'^{-1}_2 m'^{-1}_2 x^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (112)$$

$$\begin{aligned} -l'_2 m'^{-1}_2 x z^{p-1} \cdot -m'^{-1}_2 y z^{p-1} &\equiv x^p y^p \pmod{\delta'} \\ l'_2 m'^{-2}_2 (z^{p-1})^2 &\equiv x^{p-1} y^{p-1} \pmod{\delta'} \\ (m'^{-1}_2 z^{p-1})^2 &\equiv l'^{-1}_2 x^{p-1} y^{p-1} \pmod{\delta'} \end{aligned} \quad (113)$$

(111)(112)(113) より

$$\begin{aligned}
(l_2'^{-1}x^{p-1})^3 &\equiv (y^{p-1})^3 \equiv -(m_2'^{-1}z^{p-1})^3 \pmod{\delta'} \\
(y^{p-1})^3 + (m_2'^{-1}z^{p-1})^3 &\equiv (y^{p-1} + m_2'^{-1}z^{p-1})((y^{p-1})^2 - m_2'^{-1}y^{p-1}z^{p-1} + (m_2'^{-1}z^{p-1})^2) \equiv 0 \pmod{\delta'} \\
(l_2'^{-1}x^{p-1})^3 - (y^{p-1})^3 &\equiv (l_2'^{-1}x^{p-1} - y^{p-1})((l_2'^{-1}x^{p-1})^2 + l_2'^{-1}x^{p-1}y^{p-1} + (y^{p-1})^2) \equiv 0 \pmod{\delta'} \\
(l_2'^{-1}x^{p-1})^3 + (m_2'^{-1}z^{p-1})^3 &\equiv (l_2'^{-1}x^{p-1} + m_2'^{-1}z^{p-1})((l_2'^{-1}x^{p-1})^2 - l_2'^{-1}m_2'^{-1}x^{p-1}z^{p-1} + (m_2'^{-1}z^{p-1})^2) \equiv 0 \pmod{\delta'}
\end{aligned}$$

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

(111)(113) より

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

【General solution conditions】

$$\begin{aligned}
x^p + l_2'y^{p-1}x &\equiv l_2'm_2'^{-1}z^{p-1}x \pmod{\theta_4'} \\
l_2'^{-1}x^{p-1}y + y^p &\equiv m_2'^{-1}z^{p-1}y \pmod{\theta_4'} \\
l_2'^{-1}m_2'x^{p-1}z + m_2'y^{p-1}z &\equiv z^p \pmod{\theta_4'}
\end{aligned} \tag{114}$$

(114) より

$$\begin{aligned}
l_2'y^{p-1}x \cdot l_2'm_2'^{-1}z^{p-1}x &\equiv y^p z^p \pmod{\theta_4'} \\
x^2 &\equiv l_2'^{-2}m_2'yz \pmod{\theta_4'}
\end{aligned} \tag{115}$$

$$\begin{aligned}
l_2'^{-1}x^{p-1}y \cdot m_2'^{-1}z^{p-1}y &\equiv x^p z^p \pmod{\theta_4'} \\
y^2 &\equiv l_2'm_2'xz \pmod{\theta_4'}
\end{aligned} \tag{116}$$

$$\begin{aligned}
l_2'^{-1}m_2'x^{p-1}z \cdot m_2'y^{p-1}z &\equiv x^p y^p \pmod{\theta_4'} \\
z^2 &\equiv l_2'm_2'^{-2}xy \pmod{\theta_4'}
\end{aligned} \tag{117}$$

$$\begin{aligned}
(111) \text{ より } (x^{p-1})^2 &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \pmod{\theta_4'} \\
(x^2)^{p-1} &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \pmod{\theta_4'} \\
(115) \text{ より } (l_2'^{-2} m_2' y z)^{p-1} &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_2'^{-2p+2} m_2'^{p-1} y^{p-1} z^{p-1} &\equiv -l_2'^2 m_2'^{-1} y^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_2'^{-2p} m_2'^p &\equiv -1 \pmod{\theta_4'}
\end{aligned}$$

