Solution Conditions

Hajime Mashima

Abstract

For Fermat's Last Theorem, the condition that holds when there is inverse element.

Contents

1 introduction

ある三乗数を二つの三乗数の和で表すこと、あるいはある四乗数を二つの四乗数の和で表すこと、および一般に二乗より大きいべきの数を同じべきの二つの数の和で表すことは不可能である。私はこの命題の真に驚くべき証明を持っているが、余白が狭すぎるのでここに記すことはできない。

1.1 $\delta \perp xyz$

Theorem 1 (Fermat's Last Theorem)

$$x^p + y^p \neq z^p \quad (p \geqq 3\ ,\ x\ ,\ y\ ,\ z \text{ は一つが偶数で互いに素})$$

Proposition 2 p は奇素数で次の等式 $x^p + y^p = z^p$ を満たすとき

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

Proof 3

$x^p + y^p - z^p = 0 \Rightarrow p \mid (x + y - z)^p$
よって　$p \mid (z - y)$ と置ける。一般的に

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

$p^2 \mid R \Rightarrow p \mid y^{p-1}$ となってしまうため

$$p^n \mid R \quad , \ (n = 1) \tag{1}$$

また、p を除く素数に関して

$$L \perp R \tag{2}$$

Definition 4 $p \perp abc$

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

$$(z - x) - (x + y) = b^p - c^p$$
$$(z - y) - 2x = b^p - c^p \equiv 0 \mod p$$

$p \mid L' \Leftrightarrow p \mid R'$ なので、$p^2 \mid b^p - c^p = L' \cdot R'$

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

よって、少なくとも

$$p^2 \mid x \tag{3}$$

$$(x - (z - y))^p = x^p - \frac{p!}{(p-1)!1!}x^{p-1}(z - y) + \frac{p!}{(p-2)!2!}x^{p-2}(z - y)^2 - \frac{p!}{(p-3)!3!}x^{p-3}(z - y)^3 + \cdots + \frac{p!}{1!(p-1)!}x(z - y)^{p-1} - (z - y)^p$$

$x^p = (z-y)\cdot p\alpha^p$ と置き、上式に代入する。

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

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \qquad (4)$$

(3) より $x = p^2 a\alpha$ と置けるので

$$\begin{aligned}(x-(z-y))^p &= (z-y)\cdot K\\ (p^2a\alpha - p^{p-1}a^p)^p &= p^{p-1}a^pK\\ \left(p^2a\left(\alpha - p^{p-3}a^{p-1}\right)\right)^p &= p^{p-1}a^pK\\ p^{2p}a^p(\alpha - p^{p-3}a^{p-1})^p &= p^{p-1}a^pK\\ p^{p+1}(\alpha - p^{p-3}a^{p-1})^p &= K\end{aligned}$$

$$p^{p+1} \mid K$$

(4)　, $p \perp \alpha^p$ より

$$p^n \mid K \quad , \ n=1 \text{ でなければならない。}$$

よって

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

一般的に

$$p^n \mid x \ \ (n \geqq 2) \Rightarrow p^{pn} \mid x^p \quad \Rightarrow \quad p^{pn-1} \mid L$$

$$\begin{aligned}(x-(z-y))^p &= (z-y)\cdot K\\ (p^na\alpha - p^{pn-1}a^p)^p &= p^{pn-1}a^pK\\ \left(p^na\left(\alpha - p^{pn-1-n}a^{p-1}\right)\right)^p &= p^{pn-1}a^pK\\ p^{pn}a^p(\alpha - p^{pn-1-n}a^{p-1})^p &= p^{pn-1}a^pK\\ p(\alpha - p^{n(p-1)-1}a^{p-1})^p &= K\end{aligned}$$

$$(\alpha - p^{n(p-1)-1}a^{p-1}) \perp p$$

$$p^n \mid K \quad , \ (n=1)$$

□

また

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

$$p^n \mid x+y-z$$

1.1.1 $p \mid x$

$$
\begin{aligned}
x &= p^n a\alpha & z - y &= p^{pn-1}a^p \\
y &= b\beta & z - x &= b^p \\
z &= c\gamma & x + y &= c^p \\
p &\perp a\alpha yzS & 2 &\perp \delta
\end{aligned}
$$

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

Proof 6

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

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

$\delta \mid S \quad , \delta \mid a$ ならば矛盾する。よって

$$\delta \perp x$$

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

$\delta \mid bc$ ならば $\delta \mid 2x$ でなければならず矛盾する。よって

$$\delta \perp bc$$

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

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

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

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

よって $$\delta \perp \beta$$

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

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

よって $$\delta \perp \gamma$$ □

1.1.2 $p \perp x$

$$x = a'\alpha' \qquad z - y = a'^p$$
$$y = b'\beta' \qquad z - x = b'^p$$
$$z = c'\gamma' \qquad x + y = c'^p$$
$$p \perp xyzS' (※\, p \mid x - z + y) \qquad 2 \perp \delta$$

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

Proof 8

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

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

$\delta \mid S'$,$\delta \mid a'$ ならば矛盾する。よって

$$\delta \perp x$$

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

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

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

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

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

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

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

よって $$\delta \perp \beta'$$

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

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

よって $$\delta \perp \gamma'$$ □

1.2 解の条件 (Solution conditions)

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

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

$$\begin{aligned} z^p - y^p + Uz^{p-1} &\equiv Ty^{p-1} \mod \theta \\ z^p + Uz^{p-1} &\equiv Ty^{p-1} + y^p \mod \theta \\ z^{p-1}(z+U) &\equiv y^{p-1}(T+y) \mod \theta \\ z^{p-1}(yz+yU) &\equiv y \cdot y^{p-1}(T+y) \mod \theta \end{aligned} \tag{5}$$

$y^p z^p \equiv Uz^{p-1}Ty^{p-1} \mod \theta$ のとき

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

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

同様に

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

よって (**??**)、$yz \equiv UT \mod \theta$ を満たすとき解の候補は以下の 2 通りである。

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

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

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

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

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

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

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

同様に

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

よって (5)、$xz \equiv U'T' \mod \theta$ を満たすとき解の候補は以下の 2 通りである。

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

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

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

$$\begin{aligned} -U"y^{p-1} - T"x^{p-1} &\equiv x^p + y^p \mod \theta \\ -x^p - T"x^{p-1} &\equiv U"y^{p-1} + y^p \mod \theta \\ -x^{p-1}(x + T") &\equiv y^{p-1}(U" + y) \mod \theta \\ -x^{p-1}(xy + T"y) &\equiv y \cdot y^{p-1}(U" + y) \mod \theta \end{aligned} \tag{7}$$

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

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

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

同様に

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

よって (6)、$xy \equiv U"T" \mod \theta$ を満たすとき解の候補は以下の 2 通りである。

$$\begin{gathered} -U"y^{p-1} \equiv x^p \mod \theta \\ -T"x^{p-1} \equiv y^p \mod \theta \\ or \\ -U"y^{p-1} \equiv y^p \mod \theta \\ -T"x^{p-1} \equiv x^p \mod \theta \end{gathered}$$

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

【Solution conditions】

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

(5),(6),(7) から

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

$x-y\equiv -z \mod \delta$ より

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

$$yz^{p-1}\equiv y^p \mod \delta \Rightarrow -xz^{p-1}\equiv x^p \mod \delta$$

なので

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

よって

$-x^{p-1}\equiv y^{p-1}\equiv z^{p-1} \mod \delta$ は同時に成り立つ。

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

$$\begin{aligned} z-y &\not\equiv 0 \mod \delta \\ z-x &\not\equiv 0 \mod \delta \\ x+y &\not\equiv 0 \mod \delta \end{aligned} \tag{8}$$

また $p-1=2n$ より

$$z\equiv -y \mod \theta \implies z^{p-1}\equiv y^{p-1} \mod \theta$$

1 組を例とする全ての条件 (*Solution conditions is not applicable)

$$\begin{aligned} z^{p-1} &\equiv y^{p-1} \mod \theta \quad \wedge \quad -z \equiv y \mod \theta \\ z^{p-1} &\equiv y^{p-1} \mod \theta \quad \wedge \quad -z \not\equiv y \mod \theta \\ z^{p-1} &\not\equiv y^{p-1} \mod \theta \quad \wedge \quad -z \equiv y \mod \theta \\ {*}z^{p-1} &\not\equiv y^{p-1} \mod \theta \quad \wedge \quad -z \not\equiv y \mod \theta \end{aligned}$$

Definition 9 以降、例として $x^{p-1}\not\equiv y^{p-1}\not\equiv z^{p-1} \mod \theta$ と省略して記述する場合、$x^{p-1}\not\equiv z^{p-1} \mod \theta$ とも意味する。

1.3 同値変換 (Equivalence transformation)

s, t, u を変数とおく。
$\theta \perp stuxyz$ 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。

Definition 10 【Actual conditions】

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

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

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

このとき以下を同値変換の成立条件と呼び、以降 [ ] で示す。

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

1.4 一般解の条件 (General solution conditions)

Definition 11 以下の関係式を General solution conditions と呼ぶ。
3 組の Actual conditions の同値変換の成立条件が共通のとき変換できる。

$$\begin{aligned} (u_3 - t_2)x^{p-1} &\quad +t_2x^{p-1} &&\equiv u_3x^{p-1} \mod \theta \\ s_3y^{p-1} &\quad +(u_2 - s_3)y^{p-1} &&\equiv u_2y^{p-1} \mod \theta \\ s_2z^{p-1} &\quad +t_3z^{p-1} &&\equiv (s_2 + t_3)z^{p-1} \mod \theta \end{aligned}$$

1.4.1 $-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \theta_{l1}$ のとき

$$\begin{aligned} s_1x^{p-1} &\quad -t_2y^{p-1} &&\equiv -u_3z^{p-1} \mod \theta_{l1} \\ -s_3x^{p-1} &\quad +t_1y^{p-1} &&\equiv u_2z^{p-1} \mod \theta_{l1} \\ -s_2x^{p-1} &\quad +t_3y^{p-1} &&\equiv u_1z^{p-1} \mod \theta_{l1} \end{aligned}$$

$\mod \theta_{l1}$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p &\quad -yx^{p-1} &&\equiv -zx^{p-1} \mod \theta_{l1} \\ -xy^{p-1} &\quad +y^p &&\equiv zy^{p-1} \mod \theta_{l1} \\ -xz^{p-1} &\quad +yz^{p-1} &&\equiv z^p \mod \theta_{l1} \end{aligned} \tag{9}$$

1.4.2 Common to $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta_{r1}$

(9) より

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \delta \\ &\Leftrightarrow \\ x^p \quad -yx^{p-1} \quad &\equiv -zx^{p-1} \mod \theta_{l1} \\ x^p \quad +zx^{p-1} \quad &\equiv yx^{p-1} \mod \theta_{r1} \end{aligned}$$

$$\begin{aligned} -yx^{p-1} \cdot -zx^{p-1} \quad &\equiv y^p z^p \mod \delta \\ \left(x^{p-1}\right)^2 \quad &\equiv y^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{10}$$

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \delta \\ &\Leftrightarrow \\ -xy^{p-1} \quad +y^p \quad &\equiv zy^{p-1} \mod \theta_{l1} \\ -zy^{p-1} \quad +y^p \quad &\equiv xy^{p-1} \mod \theta_{r1} \end{aligned}$$

$$\begin{aligned} -xy^{p-1} \cdot zy^{p-1} \quad &\equiv x^p z^p \mod \delta \\ \left(y^{p-1}\right)^2 \quad &\equiv -x^{p-1} z^{p-1} \mod \delta \end{aligned} \tag{11}$$

$$\begin{aligned} x^p \quad +y^p \quad &\equiv z^p \mod \delta \\ &\Leftrightarrow \\ -xz^{p-1} \quad +yz^{p-1} \quad &\equiv z^p \mod \theta_{l1} \\ yz^{p-1} \quad -xz^{p-1} \quad &\equiv z^p \mod \theta_{r1} \end{aligned}$$

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

(10)(11)(12) より

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

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

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

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

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

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

$\delta \perp 3AB$ なので

$$\text{2 つの因数のうち、一方は } \delta \text{ と互いに素である。} \tag{13}$$

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

【Actual conditions】
$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \theta_{l1}$ のとき

$$\begin{aligned}
x^p \quad &+y^p &&\equiv z^p \mod \theta_{l1} \\
-xz^{p-1} \quad &-yx^{p-1} &&\equiv zy^{p-1} \mod \theta_{l1} \\
-xy^{p-1} \quad &+yz^{p-1} &&\equiv -zx^{p-1} \mod \theta_{l1}
\end{aligned}$$

$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta_{r1}$ のとき

$$\begin{aligned}
x^p \quad &+y^p &&\equiv z^p \mod \theta_{r1} \\
yz^{p-1} \quad &+zx^{p-1} &&\equiv xy^{p-1} \mod \theta_{r1} \\
-zy^{p-1} \quad &-xz^{p-1} &&\equiv yx^{p-1} \mod \theta_{r1}
\end{aligned}$$

1.4.3 $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta_{r1}$

$$
\begin{aligned}
(x^{p-1})^2 + (z^{p-1})^2 + (y^{p-1})^2 &\equiv 0 \mod \theta_{r1} \\
(x^{p-1})^2 - x^{p-1}y^{p-1} - x^{p-1}z^{p-1} &\equiv 0 \mod \theta_{r1} \\
x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \mod \theta_{r1}
\end{aligned}
$$

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

$$
\begin{aligned}
s''_1 x + t''_1 y &\equiv u''_1 z \mod \theta \\
s''_2 z + t''_2 x &\equiv u''_2 y \mod \theta \\
s''_3 y + t''_3 z &\equiv u''_3 x \mod \theta
\end{aligned}
$$

1.4.4 $-y \equiv z \equiv x \mod \theta_{l2}$ のとき

$$
\begin{aligned}
s''_1 x + t''_1 y &\equiv u''_1 z \mod \theta_{l2} \\
s''_2 x - t''_2 y &\equiv -u''_2 z \mod \theta_{l2} \\
-s''_3 x - t''_3 y &\equiv u''_3 z \mod \theta_{l2}
\end{aligned}
$$

$\mod \theta_{l2}$ として

$$
\begin{array}{llll}
s''_1 \equiv x^{p-1} & , \ t''_1 \equiv y^{p-1} & , \ u''_1 \equiv z^{p-1} \\
s''_2 \equiv x^{p-1} & , \ t''_2 \equiv -y^{p-1} & , \ u''_2 \equiv -z^{p-1} \\
s''_3 \equiv -x^{p-1} & , \ t''_3 \equiv -y^{p-1} & , \ u''_3 \equiv z^{p-1}
\end{array}
$$

$$[x^{p-1} - y^{p-1} - z^{p-1} \equiv 0 \mod \theta_{r1}]$$

【General solution conditions】

$$
\begin{array}{llll}
x^p & -y^{p-1}x & \equiv z^{p-1}x & \mod \theta_{l2} \\
-x^{p-1}y & +y^p & \equiv -z^{p-1}y & \mod \theta_{l2} \\
x^{p-1}z & -y^{p-1}z & \equiv z^p & \mod \theta_{l2}
\end{array}
\tag{14}
$$

1.4.5 Common to $-y \not\equiv z \not\equiv x \mod \theta_{r2}$

(14) より

$$\begin{aligned} -xy^{p-1} \cdot xz^{p-1} &\equiv y^p z^p \mod \theta_{r1} \\ -x^2 &\equiv yz \mod \theta_{r1} \\ x^2 &\equiv -yz \mod \theta_{r1} \end{aligned} \tag{15}$$

$$\begin{aligned} (10) \text{ より } \left(x^{p-1}\right)^2 &\equiv y^{p-1}z^{p-1} \mod \theta_{r1} \\ \left(x^2\right)^{p-1} &\equiv y^{p-1}z^{p-1} \mod \theta_{r1} \\ (-yz)^{p-1} &\equiv y^{p-1}z^{p-1} \mod \theta_{r1} \\ y^{p-1}z^{p-1} &\equiv y^{p-1}z^{p-1} \mod \theta_{r1} \end{aligned}$$

....

$$\begin{aligned} -yx^{p-1} \cdot -yz^{p-1} &\equiv x^p z^p \mod \theta_{r1} \\ y^2 &\equiv xz \mod \theta_{r1} \end{aligned} \tag{16}$$

$$\begin{aligned} (11) \text{ より } \left(y^{p-1}\right)^2 &\equiv -x^{p-1}z^{p-1} \mod \theta_{r1} \\ \left(y^2\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_{r1} \\ (xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_{r1} \\ x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_{r1} \end{aligned}$$

δ の定義に反する。

....

$$\begin{aligned} zx^{p-1} \cdot -zy^{p-1} &\equiv x^p y^p \mod \theta_{r1} \\ -z^2 &\equiv xy \mod \theta_{r1} \\ z^2 &\equiv -xy \mod \theta_{r1} \end{aligned} \tag{17}$$

$$\begin{aligned} (12) \text{ より } \left(z^{p-1}\right)^2 &\equiv -x^{p-1}y^{p-1} \mod \theta_{r1} \\ \left(z^2\right)^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \theta_{r1} \\ (-xy)^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \theta_{r1} \\ x^{p-1}y^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \theta_{r1} \end{aligned}$$

δ の定義に反するので $\theta_{r1} \neq \delta$

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

よって $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \delta$ のとき
$-y \equiv z \equiv x \mod \delta$ or $-y \not\equiv z \not\equiv x \mod \delta$ は成り立たないので $\theta_{l1} = \delta$