$$\begin{aligned}
(112) \text{ より } (y^{p-1})^2 &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
(y^2)^{p-1} &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
(116) \text{ より } (l_2' m_2' x z)^{p-1} &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_2'^{p-1} m_2'^{p-1} x^{p-1} z^{p-1} &\equiv -l_2'^{-1} m_2'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_2'^p m_2'^p &\equiv -1 \pmod{\theta_4'}
\end{aligned}$$

$$\begin{aligned}
(113) \text{ より } (z^{p-1})^2 &\equiv l_2'^{-1} m_2'^2 x^{p-1} y^{p-1} \pmod{\theta_4'} \\
(z^2)^{p-1} &\equiv l_2'^{-1} m_2'^2 x^{p-1} y^{p-1} \pmod{\theta_4'} \\
(117) \text{ より } (l_2' m_2'^{-2} x y)^{p-1} &\equiv l_2'^{-1} m_2'^2 x^{p-1} y^{p-1} \pmod{\theta_4'} \\
l_2'^{p-1} m_2'^{-2p+2} x^{p-1} y^{p-1} &\equiv l_2'^{-1} m_2'^2 x^{p-1} y^{p-1} \pmod{\theta_4'} \\
l_2'^p m_2'^{-2p} &\equiv 1 \pmod{\theta_4'}
\end{aligned}$$

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

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

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

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

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

よって $m_2'^p + l_2'^p \not\equiv 0 \pmod{\theta_4}$

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

(100)(110) より

$$\begin{aligned}
l_2'^{-1} y x^{p-1} &\equiv l_1' y x^{p-1} \pmod{\delta'} \\
l_2'^{-1} &\equiv l_1' \pmod{\delta'} \\
1 &\equiv l_1'^p l_2'^p \pmod{\delta'}
\end{aligned} \tag{118}$$

$l_2'^p m_2'^p \equiv -1 \pmod{\theta_4'}$ なので

$$l_2'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta_4'} \tag{119}$$

$$m_2'^p \equiv \frac{1 \mp \sqrt{-3}}{2} \pmod{\theta_4'} \tag{120}$$

$$x - k'_3 + y + k'_3 \equiv -z \pmod{\delta'} \text{ より}$$

Definition 25 $x - k'_3 \equiv m'_3 x \pmod{\delta'}$, $y + k'_3 \equiv l'_3 y \pmod{\delta'}$, $l'_3 m'_3 \perp \delta'$

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

$$m'_3 x + l'_3 y \equiv -z \pmod{\delta'} \text{ より}$$

$$\begin{array}{rcl} x^p + l'_3 m'^{-1}_3 y x^{p-1} & \equiv & -m'^{-1}_3 z x^{p-1} \pmod{\delta'} \\ l'^{-1}_3 m'_3 x y^{p-1} + y^p & \equiv & -l'^{-1}_3 z y^{p-1} \pmod{\delta'} \\ -m'_3 x z^{p-1} - l'_3 y z^{p-1} & \equiv & z^p \pmod{\delta'} \end{array} \quad (121)$$

ここで

$$\begin{aligned} -m'_3 x z^{p-1} \equiv x^p \pmod{\delta'} &\Rightarrow -l'_3 y z^{p-1} \equiv y^p \pmod{\delta'} \\ -m'_3 z^{p-1} \equiv x^{p-1} \pmod{\delta'} &\Rightarrow -l'_3 z^{p-1} \equiv y^{p-1} \pmod{\delta'} \end{aligned}$$

であるから自動的に

$$\begin{aligned} l'_3 m'^{-1}_3 y x^{p-1} &\equiv y^p \pmod{\delta'} , \quad -m'^{-1}_3 z x^{p-1} \equiv z^p \pmod{\delta'} \\ l'^{-1}_3 m'_3 x y^{p-1} &\equiv x^p \pmod{\delta'} , \quad -l'^{-1}_3 z y^{p-1} \equiv z^p \pmod{\delta'} \end{aligned}$$