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

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。
【Actual conditions】

$$s'_1 x^{p-2} + t'_1 y^{p-2} \equiv u'_1 z^{p-2} \mod \theta$$

$$s'_2 z^{p-2} + t'_2 x^{p-2} \equiv u'_2 y^{p-2} \mod \theta$$

$$s'_3 y^{p-2} + t'_3 z^{p-2} \equiv u'_3 x^{p-2} \mod \theta$$

1.4.6 $x^{p-2} \equiv y^{p-2} \equiv z^{p-2} \mod \theta_{L1}$ のとき

$$\begin{aligned} s'_1 x^{p-2} + t'_1 y^{p-2} &\equiv u'_1 z^{p-2} \mod \theta_{L1} \\ s'_2 x^{p-2} + t'_2 y^{p-2} &\equiv u'_2 z^{p-2} \mod \theta_{L1} \\ s'_3 x^{p-2} + t'_3 y^{p-2} &\equiv u'_3 z^{p-2} \mod \theta_{L1} \end{aligned}$$

$\mod \theta_{L1}$ として

$$\begin{aligned} s'_1 &\equiv x^2 \quad , \ t'_1 \equiv y^2 \quad , \ u'_1 \equiv z^2 \\ s'_2 &\equiv x^2 \quad , \ t'_2 \equiv y^2 \quad , \ u'_2 \equiv z^2 \\ s'_3 &\equiv x^2 \quad , \ t'_3 \equiv y^2 \quad , \ u'_3 \equiv z^2 \end{aligned}$$

$$[x^2 + y^2 - z^2 \equiv 0 \mod \theta_0]$$

【General solution conditions】

$$\begin{aligned} x^p \quad + y^2 x^{p-2} &\equiv z^2 x^{p-2} \mod \theta_{L1} \\ x^2 y^{p-2} \quad + y^p &\equiv z^2 y^{p-2} \mod \theta_{L1} \\ x^2 z^{p-2} \quad + y^2 z^{p-2} &\equiv z^p \mod \theta_{L1} \end{aligned} \tag{18}$$

1.4.7 Common to $x^{p-2} \not\equiv y^{p-2} \not\equiv z^{p-2} \mod \theta_{R1}$

(18) より

$$\begin{aligned} x^p &+ y^2 x^{p-2} &\equiv z^2 x^{p-2} &\mod \theta_{L1} \\ x^p &- z^2 x^{p-2} &\equiv -y^2 x^{p-2} &\mod \theta_{R1} \end{aligned}$$

$$\begin{aligned} y^2 x^{p-2} \cdot z^2 x^{p-2} &\equiv y^p z^p \mod \theta_0 \\ \left(x^{p-2}\right)^2 &\equiv y^{p-2} z^{p-2} \mod \theta_0 \end{aligned} \tag{19}$$

$$\begin{aligned} x^2 y^{p-2} &+ y^p &\equiv z^2 y^{p-2} &\mod \theta_{L1} \\ -z^2 y^{p-2} &+ y^p &\equiv -x^2 y^{p-2} &\mod \theta_{R1} \end{aligned}$$

$$\begin{aligned} x^2 y^{p-2} \cdot z^2 y^{p-2} &\equiv x^p z^p \mod \theta_0 \\ \left(y^{p-2}\right)^2 &\equiv x^{p-2} z^{p-2} \mod \theta_0 \end{aligned} \tag{20}$$

$$\begin{aligned} x^2 z^{p-2} &+ y^2 z^{p-2} &\equiv z^p &\mod \theta_{L1} \\ y^2 z^{p-2} &+ x^2 z^{p-2} &\equiv z^p &\mod \theta_{R1} \end{aligned}$$

$$\begin{aligned} x^2 z^{p-2} \cdot y^2 z^{p-2} &\equiv x^p y^p \mod \theta_0 \\ \left(z^{p-2}\right)^2 &\equiv x^{p-2} y^{p-2} \mod \theta_0 \end{aligned} \tag{21}$$

(19)(20)(21) より

$$\left(x^{p-2}\right)^3 \equiv \left(y^{p-2}\right)^3 \equiv \left(z^{p-2}\right)^3 \mod \theta_0$$

$$\begin{aligned}
\left(z^{p-2}\right)^3 - \left(y^{p-2}\right)^3 &\equiv (z^{p-2} - y^{p-2})((z^{p-2})^2 + y^{p-2}z^{p-2} + (y^{p-2})^2) \equiv 0 \mod \theta_0 \\
\left(x^{p-2}\right)^3 - \left(z^{p-2}\right)^3 &\equiv (x^{p-2} - z^{p-2})((x^{p-2})^2 + x^{p-2}z^{p-2} + (z^{p-2})^2) \equiv 0 \mod \theta_0 \\
\left(x^{p-2}\right)^3 - \left(y^{p-2}\right)^3 &\equiv (x^{p-2} - y^{p-2})((x^{p-2})^2 + x^{p-2}y^{p-2} + (y^{p-2})^2) \equiv 0 \mod \theta_0
\end{aligned}$$

1.4.8 $x^{p-2} \not\equiv y^{p-2} \not\equiv z^{p-2} \mod \theta_{R1}$

$$\begin{aligned}
(x^{p-2})^2 + (z^{p-2})^2 + (y^{p-2})^2 &\equiv 0 \mod \theta_{R1} \\
(x^{p-2})^2 + x^{p-2}y^{p-2} + x^{p-2}z^{p-2} &\equiv 0 \mod \theta_{R1} \\
x^{p-2} + y^{p-2} + z^{p-2} &\equiv 0 \mod \theta_{R1} \\
x^{p-2} + y^{p-2} &\equiv -z^{p-2} \mod \theta_{R1}
\end{aligned}$$

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。

$$\begin{aligned}
s''_1x^2 + t''_1y^2 &\equiv u''_1z^2 \mod \theta \\
s''_2z^2 + t''_2x^2 &\equiv u''_2y^2 \mod \theta \\
s''_3y^2 + t''_3z^2 &\equiv u''_3x^2 \mod \theta
\end{aligned}$$

1.4.9 $-z^2 \equiv x^2 \equiv y^2 \mod \theta_{L2}$ のとき

$$\begin{aligned}
s''_1x^2 + t''_1y^2 &\equiv u''_1z^2 \mod \theta_{L2} \\
-s''_2x^2 + t''_2y^2 &\equiv -u''_2z^2 \mod \theta_{L2} \\
s''_3x^2 - t''_3y^2 &\equiv -u''_3z^2 \mod \theta_{L2}
\end{aligned}$$

$\mod \theta_{L2}$ として

$$\begin{aligned}
s''_1 &\equiv x^{p-2} \quad , \quad t''_1 \equiv y^{p-2} \quad , \quad u''_1 \equiv z^{p-2} \\
s''_2 &\equiv -x^{p-2} \quad , \quad t''_2 \equiv y^{p-2} \quad , \quad u''_2 \equiv -z^{p-2} \\
s''_3 &\equiv x^{p-2} \quad , \quad t''_3 \equiv -y^{p-2} \quad , \quad u''_3 \equiv -z^{p-2}
\end{aligned}$$

$$[x^{p-2} + y^{p-2} + z^{p-2} \equiv 0 \mod \theta_{R1}]$$

【General solution conditions】

$$\begin{array}{rrl}
x^p & +x^2y^{p-2} & \equiv -x^2z^{p-2} \mod \theta_{L2} \\
y^2x^{p-2} & +y^p & \equiv -y^2z^{p-2} \mod \theta_{L2} \\
-z^2x^{p-2} & -z^2y^{p-2} & \equiv z^p \mod \theta_{L2}
\end{array} \tag{22}$$

1.4.10 Common to $-z^2 \not\equiv x^2 \not\equiv y^2 \mod \theta_{R2}$

(22) より

$$\begin{aligned} x^2 y^{p-2} \cdot -x^2 z^{p-2} &\equiv y^p z^p \mod \theta_0 \\ x^4 &\equiv -y^2 z^2 \mod \theta_0 \end{aligned} \tag{23}$$

$$\begin{aligned} (19)\text{ より } \left(x^{p-2}\right)^2 &\equiv y^{p-2} z^{p-2} \mod \theta_0 \\ \left(x^4\right)^{p-2} &\equiv \left(y^{p-2} z^{p-2}\right)^2 \mod \theta_0 \\ (23)\text{ より } \left(-y^2 z^2\right)^{p-2} &\equiv \left(y^{p-2} z^{p-2}\right)^2 \mod \theta_0 \\ -\left(y^{p-2} z^{p-2}\right)^2 &\equiv \left(y^{p-2} z^{p-2}\right)^2 \mod \theta_0 \end{aligned}$$

これは δ の定義に反する。

....

$$\begin{aligned} y^2 x^{p-2} \cdot -y^2 z^{p-2} &\equiv x^p z^p \mod \theta_0 \\ y^4 &\equiv -x^2 z^2 \mod \theta_0 \end{aligned} \tag{24}$$

$$\begin{aligned} (20)\text{ より } \left(y^{p-2}\right)^2 &\equiv x^{p-2} z^{p-2} \mod \theta_0 \\ \left(y^4\right)^{p-2} &\equiv \left(x^{p-2} z^{p-2}\right)^2 \mod \theta_0 \\ (24)\text{ より } \left(-x^2 z^2\right)^{p-2} &\equiv \left(x^{p-2} z^{p-2}\right)^2 \mod \theta_0 \\ -\left(x^{p-2} z^{p-2}\right)^2 &\equiv \left(x^{p-2} z^{p-2}\right)^2 \mod \theta_0 \end{aligned}$$

これは δ の定義に反する。

....

$$\begin{aligned} -z^2 x^{p-2} \cdot -z^2 y^{p-2} &\equiv x^p y^p \mod \theta_0 \\ z^4 &\equiv x^2 y^2 \mod \theta_0 \end{aligned} \tag{25}$$

$$\begin{aligned} (21)\text{ より } \left(z^{p-2}\right)^2 &\equiv x^{p-2} y^{p-2} \mod \theta_0 \\ \left(z^4\right)^{p-2} &\equiv \left(x^{p-2} y^{p-2}\right)^2 \mod \theta_0 \\ (25)\text{ より } \left(x^2 y^2\right)^{p-2} &\equiv \left(x^{p-2} y^{p-2}\right)^2 \mod \theta_0 \\ \left(x^{p-2} y^{p-2}\right)^2 &\equiv \left(x^{p-2} y^{p-2}\right)^2 \mod \theta_0 \end{aligned}$$

$$
\begin{aligned}
(x+z-y)^2 &\equiv 0 \mod \delta \\
x^2+y^2+z^2-2(xy-xz+yz) &\equiv 0 \mod \delta \\
x^2+y^2+z^2-2(xy+(y-x)z) &\equiv 0 \mod \delta \\
x^2+y^2+z^2-2(xy+z^2) &\equiv 0 \mod \delta \\
x^2+y^2-z^2-2xy &\equiv 0 \mod \delta \\
-2xy &\equiv 0 \mod \theta_0
\end{aligned}
$$

また $-x^{p-1} \equiv z^{p-1} \mod \delta$ ，$-x^{p-1} \equiv y^{p-1} \mod \delta$ ，$z^{p-1} \equiv y^{p-1} \mod \delta$ のとき (8) ，$-x \not\equiv z \mod \delta$ より

$$
\begin{aligned}
x^{p-2} \not\equiv z^{p-2} \mod \delta \\
x^{p-2} \not\equiv y^{p-2} \mod \delta \\
z^{p-2} \not\equiv y^{p-2} \mod \delta
\end{aligned}
$$

よって $\delta \neq \theta_0$ ，$\delta \neq \theta_{L1}$ なので $\delta = \theta_{R1}$ に属する。

1.4.11 $-z^2 \equiv x^2 \equiv y^2 \mod \delta$ or $-z^2 \not\equiv x^2 \not\equiv y^2 \mod \delta$ のとき

(23)(24)(25) より

$$x^6 \equiv y^6 \equiv -z^6 \mod \delta$$

$$
\begin{aligned}
z^6+y^6 &\equiv (z^2+y^2)(z^4-y^2z^2+y^4) \equiv 0 \mod \delta \\
x^6+z^6 &\equiv (x^2+z^2)(x^4-x^2z^2+z^4) \equiv 0 \mod \delta \\
x^6-y^6 &\equiv (x^2-y^2)(x^4+x^2y^2+y^4) \equiv 0 \mod \delta
\end{aligned}
$$

$$x^4+x^2y^2+y^4 \equiv 0 \mod \theta_{R2} \wedge x^p+y^p \equiv z^p \mod \theta_{R2}$$

が成り立つならば、$\theta_{R1} = \theta_{R2}$
(23)(24)(25) より

$$x^2+y^2-z^2 \equiv 0 \mod \theta_{R2}$$

これは $\theta_0 \neq \theta_{R1}$ と矛盾するので

$$x^p+y^p \not\equiv z^p \mod \theta_{R2}$$

よって $\delta \neq \theta_{R2}$ なので $\delta = \theta_{L2}$ に属する。

$$
\begin{aligned}
z^2+y^2 &\equiv 0 \mod \delta \\
x^2+z^2 &\equiv 0 \mod \delta \\
x^2-y^2 &\equiv 0 \mod \delta
\end{aligned}
$$

これは $x^2-y^2 \not\equiv 0 \mod \delta$ に反するので $\delta \neq \theta_{L2}$
以上より

$$\delta \neq odd$$

1.5 $\delta = 2$

1.5.1 $2 \mid x$, $2 \perp yz$

$S = 2^k$ のとき

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

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

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

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

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

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

$S' = 2^k$ のとき

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

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

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

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

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

しかし、$\alpha' + a'^{p-1} > 1$ なので矛盾する。

よって $2 \mid x$ のとき成り立たない。

1.6 $\delta' \perp xyz$

1.6.1 $p \mid z$

$$
\begin{aligned}
x &= a\alpha & y &= b\beta & z &= p^n c\gamma \\
z - y &= a^p & z - x &= b^p & x + y &= p^{pn-1}c^p \\
p &\perp xyc\gamma S" & & & 2 &\perp \delta'
\end{aligned}
$$

Proposition 12 $z + x + y = p^n cS"$, $\delta' \mid S" \Rightarrow \delta' \perp xyz$

Proof 13

$$
\begin{aligned}
z + x + y &= p^n c\gamma + p^{pn-1}c^p \\
&= p^n c(\gamma + p^{(p-1)n-1}c^{p-1})
\end{aligned}
$$

$$
\begin{aligned}
p\gamma^p = R &= py^{p-1} + (x+y)(\ldots) \\
R &\equiv py^{p-1} \mod c \\
py^{p-1} &\perp c \\
\gamma &\perp c
\end{aligned}
$$

$\delta' \mid S"$,$\delta' \mid c$ ならば矛盾する。よって

$$\delta' \perp z$$

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

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

$$\delta' \perp ab$$

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

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

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

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

よって $$\delta' \perp \beta$$

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

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

よって $$\delta' \perp \alpha$$ □

$x+y\equiv -z \mod \delta'$ より

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

$$-yz^{p-1}\equiv y^p \mod \delta' \Rightarrow -xz^{p-1}\equiv x^p \mod \delta'$$

なので

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

よって

$-z^{p-1}\equiv x^{p-1}\equiv y^{p-1} \mod \delta'$ は同時に成り立つ。

$$x\equiv y \mod \theta \implies x^{p-1}\equiv y^{p-1} \mod \theta$$

1 組を例とする全ての条件 (*Solution conditions is not applicable)

$$\begin{aligned} -z^{p-1} &\equiv y^{p-1} \mod \theta \wedge z \equiv y \mod \theta \\ -z^{p-1} &\equiv y^{p-1} \mod \theta \wedge z \not\equiv y \mod \theta \\ -z^{p-1} &\not\equiv y^{p-1} \mod \theta \wedge z \equiv y \mod \theta \\ *-z^{p-1} &\not\equiv y^{p-1} \mod \theta \wedge z \not\equiv y \mod \theta \end{aligned}$$

1.6.2 同値変換 (Equivalence transformation)

【Actual conditions】

$$\begin{aligned} (u_3-t_2)x^{p-1} &+t_2x^{p-1} \equiv u_3x^{p-1} \mod \theta \\ s_3y^{p-1} &+(u_2-s_3)y^{p-1} \equiv u_2y^{p-1} \mod \theta \\ s_2z^{p-1} &+t_3z^{p-1} \equiv (s_2+t_3)z^{p-1} \mod \theta \end{aligned}$$

1.6.3 $-z^{p-1}\equiv x^{p-1}\equiv y^{p-1} \mod \theta'_{l1}$ のとき

$$\begin{aligned} s_1x^{p-1} &+t_2y^{p-1} \equiv -u_3z^{p-1} \mod \theta'_{l1} \\ s_3x^{p-1} &+t_1y^{p-1} \equiv -u_2z^{p-1} \mod \theta'_{l1} \\ -s_2x^{p-1} &-t_3y^{p-1} \equiv u_1z^{p-1} \mod \theta'_{l1} \end{aligned}$$

$\mod \theta'_{l1}$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p &+yx^{p-1} \equiv -zx^{p-1} \mod \theta'_{l1} \\ xy^{p-1} &+y^p \equiv -zy^{p-1} \mod \theta'_{l1} \\ -xz^{p-1} &-yz^{p-1} \equiv z^p \mod \theta'_{l1} \end{aligned} \tag{26}$$