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

$$\begin{aligned} m'^{-1}_3 x^{p-1} &\equiv l'^{-1}_3 y^{p-1} \equiv -z^{p-1} \pmod{\delta'} \\ \text{or} \\ m'^{-1}_3 x^{p-1} &\not\equiv l'^{-1}_3 y^{p-1} \not\equiv -z^{p-1} \pmod{\delta'} \end{aligned}$$

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

(121) より

$$\begin{aligned} l'_3 m'^{-1}_3 y x^{p-1} \cdot -m'^{-1}_3 z x^{p-1} &\equiv y^p z^p \pmod{\delta'} \\ l'^{-2}_3 m'^{-2}_3 (x^{p-1})^2 &\equiv -y^{p-1} z^{p-1} \pmod{\delta'} \\ (m'^{-1}_3 x^{p-1})^2 &\equiv -l'^{-1}_3 y^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (122)$$

$$\begin{aligned} l'^{-1}_3 m'_3 x y^{p-1} \cdot -l'^{-1}_3 z y^{p-1} &\equiv x^p z^p \pmod{\delta'} \\ l'^{-2}_3 m'^{-2}_3 (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta'} \\ (l'^{-1}_3 y^{p-1})^2 &\equiv -m'^{-1}_3 x^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (123)$$

$$\begin{aligned} -m'_3 x z^{p-1} \cdot -l'_3 y z^{p-1} &\equiv x^p y^p \pmod{\delta'} \\ l'_3 m'_3 (z^{p-1})^2 &\equiv x^{p-1} y^{p-1} \pmod{\delta'} \\ (z^{p-1})^2 &\equiv l'^{-1}_3 m'^{-1}_3 x^{p-1} y^{p-1} \pmod{\delta'} \end{aligned} \quad (124)$$

(122)(123)(124) より

$$\begin{aligned}
(m_3'^{-1}x^{p-1})^3 &\equiv (l_3'^{-1}y^{p-1})^3 \equiv -(z^{p-1})^3 \pmod{\delta'} \\
(z^{p-1})^3 + (l_3'^{-1}y^{p-1})^3 &\equiv (z^{p-1} + l_3'^{-1}y^{p-1})((z^{p-1})^2 - l_3'^{-1}y^{p-1}z^{p-1} + (l_3'^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta'} \\
(m_3'^{-1}x^{p-1})^3 + (z^{p-1})^3 &\equiv (m_3'^{-1}x^{p-1} + z^{p-1})((m_3'^{-1}x^{p-1})^2 - m_3'^{-1}x^{p-1}z^{p-1} + (z^{p-1})^2) \equiv 0 \pmod{\delta'} \\
(m_3'^{-1}x^{p-1})^3 - (l_3'^{-1}y^{p-1})^3 &\equiv (m_3'^{-1}x^{p-1} - l_3'^{-1}y^{p-1})((m_3'^{-1}x^{p-1})^2 + l_3'^{-1}m_3'^{-1}x^{p-1}y^{p-1} + (l_3'^{-1}y^{p-1})^2) \equiv 0 \pmod{\delta'}
\end{aligned}$$

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

(122)(123) より

$$\begin{aligned}
(l_3'^{-1}y^{p-1})^2 + (m_3'^{-1}x^{p-1})^2 + (z^{p-1})^2 &\equiv 0 \pmod{\theta'_4} \\
-m_3'^{-1}x^{p-1}z^{p-1} - l_3'^{-1}y^{p-1}z^{p-1} + (z^{p-1})^2 &\equiv 0 \pmod{\theta'_4} \\
m_3'^{-1}x^{p-1} + l_3'^{-1}y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta'_4} \\
m_3'^{-1}x^{p-1} + l_3'^{-1}y^{p-1} &\equiv z^{p-1} \pmod{\theta'_4}
\end{aligned}$$

【General solution conditions】

$$\begin{aligned}
x^p + l_3'^{-1}m_3' y^{p-1} x &\equiv m_3' z^{p-1} x \pmod{\theta'_4} \\
l_3' m_3'^{-1} x^{p-1} y + y^p &\equiv l_3' z^{p-1} y \pmod{\theta'_4} \\
m_3'^{-1} x^{p-1} z + l_3'^{-1} y^{p-1} z &\equiv z^p \pmod{\theta'_4}
\end{aligned} \tag{125}$$

(125) より

$$\begin{aligned}
l_3'^{-1}m_3' y^{p-1} x \cdot m_3' z^{p-1} x &\equiv y^p z^p \pmod{\theta'_4} \\
x^2 &\equiv l_3' m_3'^{-2} y z \pmod{\theta'_4}
\end{aligned} \tag{126}$$

$$\begin{aligned}
l_3' m_3'^{-1} x^{p-1} y \cdot l_3' z^{p-1} y &\equiv x^p z^p \pmod{\theta'_4} \\
y^2 &\equiv l_3'^{-2} m_3' x z \pmod{\theta'_4}
\end{aligned} \tag{127}$$

$$\begin{aligned}
m_3'^{-1} x^{p-1} z \cdot l_3'^{-1} y^{p-1} z &\equiv x^p y^p \pmod{\theta'_4} \\
z^2 &\equiv l_3' m_3' x y \pmod{\theta'_4}
\end{aligned} \tag{128}$$

$$\begin{aligned}
(122) \text{ より } (x^{p-1})^2 &\equiv -l_3'^{-1} m_3'^2 y^{p-1} z^{p-1} \pmod{\theta_4'} \\
(x^2)^{p-1} &\equiv -l_3'^{-1} m_3'^2 y^{p-1} z^{p-1} \pmod{\theta_4'} \\
(126) \text{ より } (l_3' m_3'^{-2} yz)^{p-1} &\equiv -l_3'^{-1} m_3'^2 y^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_3'^{p-1} m_3'^{-2p+2} y^{p-1} z^{p-1} &\equiv -l_3'^{-1} m_3'^2 y^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_3'^p m_3'^{-2p} &\equiv -1 \pmod{\theta_4'}
\end{aligned}$$

$$\begin{aligned}
(123) \text{ より } (y^{p-1})^2 &\equiv -l_3'^2 m_3'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
(y^2)^{p-1} &\equiv -l_3'^2 m_3'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
(127) \text{ より } (l_3'^{-2} m_3' xz)^{p-1} &\equiv -l_3'^2 m_3'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_3'^{-2p+2} m_3'^{p-1} x^{p-1} z^{p-1} &\equiv -l_3'^2 m_3'^{-1} x^{p-1} z^{p-1} \pmod{\theta_4'} \\
l_3'^{-2p} m_3'^p &\equiv -1 \pmod{\theta_4'}
\end{aligned}$$

$$\begin{aligned}
(124) \text{ より } (z^{p-1})^2 &\equiv l_3'^{-1} m_3'^{-1} x^{p-1} y^{p-1} \pmod{\theta_4'} \\
(z^2)^{p-1} &\equiv l_3'^{-1} m_3'^{-1} x^{p-1} y^{p-1} \pmod{\theta_4'} \\
(128) \text{ より } (l_3' m_3' xy)^{p-1} &\equiv l_3'^{-1} m_3'^{-1} x^{p-1} y^{p-1} \pmod{\theta_4'} \\
l_3'^{p-1} m_3'^{p-1} x^{p-1} y^{p-1} &\equiv l_3'^{-1} m_3'^{-1} x^{p-1} y^{p-1} \pmod{\theta_4'} \\
l_3'^p m_3'^p &\equiv 1 \pmod{\theta_4'}
\end{aligned}$$

$$\begin{aligned}
l_3^p m_3'^p &\equiv 1 \pmod{\theta'_4} \\
l_3'^{-2p} m_3'^p &\equiv -1 \pmod{\theta'_4} \\
l_3'^p m_3'^{-2p} &\equiv -1 \pmod{\theta'_4}
\end{aligned} \tag{129}$$