1.6.4 Common to $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \mod \theta'_{r1}$

(26) より

$$\begin{aligned} yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \mod \delta' \\ \left(x^{p-1}\right)^2 &\equiv -y^{p-1}z^{p-1} \mod \delta' \end{aligned} \tag{27}$$

$$\begin{aligned} xy^{p-1} \cdot -zy^{p-1} &\equiv x^p z^p \mod \delta' \\ \left(y^{p-1}\right)^2 &\equiv -x^{p-1}z^{p-1} \mod \delta' \end{aligned} \tag{28}$$

$$\begin{aligned} -xz^{p-1} \cdot -yz^{p-1} &\equiv x^p y^p \mod \delta' \\ \left(z^{p-1}\right)^2 &\equiv x^{p-1}y^{p-1} \mod \delta' \end{aligned} \tag{29}$$

(27)(28)(29) より

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

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

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

$$\begin{aligned} x \cdot x^{p-1} + y \cdot y^{p-1} \equiv z \cdot z^{p-1} &\mod 3 \\ x \equiv \pm 1 &\mod 3 \\ y \equiv \pm 1 &\mod 3 \\ z \equiv \mp 1 &\mod 3 \\ \delta' \neq 3 & \end{aligned}$$

(13) と同様

2 つの因数のうち、一方は δ' と互いに素である。 (30)

【Actual conditions】

$-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \mod \theta'_{l1}$ のとき

$$\begin{aligned} x^p \quad +y^p &\equiv z^p \mod \theta'_{l1} \\ -xz^{p-1} \quad +yx^{p-1} &\equiv -zy^{p-1} \mod \theta'_{l1} \\ xy^{p-1} \quad -yz^{p-1} &\equiv -zx^{p-1} \mod \theta'_{l1} \end{aligned}$$

$-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \mod \theta'_{r1}$ のとき

$$\begin{aligned} x^p \quad +y^p &\equiv z^p \mod \theta'_{r1} \\ -yz^{p-1} \quad +zx^{p-1} &\equiv -xy^{p-1} \mod \theta'_{r1} \\ zy^{p-1} \quad -xz^{p-1} &\equiv -yx^{p-1} \mod \theta'_{r1} \end{aligned}$$

1.6.5 $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \mod \theta'_{r1}$

$$
\begin{aligned}
(x^{p-1})^2 + (z^{p-1})^2 + (y^{p-1})^2 &\equiv 0 \mod \theta'_{r1} \\
(x^{p-1})^2 + x^{p-1}y^{p-1} - x^{p-1}z^{p-1} &\equiv 0 \mod \theta'_{r1} \\
x^{p-1} + y^{p-1} - z^{p-1} &\equiv 0 \mod \theta'_{r1}
\end{aligned}
$$

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

$$
\begin{aligned}
s''_1 x + t''_1 y &\equiv u''_1 z \mod \theta \\
s''_2 z + t''_2 x &\equiv u''_2 y \mod \theta \\
s''_3 y + t''_3 z &\equiv u''_3 x \mod \theta
\end{aligned}
$$

1.6.6 $z \equiv x \equiv y \mod \theta'_{l2}$ のとき

$$
\begin{aligned}
s''_1 x + t''_1 y &\equiv u''_1 z \mod \theta'_{l2} \\
s''_2 x + t''_2 y &\equiv u''_2 z \mod \theta'_{l2} \\
s''_3 x + t''_3 y &\equiv u''_3 z \mod \theta'_{l2}
\end{aligned}
$$

$\mod \theta'_{l2}$ として

$$
\begin{aligned}
s''_1 &\equiv x^{p-1} \quad , \quad t''_1 \equiv y^{p-1} \quad , \quad u''_1 \equiv z^{p-1} \\
s''_2 &\equiv x^{p-1} \quad , \quad t''_2 \equiv y^{p-1} \quad , \quad u''_2 \equiv z^{p-1} \\
s''_3 &\equiv x^{p-1} \quad , \quad t''_3 \equiv y^{p-1} \quad , \quad u''_3 \equiv z^{p-1}
\end{aligned}
$$

$$[x^{p-1} + y^{p-1} - z^{p-1} \equiv 0 \mod \theta'_{r1}]$$

【General solution conditions】

$$
\begin{aligned}
x^p \quad + xy^{p-1} &\equiv xz^{p-1} \mod \theta'_{l2} \\
yx^{p-1} \quad + y^p &\equiv yz^{p-1} \mod \theta'_{l2} \\
zx^{p-1} \quad + zy^{p-1} &\equiv z^p \mod \theta'_{l2}
\end{aligned}
\tag{31}
$$

1.6.7 Common to $z \not\equiv x \not\equiv y \mod \theta'_{r2}$

(31) より

$$\begin{aligned} xy^{p-1} \cdot xz^{p-1} &\equiv y^p z^p \mod \theta'_{r1} \\ x^2 &\equiv yz \mod \theta'_{r1} \end{aligned} \tag{32}$$

$$\begin{aligned} (27)\text{ より } \left(x^{p-1}\right)^2 &\equiv -y^{p-1}z^{p-1} \mod \theta'_{r1} \\ \left(x^2\right)^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta'_{r1} \\ (yz)^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta'_{r1} \\ y^{p-1}z^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta'_{r1} \end{aligned}$$

δ' の定義に反する。

. . . .

$$\begin{aligned} yx^{p-1} \cdot yz^{p-1} &\equiv x^p z^p \mod \theta'_{r1} \\ y^2 &\equiv xz \mod \theta'_{r1} \end{aligned} \tag{33}$$

$$\begin{aligned} (28)\text{ より } \left(y^{p-1}\right)^2 &\equiv -x^{p-1}z^{p-1} \mod \theta'_{r1} \\ \left(y^2\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta'_{r1} \\ (xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta'_{r1} \\ x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta'_{r1} \end{aligned}$$

δ' の定義に反する。

. . . .

$$\begin{aligned} zx^{p-1} \cdot zy^{p-1} &\equiv x^p y^p \mod \theta'_{r1} \\ z^2 &\equiv xy \mod \theta'_{r1} \end{aligned} \tag{34}$$

$$\begin{aligned} (29)\text{ より } \left(z^{p-1}\right)^2 &\equiv x^{p-1}y^{p-1} \mod \theta'_{r1} \\ \left(z^2\right)^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta'_{r1} \\ (xy)^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta'_{r1} \\ x^{p-1}y^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta'_{r1} \end{aligned}$$

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

よって $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \mod \delta'$ のとき
$z \equiv x \equiv y \mod \delta'$ or $z \not\equiv x \not\equiv y \mod \delta'$ は成り立たないので $\theta'_{l1} = \delta'$

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

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。
【Actual conditions】

$$s'_1 x^{p-2} + t'_1 y^{p-2} \equiv u'_1 z^{p-2} \mod \theta$$

$$s'_2 z^{p-2} + t'_2 x^{p-2} \equiv u'_2 y^{p-2} \mod \theta$$

$$s'_3 y^{p-2} + t'_3 z^{p-2} \equiv u'_3 x^{p-2} \mod \theta$$

1.6.8 $-y^{p-2} \equiv x^{p-2} \equiv z^{p-2} \mod \theta'_{L1}$ のとき

$$\begin{aligned} s'_1 x^{p-2} + t'_1 y^{p-2} &\equiv u'_1 z^{p-2} \mod \theta'_{L1} \\ s'_2 x^{p-2} - t'_2 y^{p-2} &\equiv -u'_2 z^{p-2} \mod \theta'_{L1} \\ -s'_3 x^{p-2} - t'_3 y^{p-2} &\equiv u'_3 z^{p-2} \mod \theta'_{L1} \end{aligned}$$

$\mod \theta'_{L1}$ として

$$\begin{array}{lll} s'_1 \equiv x^2 & , \ t'_1 \equiv y^2 & , \ u'_1 \equiv z^2 \\ s'_2 \equiv x^2 & , \ t'_2 \equiv -y^2 & , \ u'_2 \equiv -z^2 \\ s'_3 \equiv -x^2 & , \ t'_3 \equiv -y^2 & , \ u'_3 \equiv z^2 \end{array}$$

$$[x^2 - y^2 - z^2 \equiv 0 \mod \theta'_0]$$

【General solution conditions】

$$\begin{array}{llll} x^p & -y^2 x^{p-2} & \equiv z^2 x^{p-2} & \mod \theta'_{L1} \\ -x^2 y^{p-2} & +y^p & \equiv -z^2 y^{p-2} & \mod \theta'_{L1} \\ x^2 z^{p-2} & -y^2 z^{p-2} & \equiv z^p & \mod \theta'_{L1} \end{array} \tag{35}$$

1.6.9 Common to $-y^{p-2} \not\equiv x^{p-2} \not\equiv z^{p-2} \mod \theta'_{R1}$

(35) より

$$\begin{aligned} x^p \quad -y^2x^{p-2} &\equiv z^2x^{p-2} \mod \theta'_{L1} \\ x^p \quad -z^2x^{p-2} &\equiv y^2x^{p-2} \mod \theta'_{R1} \end{aligned}$$

$$\begin{aligned} -y^2x^{p-2}\cdot z^2x^{p-2} &\equiv y^pz^p \mod \theta'_0 \\ \left(x^{p-2}\right)^2 &\equiv -y^{p-2}z^{p-2} \mod \theta'_0 \end{aligned} \tag{36}$$

$$\begin{aligned} -x^2y^{p-2} \quad +y^p &\equiv -z^2y^{p-2} \mod \theta'_{L1} \\ z^2y^{p-2} \quad +y^p &\equiv x^2y^{p-2} \mod \theta'_{R1} \end{aligned}$$

$$\begin{aligned} -x^2y^{p-2}\cdot -z^2y^{p-2} &\equiv x^pz^p \mod \theta'_0 \\ \left(y^{p-2}\right)^2 &\equiv x^{p-2}z^{p-2} \mod \theta'_0 \end{aligned} \tag{37}$$

$$\begin{aligned} x^2z^{p-2} \quad -y^2z^{p-2} &\equiv z^p \mod \theta'_{L1} \\ -y^2z^{p-2} \quad +x^2z^{p-2} &\equiv z^p \mod \theta'_{R1} \end{aligned}$$

$$\begin{aligned} x^2z^{p-2}\cdot -y^2z^{p-2} &\equiv x^py^p \mod \theta'_0 \\ \left(z^{p-2}\right)^2 &\equiv -x^{p-2}y^{p-2} \mod \theta'_0 \end{aligned} \tag{38}$$

(36)(37)(38) より

$$-\left(y^{p-2}\right)^3 \equiv \left(x^{p-2}\right)^3 \equiv \left(z^{p-2}\right)^3 \mod \theta'_0$$

$$\begin{aligned}
\left(z^{p-2}\right)^3+\left(y^{p-2}\right)^3 &\equiv (z^{p-2}+y^{p-2})((z^{p-2})^2-y^{p-2}z^{p-2}+(y^{p-2})^2)\equiv 0 \mod \theta'_0\\
\left(x^{p-2}\right)^3-\left(z^{p-2}\right)^3 &\equiv (x^{p-2}-z^{p-2})((x^{p-2})^2+x^{p-2}z^{p-2}+(z^{p-2})^2)\equiv 0 \mod \theta'_0\\
\left(x^{p-2}\right)^3+\left(y^{p-2}\right)^3 &\equiv (x^{p-2}+y^{p-2})((x^{p-2})^2-x^{p-2}y^{p-2}+(y^{p-2})^2)\equiv 0 \mod \theta'_0
\end{aligned}$$

1.6.10 $-y^{p-2} \not\equiv x^{p-2} \not\equiv z^{p-2} \mod \theta'_{R1}$

$$\begin{aligned}
(x^{p-2})^2+(z^{p-2})^2+(y^{p-2})^2 &\equiv 0 \mod \theta'_{R1}\\
(x^{p-2})^2-x^{p-2}y^{p-2}+x^{p-2}z^{p-2} &\equiv 0 \mod \theta'_{R1}\\
x^{p-2}-y^{p-2}+z^{p-2} &\equiv 0 \mod \theta'_{R1}\\
x^{p-2}-y^{p-2} &\equiv -z^{p-2} \mod \theta'_{R1}
\end{aligned}$$

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。

$$\begin{aligned}
s''_1x^2+t''_1y^2 &\equiv u''_1z^2 \mod \theta'\\
s''_2z^2+t''_2x^2 &\equiv u''_2y^2 \mod \theta'\\
s''_3y^2+t''_3z^2 &\equiv u''_3x^2 \mod \theta'
\end{aligned}$$

1.6.11 $-x^2 \equiv y^2 \equiv z^2 \mod \theta'_{L2}$ **のとき**

$$\begin{aligned}
s''_1x^2+t''_1y^2 &\equiv u''_1z^2 \mod \theta'_{L2}\\
-s''_2x^2-t''_2y^2 &\equiv u''_2z^2 \mod \theta'_{L2}\\
-s''_3x^2+t''_3y^2 &\equiv -u''_3z^2 \mod \theta'_{L2}
\end{aligned}$$

$\mod \theta'_{L2}$ として

$$\begin{aligned}
s''_1 &\equiv x^{p-2} \quad , \quad t''_1 \equiv y^{p-2} \quad , \quad u''_1 \equiv z^{p-2}\\
s''_2 &\equiv -x^{p-2} \quad , \quad t''_2 \equiv -y^{p-2} \quad , \quad u''_2 \equiv z^{p-2}\\
s''_3 &\equiv -x^{p-2} \quad , \quad t''_3 \equiv y^{p-2} \quad , \quad u''_3 \equiv -z^{p-2}
\end{aligned}$$

$$[x^{p-2}-y^{p-2}+z^{p-2} \equiv 0 \mod \theta'_{R1}]$$

【General solution conditions】

$$\begin{aligned}
x^p \quad -x^2y^{p-2} &\equiv -x^2z^{p-2} \mod \theta'_{L2}\\
-y^2x^{p-2} \quad +y^p &\equiv y^2z^{p-2} \mod \theta'_{L2}\\
-z^2x^{p-2} \quad +z^2y^{p-2} &\equiv z^p \mod \theta'_{L2}
\end{aligned} \tag{39}$$

1.6.12 Common to $-y^2 \not\equiv x^2 \not\equiv z^2 \mod \theta'_{R2}$

(39) より

$$\begin{aligned} -x^2y^{p-2}\cdot -x^2z^{p-2} &\equiv y^pz^p \mod \theta'_0 \\ x^4 &\equiv y^2z^2 \mod \theta'_0 \end{aligned} \tag{40}$$

$$\begin{aligned} (36)\text{ より } \left(x^{p-2}\right)^2 &\equiv -y^{p-2}z^{p-2} \mod \theta'_0 \\ \left(x^4\right)^{p-2} &\equiv \left(-y^{p-2}z^{p-2}\right)^2 \mod \theta'_0 \\ (40)\text{ より } \left(y^2z^2\right)^{p-2} &\equiv \left(y^{p-2}z^{p-2}\right)^2 \mod \theta'_0 \\ \left(y^{p-2}z^{p-2}\right)^2 &\equiv \left(y^{p-2}z^{p-2}\right)^2 \mod \theta'_0 \end{aligned}$$

··

$$\begin{aligned} -y^2x^{p-2}\cdot y^2z^{p-2} &\equiv x^pz^p \mod \theta'_0 \\ y^4 &\equiv -x^2z^2 \mod \theta'_0 \end{aligned} \tag{41}$$

$$\begin{aligned} (37)\text{ より } \left(y^{p-2}\right)^2 &\equiv x^{p-2}z^{p-2} \mod \theta'_0 \\ \left(y^4\right)^{p-2} &\equiv \left(x^{p-2}z^{p-2}\right)^2 \mod \theta'_0 \\ (41)\text{ より } \left(-x^2z^2\right)^{p-2} &\equiv \left(x^{p-2}z^{p-2}\right)^2 \mod \theta'_0 \\ -\left(x^{p-2}z^{p-2}\right)^2 &\equiv \left(x^{p-2}z^{p-2}\right)^2 \mod \theta'_0 \end{aligned}$$

これは δ' の定義に反する。

··

$$\begin{aligned} -z^2x^{p-2}\cdot z^2y^{p-2} &\equiv x^py^p \mod \theta'_0 \\ z^4 &\equiv -x^2y^2 \mod \theta'_0 \end{aligned} \tag{42}$$

$$\begin{aligned} (38)\text{ より } \left(z^{p-2}\right)^2 &\equiv -x^{p-2}y^{p-2} \mod \theta'_0 \\ \left(z^4\right)^{p-2} &\equiv \left(-x^{p-2}y^{p-2}\right)^2 \mod \theta'_0 \\ (42)\text{ より } \left(-x^2y^2\right)^{p-2} &\equiv \left(x^{p-2}y^{p-2}\right)^2 \mod \theta'_0 \\ -\left(x^{p-2}y^{p-2}\right)^2 &\equiv \left(x^{p-2}y^{p-2}\right)^2 \mod \theta'_0 \end{aligned}$$

これは δ' の定義に反する。

$$
\begin{aligned}
(x+z+y)^2 &\equiv 0 \mod \delta' \\
x^2+y^2+z^2+2(xy+xz+yz) &\equiv 0 \mod \delta' \\
x^2+y^2+z^2+2(x(y+z)+yz) &\equiv 0 \mod \delta' \\
x^2+y^2+z^2+2(-x^2+yz) &\equiv 0 \mod \delta' \\
-x^2+y^2+z^2+2yz &\equiv 0 \mod \delta' \\
-2yz &\equiv 0 \mod \theta'_0
\end{aligned}
$$