$$\begin{aligned}
m_3'^{3p} &\equiv l_3'^{3p} \pmod{\theta'_4} \\
m_3'^{3p} - l_3'^{3p} &\equiv (m_3'^p - l_3'^p)(m_3'^{2p} + l_3'^p m_3'^p + l_3'^{2p}) \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
-m_3'^p &\equiv l_3'^{2p} \pmod{\theta'_4} \\
l_3'^p &\equiv -m_3'^{2p} \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
l_3'^p - m_3'^p &\equiv l_3'^{2p} - m_3'^{2p} \pmod{\theta'_4} \\
l_3'^p - m_3'^p &\equiv (l_3'^p + m_3'^p)(l_3'^p - m_3'^p) \pmod{\theta'_4} \\
1 &\equiv l_3'^p + m_3'^p \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
(l_3'^p + m_3'^p)^2 &\equiv 1^2 \pmod{\theta'_4} \\
l_3'^{2p} + 2l_3'^p m_3'^p + m_3'^{2p} &\equiv 1 \pmod{\theta'_4} \\
l_3'^{2p} + 2l_3'^p m_3'^p + m_3'^{2p} &\equiv l_3'^p m_3'^p \pmod{\theta'_4} \\
l_3'^{2p} + l_3'^p m_3'^p + m_3'^{2p} &\equiv 0 \pmod{\theta'_4}
\end{aligned}$$

$m_3'^p - l_3'^p \not\equiv 0 \pmod{\theta'_4}$ ないので $m_3' \equiv 1 \pmod{\theta'_4}$, $l_3' \equiv 1 \pmod{\theta'_4}$ のとき
 $x^p + y^p \not\equiv z^p \pmod{\theta'_4}$

$$\begin{aligned}
l_3'^p + m_3'^p &\equiv 1 \pmod{\theta'_4} \\
l_3'^{2p} + l_3'^p m_3'^p &\equiv l_3'^p \pmod{\theta'_4} \\
l_3'^{2p} - l_3'^p + 1 &\equiv 0 \pmod{\theta'_4}
\end{aligned}$$

(100)(110)(121) より

$$\begin{aligned}
-m_1'^{-1} x z^{p-1} &\equiv -m_3' x z^{p-1} \pmod{\delta'} \\
m_1'^{-1} &\equiv m_3' \pmod{\delta'} \\
1 &\equiv m_1^p m_3'^p \pmod{\delta'}
\end{aligned} \tag{130}$$

$$\begin{aligned}
-l_3'^{-1} z y^{p-1} &\equiv -m_2' z y^{p-1} \pmod{\delta'} \\
l_3'^{-1} &\equiv m_2' \pmod{\delta'}
\end{aligned} \tag{131}$$

$l_3'^p m_3'^p \equiv 1 \pmod{\theta'_4}$ ないので

$$l_3'^p \equiv \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \tag{132}$$

$$m_3'^p \equiv \frac{1 \mp \sqrt{-3}}{2} \pmod{\theta'_4} \tag{133}$$

1.9.8 A splice

(105) より

$$\begin{aligned}
x^2 &\equiv l'_1 m'_1 y z \pmod{\theta'_4} \\
-x^2 &\equiv l'_1 y \cdot -m'_1 z \pmod{\theta'_4} \\
-x^2 &\equiv (y + k'_1)(-z + k'_1) \pmod{\theta'_4} \\
-x^2 &\equiv -yz + (y - z)k'_1 + k_1'^2 \pmod{\theta'_4} \\
0 &\equiv k_1'^2 + (y - z)k'_1 - yz + x^2 \pmod{\theta'_4}
\end{aligned}$$

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

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

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

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

$$\begin{aligned}
-z^p &\equiv x^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\
-y^p &\equiv x^p \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4}
\end{aligned} \tag{134}$$

$$\begin{aligned}
y &\equiv xl_1'^{-1} \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\
-z &\equiv xm_1'^{-1} \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4}
\end{aligned}$$

(118)(130) より

$$\begin{aligned}
y &\equiv xl_2' \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\
-z &\equiv xm_3' \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4}
\end{aligned}$$

$$\begin{aligned}
y^p &\equiv x^p l_2'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta'_4} \\
-z^p &\equiv x^p m_3'^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta'_4}
\end{aligned}$$

(134) より

$$\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv l_2'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta'_4} \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv m_3'^p \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta'_4}
\end{aligned}$$

(119)(133) より

$$\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \mp \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^{6n+3} \pmod{\theta'_4} \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \mp \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^{6n+3} \pmod{\theta'_4}
\end{aligned}$$