また $-z^{p-1} \equiv x^{p-1} \mod \delta'$, $-y^{p-1} \equiv z^{p-1} \mod \delta'$, $y^{p-1} \equiv x^{p-1} \mod \delta'$ のとき $\delta' \perp xyz$, $-z \not\equiv x \mod \delta'$ より

$$
\begin{aligned}
z^{p-2} &\not\equiv x^{p-2} \mod \delta' \\
-y^{p-2} &\not\equiv z^{p-2} \mod \delta' \\
-y^{p-2} &\not\equiv x^{p-2} \mod \delta'
\end{aligned}
$$

よって $\delta' \neq \theta'_0$, $\delta' \neq \theta'_{L1}$ なので $\delta' = \theta'_{R1}$ に属する。

1.6.13 $-y^2 \equiv x^2 \equiv z^2 \mod \delta'$ or $-y^2 \not\equiv x^2 \not\equiv z^2 \mod \delta'$ のとき

(40)(41)(42) より

$$-x^6 \equiv y^6 \equiv z^6 \mod \delta'$$

$$
\begin{aligned}
z^6 - y^6 &\equiv (z^2-y^2)(z^4+y^2z^2+y^4) \equiv 0 \mod \delta' \\
x^6 + z^6 &\equiv (x^2+z^2)(x^4-x^2z^2+z^4) \equiv 0 \mod \delta' \\
x^6 + y^6 &\equiv (x^2+y^2)(x^4-x^2y^2+y^4) \equiv 0 \mod \delta'
\end{aligned}
$$

$$x^4 - x^2y^2 + y^4 \equiv 0 \mod \theta'_{R2} \ \wedge \ x^p + y^p \equiv z^p \mod \theta'_{R2}$$

が成り立つならば、$\theta'_{R1} = \theta'_{R2}$
(40)(41)(42) より

$$x^2 - y^2 - z^2 \equiv 0 \mod \theta'_{R2}$$

これは $\theta'_0 \neq \theta'_{R1}$ と矛盾するので

$$x^p + y^p \not\equiv z^p \mod \theta'_{R2}$$

よって $\delta' \neq \theta'_{R2}$ なので $\delta' = \theta'_{L2}$ に属する。

$$
\begin{aligned}
z^2 - y^2 &\equiv 0 \mod \delta' \\
x^2 + z^2 &\equiv 0 \mod \delta' \\
x^2 + y^2 &\equiv 0 \mod \delta'
\end{aligned}
$$

これは $z^2 - y^2 \not\equiv 0 \mod \delta'$ に反するので $\delta' \neq \theta'_{L2}$
以上より

$$\delta' \neq odd$$

1.6.14 $2 \mid z$, $2 \perp xy$

$S" = 2^k$ のとき

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

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

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

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

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

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

よって $2 \mid z$ のとき成り立たない。

$y + z - x$ などの条件は省略しているが $2 \mid y$ も同様に成り立たない。以上より

$$x^p + y^p \neq z^p$$

1.7 補足 1(supplement 1)

$$-y \equiv z \equiv x \mod \theta_{l2}$$

$$[x^{p-1} - y^{p-1} - z^{p-1} \equiv 0 \mod \theta_{r1}]$$

【General solution conditions】

$$\begin{aligned} x^p \quad -y^{p-1}x &\equiv z^{p-1}x \mod \theta_{l2} \\ -x^{p-1}y \quad +y^p &\equiv -z^{p-1}y \mod \theta_{l2} \\ x^{p-1}z \quad -y^{p-1}z &\equiv z^p \mod \theta_{l2} \end{aligned}$$

Common to $-y \not\equiv z \not\equiv x \mod \theta_{r2}$

$$\begin{aligned} -y^{p-1}x \cdot z^{p-1}x &\equiv y^p z^p \mod \theta_{r1} \\ x^2 &\equiv -yz \mod \theta_{r1} \end{aligned} \tag{43}$$

$$\begin{aligned} -x^{p-1}y \cdot -z^{p-1}y &\equiv x^p z^p \mod \theta_{r1} \\ y^2 &\equiv xz \mod \theta_{r1} \end{aligned} \tag{44}$$

$$\begin{aligned} x^{p-1}z \cdot -y^{p-1}z &\equiv x^p y^p \mod \theta_{r1} \\ z^2 &\equiv -xy \mod \theta_{r1} \end{aligned} \tag{45}$$

(43)(44)(45) より

$$-y^3 \equiv z^3 \equiv x^3 \mod \theta_{r1}$$

$$\begin{aligned} z^3 + y^3 &\equiv (z+y)(z^2 - yz + y^2) \equiv 0 \mod \theta_{r1} \\ x^3 - z^3 &\equiv (x-z)(x^2 + xz + z^2) \equiv 0 \mod \theta_{r1} \\ x^3 + y^3 &\equiv (x+y)(x^2 - xy + y^2) \equiv 0 \mod \theta_{r1} \end{aligned}$$

(45) より

$$\begin{aligned} x^2 + xz + z^2 &\equiv 0 \mod \theta_{r1} \\ x^2 + xz - xy &\equiv 0 \mod \theta_{r1} \\ x + z - y &\equiv 0 \mod \theta_{r1} \end{aligned}$$

これは $\delta \neq \theta_{r1}$ に反するので $-y \not\equiv z \not\equiv x \mod \theta_{r2}$ のとき
【Actual conditions】

$$\begin{aligned} x^p \quad +y^p &\not\equiv z^p \mod \theta_{r2} \\ -y^{p-1}z \quad -z^{p-1}x &\not\equiv x^{p-1}y \mod \theta_{r2} \\ z^{p-1}y \quad +x^{p-1}z &\not\equiv y^{p-1}x \mod \theta_{r2} \end{aligned}$$

1.8 補足 2(supplement 2)

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。
【Actual conditions】

$$s'_1 x^{p-2} + t'_1 y^{p-2} \equiv u'_1 z^{p-2} \mod \Theta$$

$$s'_2 z^{p-2} + t'_2 x^{p-2} \equiv u'_2 y^{p-2} \mod \Theta$$

$$s'_3 y^{p-2} + t'_3 z^{p-2} \equiv u'_3 x^{p-2} \mod \Theta$$

1.8.1 $-z^{p-2} \equiv x^{p-2} \equiv y^{p-2} \mod \Theta_{L1}$ のとき

$$\begin{aligned} s'_1 x^{p-2} + t'_1 y^{p-2} &\equiv u'_1 z^{p-2} \mod \Theta_{L1} \\ -s'_2 x^{p-2} + t'_2 y^{p-2} &\equiv -u'_2 z^{p-2} \mod \Theta_{L1} \\ s'_3 x^{p-2} - t'_3 y^{p-2} &\equiv -u'_3 z^{p-2} \mod \Theta_{L1} \end{aligned}$$

$\mod \Theta_{L1}$ として

$$\begin{array}{lll} s'_1 \equiv x^2 & , \ t'_1 \equiv y^2 & , \ u'_1 \equiv z^2 \\ s'_2 \equiv -x^2 & , \ t'_2 \equiv y^2 & , \ u'_2 \equiv -z^2 \\ s'_3 \equiv x^2 & , \ t'_3 \equiv -y^2 & , \ u'_3 \equiv -z^2 \end{array}$$

$$[x^2 + y^2 + z^2 \equiv 0 \mod \Theta_0]$$

【General solution conditions】

$$\begin{array}{rcl} x^p \quad +y^2 x^{p-2} & \equiv -z^2 x^{p-2} & \mod \Theta_{L1} \\ x^2 y^{p-2} \quad +y^p & \equiv -z^2 y^{p-2} & \mod \Theta_{L1} \\ -x^2 z^{p-2} \quad -y^2 z^{p-2} & \equiv z^p & \mod \Theta_{L1} \end{array} \tag{46}$$

1.8.2 Common to $-z^{p-2} \not\equiv x^{p-2} \not\equiv y^{p-2} \mod \Theta_{R1}$

(46) より

$$\begin{aligned} x^p \quad +y^2x^{p-2} &\equiv -z^2x^{p-2} \mod \Theta_{L1} \\ x^p \quad +z^2x^{p-2} &\equiv -y^2x^{p-2} \mod \Theta_{R1} \end{aligned}$$

$$\begin{aligned} y^2x^{p-2}\cdot -z^2x^{p-2} &\equiv y^pz^p \mod \Theta_0 \\ \left(x^{p-2}\right)^2 &\equiv -y^{p-2}z^{p-2} \mod \Theta_0 \end{aligned} \tag{47}$$

$$\begin{aligned} x^2y^{p-2} \quad +y^p &\equiv -z^2y^{p-2} \mod \Theta_{L1} \\ z^2y^{p-2} \quad +y^p &\equiv -x^2y^{p-2} \mod \Theta_{R1} \end{aligned}$$

$$\begin{aligned} x^2y^{p-2}\cdot -z^2y^{p-2} &\equiv x^pz^p \mod \Theta_0 \\ \left(y^{p-2}\right)^2 &\equiv -x^{p-2}z^{p-2} \mod \Theta_0 \end{aligned} \tag{48}$$

$$\begin{aligned} -x^2z^{p-2} \quad -y^2z^{p-2} &\equiv z^p \mod \Theta_{L1} \\ -y^2z^{p-2} \quad -x^2z^{p-2} &\equiv z^p \mod \Theta_{R1} \end{aligned}$$

$$\begin{aligned} -x^2z^{p-2}\cdot -y^2z^{p-2} &\equiv x^py^p \mod \Theta_0 \\ \left(z^{p-2}\right)^2 &\equiv x^{p-2}y^{p-2} \mod \Theta_0 \end{aligned} \tag{49}$$