$l_1'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta'_4}$ のとき

$$\begin{aligned}
\frac{-1 \mp \sqrt{-3}}{2} &\equiv \frac{-1 \pm \sqrt{-3}}{2} \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^{6n+1} \pmod{\theta'_4} \\
\frac{-1 \pm \sqrt{-3}}{2} &\equiv \frac{1 \pm \sqrt{-3}}{2} \cdot \left(\frac{1 \pm \sqrt{-3}}{2} \right)^{6n+1} \pmod{\theta'_4}
\end{aligned}$$

(116) より

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

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

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

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

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

(134) より $\pm$ の調整

$$\begin{aligned}
-z^p &\equiv y^p \cdot \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta'_4} \\
-x^p &\equiv y^p \cdot \frac{1 \mp \sqrt{-3}}{2} \pmod{\theta'_4}
\end{aligned} \tag{135}$$

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

(118)(131) より

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

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

(135) より

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

(108)(132) より

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

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

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

(128) より

$$\begin{aligned}
z^2 &\equiv l'_3 m'_3 xy \pmod{\theta'_4} \\
-z^2 &\equiv -m'_3 x \cdot l'_3 y \pmod{\theta'_4} \\
-z^2 &\equiv (-x + k''_3)(y + k''_3) \pmod{\theta'_4} \\
-z^2 &\equiv -xy + (y - x)k''_3 + k''_3{}^2 \pmod{\theta'_4} \\
0 &\equiv k''_3{}^2 + (y - x)k''_3 - xy + z^2 \pmod{\theta'_4} \\
\\
k''_3 &\equiv \frac{x - y \pm \sqrt{(y - x)^2 - 4(-xy + z^2)}}{2} \pmod{\theta'_4} \\
k''_3 &\equiv \frac{x - y \pm \sqrt{(y + x)^2 - 4z^2}}{2} \pmod{\theta'_4} \\
k''_3 &\equiv \frac{x - y \pm \sqrt{z^2 - 4z^2}}{2} \pmod{\theta'_4} \\
k''_3 &\equiv \frac{x - y \pm \sqrt{-3z^2}}{2} \pmod{\theta'_4} \\
\\
y + k''_3 &\equiv \frac{x + y \pm \sqrt{-3z^2}}{2} \pmod{\theta'_4} \\
-x + k''_3 &\equiv \frac{-x - y \pm \sqrt{-3z^2}}{2} \pmod{\theta'_4} \\
\\
l'_3 y &\equiv z \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\
-m'_3 x &\equiv z \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\
\\
l'_3 y z^{p-1} &\equiv z^p \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\
-m'_3 x z^{p-1} &\equiv z^p \cdot \frac{1 \pm \sqrt{-3}}{2} \pmod{\theta'_4}
\end{aligned}$$

(134) より $\pm$ の調整

$$\begin{aligned}
-x^p &\equiv z^p \cdot \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta'_4} \\
y^p &\equiv z^p \cdot \frac{1 \mp \sqrt{-3}}{2} \pmod{\theta'_4}
\end{aligned} \tag{136}$$

$$\begin{aligned} y &\equiv z l_3'^{-1} \cdot \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta'_4} \\ -x &\equiv z m_3'^{-1} \cdot \frac{1 \mp \sqrt{-3}}{2} \pmod{\theta'_4} \end{aligned}$$

(131)(130) より

$$\begin{aligned} y &\equiv z m_2' \cdot \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta'_4} \\ x &\equiv z m_1' \cdot \frac{-1 \pm \sqrt{-3}}{2} \pmod{\theta'_4} \\ y^p &\equiv z^p m_2'^p \cdot \left(\frac{-1 \mp \sqrt{-3}}{2} \right)^p \pmod{\theta'_4} \\ x^p &\equiv z^p m_1'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta'_4} \end{aligned}$$

(136) より

$$\begin{aligned} \frac{1 \mp \sqrt{-3}}{2} &\equiv m_2'^p \cdot \left(\frac{-1 \mp \sqrt{-3}}{2} \right)^p \pmod{\theta'_4} \\ \frac{1 \pm \sqrt{-3}}{2} &\equiv m_1'^p \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^p \pmod{\theta'_4} \end{aligned}$$

(120)(109) より

$$\begin{aligned} \frac{1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{1 \mp \sqrt{-3}}{2} \right) \cdot \left(\frac{-1 \mp \sqrt{-3}}{2} \right)^{6n+3} \pmod{\theta'_4} \\ \frac{1 \pm \sqrt{-3}}{2} &\equiv \left(\frac{1 \pm \sqrt{-3}}{2} \right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^{6n+3} \pmod{\theta'_4} \end{aligned}$$

$l_1'^p \equiv \frac{-1 \mp \sqrt{-3}}{2} \pmod{\theta'_4}$ のとき

$$\begin{aligned} \frac{1 \mp \sqrt{-3}}{2} &\equiv \left(\frac{1 \pm \sqrt{-3}}{2} \right) \cdot \left(\frac{-1 \mp \sqrt{-3}}{2} \right)^{6n+1} \pmod{\theta'_4} \\ \frac{1 \pm \sqrt{-3}}{2} &\equiv \left(\frac{1 \mp \sqrt{-3}}{2} \right) \cdot \left(\frac{-1 \pm \sqrt{-3}}{2} \right)^{6n+1} \pmod{\theta'_4} \end{aligned}$$

1.9.9 $p = 6n + 1$ のとき

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

(105)(116)(128) より

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

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

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

$$-z^3 \equiv x^3 \equiv y^3 \pmod{\theta_4'}$$

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

$x + z + y \equiv 0 \pmod{\theta_4'}$ なので

$$x + z \not\equiv 0 \pmod{\theta_4'}$$

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

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 $n = 0$, $p = 3$ 、 $x^3 + y^3 \equiv z^3 \pmod{\theta'_4}$

$$(x + z + y)^3 \equiv x^3 + z^3 + y^3 + 3x^2y + 3x^2z + 3xy^2 + 3xz^2 + 3y^2z + 3yz^2 + 6xyz \pmod{\theta'_4}$$

$$(x + z + y)^3 \equiv 2z^3 + 3(x^2y + x^2z + xy^2 + xz^2 + y^2z + yz^2 + 2xyz) \pmod{\theta'_4}$$

$$(x + z + y)^3 \equiv 2z^3 + 3(y(x^2 + 2xz + z^2) + (x + z)xz + (x + z)y^2) \pmod{\theta'_4}$$

$$(x + z + y)^3 \equiv 2z^3 + 3(y(x + z)^2 + (x + z)xz + (x + z)y^2) \pmod{\theta'_4}$$

$$(x + z + y)^3 \equiv 2z^3 + 3(x + z)(xy + yz + xz + y^2) \pmod{\theta'_4}$$

$$(x + z + y)^3 \equiv 2z^3 + 3(x + z)(x(y + z) + y(y + z)) \pmod{\theta'_4}$$

$$(x + z + y)^3 \equiv 2z^3 + 3(x + z)(y + z)(y + x) \pmod{\theta'_4}$$

$$0 \equiv 2z^3 - 3yxz \pmod{\theta'_4}$$

$$2z^2 \equiv 3xy \pmod{\theta'_4}$$

(128) より

$$2l'_3m'_3xy \equiv 3xy \pmod{\theta'_4}$$

$$2l'_3m'_3 \equiv 3 \pmod{\theta'_4}$$

$$2^p l'^p_3 m'^p_3 \equiv 3^p \pmod{\theta'_4}$$

(129) より

$$2^3 \equiv 3^3 \pmod{\theta'_4}$$

$$8 \equiv 27 \pmod{\theta'_4}$$

$$0 \equiv 19 \pmod{\theta'_4}$$

$$x + z + y \equiv 0 \pmod{19}$$

$x + z - y \equiv 0 \pmod{19}$ 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

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

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

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

$$2 \mid c$$

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

$$2 \perp \gamma$$

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

$$2^k = \gamma + p^{(p-1)n-1} c^{p-1} = \text{odd}$$

$$2^0 = 1$$

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

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