(47)(48)(49) より

$$\left(x^{p-2}\right)^3 \equiv \left(y^{p-2}\right)^3 \equiv -\left(z^{p-2}\right)^3 \mod \Theta_0$$

$$\begin{aligned}
\left(z^{p-2}\right)^3+\left(y^{p-2}\right)^3 &\equiv (z^{p-2}+y^{p-2})((z^{p-2})^2-y^{p-2}z^{p-2}+(y^{p-2})^2)\equiv 0 \mod \Theta_0\\
\left(x^{p-2}\right)^3+\left(z^{p-2}\right)^3 &\equiv (x^{p-2}+z^{p-2})((x^{p-2})^2-x^{p-2}z^{p-2}+(z^{p-2})^2)\equiv 0 \mod \Theta_0\\
\left(x^{p-2}\right)^3-\left(y^{p-2}\right)^3 &\equiv (x^{p-2}-y^{p-2})((x^{p-2})^2+x^{p-2}y^{p-2}+(y^{p-2})^2)\equiv 0 \mod \Theta_0
\end{aligned}$$

1.8.3 $-z^{p-2} \not\equiv x^{p-2} \not\equiv y^{p-2} \mod \Theta_{R1}$

$$\begin{aligned}
(x^{p-2})^2+(z^{p-2})^2+(y^{p-2})^2 &\equiv 0 \mod \Theta_{R1}\\
(x^{p-2})^2+x^{p-2}y^{p-2}-x^{p-2}z^{p-2} &\equiv 0 \mod \Theta_{R1}\\
x^{p-2}+y^{p-2}-z^{p-2} &\equiv 0 \mod \Theta_{R1}\\
x^{p-2}+y^{p-2} &\equiv z^{p-2} \mod \Theta_{R1}
\end{aligned}$$

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。

$$\begin{aligned}
s''_1x^2+t''_1y^2 &\equiv u''_1z^2 \mod \Theta\\
s''_2z^2+t''_2x^2 &\equiv u''_2y^2 \mod \Theta\\
s''_3y^2+t''_3z^2 &\equiv u''_3x^2 \mod \Theta
\end{aligned}$$

1.8.4 $x^2 \equiv y^2 \equiv z^2 \mod \Theta_{L2}$ のとき

$$\begin{aligned}
s''_1x^2+t''_1y^2 &\equiv u''_1z^2 \mod \Theta_{L2}\\
s''_2x^2+t''_2y^2 &\equiv u''_2z^2 \mod \Theta_{L2}\\
s''_3x^2+t''_3y^2 &\equiv u''_3z^2 \mod \Theta_{L2}
\end{aligned}$$

$\mod \Theta_{L2}$ として

$$\begin{aligned}
s''_1 &\equiv x^{p-2} \quad , \quad t''_1 \equiv y^{p-2} \quad , \quad u''_1 \equiv z^{p-2}\\
s''_2 &\equiv x^{p-2} \quad , \quad t''_2 \equiv y^{p-2} \quad , \quad u''_2 \equiv z^{p-2}\\
s''_3 &\equiv x^{p-2} \quad , \quad t''_3 \equiv y^{p-2} \quad , \quad u''_3 \equiv z^{p-2}
\end{aligned}$$

$$[x^{p-2}+y^{p-2}-z^{p-2} \equiv 0 \mod \Theta_{R1}]$$

【General solution conditions】

$$\begin{aligned}
x^p \quad +x^2y^{p-2} &\equiv x^2z^{p-2} \mod \Theta_{L2}\\
y^2x^{p-2} \quad +y^p &\equiv y^2z^{p-2} \mod \Theta_{L2}\\
z^2x^{p-2} \quad +z^2y^{p-2} &\equiv z^p \mod \Theta_{L2}
\end{aligned} \tag{50}$$

1.8.5 Common to $x^2 \not\equiv y^2 \not\equiv z^2 \mod \Theta_{R2}$

(50) より

$$\begin{aligned} x^2y^{p-2} \cdot x^2z^{p-2} &\equiv y^pz^p \mod \Theta_0 \\ x^4 &\equiv y^2z^2 \mod \Theta_0 \end{aligned} \tag{51}$$

$$\begin{aligned} \text{(47) より } \left(x^{p-2}\right)^2 &\equiv -y^{p-2}z^{p-2} \mod \Theta_0 \\ \left(x^4\right)^{p-2} &\equiv \left(-y^{p-2}z^{p-2}\right)^2 \mod \Theta_0 \\ \text{(51) より } \left(y^2z^2\right)^{p-2} &\equiv \left(y^{p-2}z^{p-2}\right)^2 \mod \Theta_0 \\ \left(y^{p-2}z^{p-2}\right)^2 &\equiv \left(y^{p-2}z^{p-2}\right)^2 \mod \Theta_0 \end{aligned}$$

....

$$\begin{aligned} y^2x^{p-2} \cdot y^2z^{p-2} &\equiv x^pz^p \mod \Theta_0 \\ y^4 &\equiv x^2z^2 \mod \Theta_0 \end{aligned} \tag{52}$$

$$\begin{aligned} \text{(48) より } \left(y^{p-2}\right)^2 &\equiv -x^{p-2}z^{p-2} \mod \Theta_0 \\ \left(y^4\right)^{p-2} &\equiv \left(-x^{p-2}z^{p-2}\right)^2 \mod \Theta_0 \\ \text{(52) より } \left(x^2z^2\right)^{p-2} &\equiv \left(x^{p-2}z^{p-2}\right)^2 \mod \Theta_0 \\ \left(x^{p-2}z^{p-2}\right)^2 &\equiv \left(x^{p-2}z^{p-2}\right)^2 \mod \Theta_0 \end{aligned}$$

....

$$\begin{aligned} z^2x^{p-2} \cdot z^2y^{p-2} &\equiv x^py^p \mod \Theta_0 \\ z^4 &\equiv x^2y^2 \mod \Theta_0 \end{aligned} \tag{53}$$

$$\begin{aligned} \text{(49) より } \left(z^{p-2}\right)^2 &\equiv x^{p-2}y^{p-2} \mod \Theta_0 \\ \left(z^4\right)^{p-2} &\equiv \left(x^{p-2}y^{p-2}\right)^2 \mod \Theta_0 \\ \text{(53) より } \left(x^2y^2\right)^{p-2} &\equiv \left(x^{p-2}y^{p-2}\right)^2 \mod \Theta_0 \\ \left(x^{p-2}y^{p-2}\right)^2 &\equiv \left(x^{p-2}y^{p-2}\right)^2 \mod \Theta_0 \end{aligned}$$

よって $\Theta_0 = \Theta_{R1}$ なので $\Theta_0 \neq \Theta_{L1}$

1.8.6 $x^2 \equiv y^2 \equiv z^2 \mod \Theta_0$ or $x^2 \not\equiv y^2 \not\equiv z^2 \mod \Theta_0$ のとき

(51)(52)(53) より

$$x^6 \equiv y^6 \equiv z^6 \mod \Theta_0$$

$$\begin{aligned} z^6 - y^6 &\equiv (z^2 - y^2)(z^4 + y^2 z^2 + y^4) \equiv 0 \mod \Theta_0 \\ x^6 - z^6 &\equiv (x^2 - z^2)(x^4 + x^2 z^2 + z^4) \equiv 0 \mod \Theta_0 \\ x^6 - y^6 &\equiv (x^2 - y^2)(x^4 + x^2 y^2 + y^4) \equiv 0 \mod \Theta_0 \end{aligned}$$

(51)(52)(53) より

$$x^4 + x^2 y^2 + y^4 \equiv x^2 + y^2 + z^2 \mod \Theta_0$$

$$\begin{aligned} x^2 - z^2 &\not\equiv 0 \mod \delta \\ x^2 - y^2 &\not\equiv 0 \mod \delta \end{aligned}$$

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

(17) より $xy + z^2 \not\equiv 0 \mod \delta$ であるから $\Theta_0 \neq \delta$

$$\begin{aligned} -z^{p-2} &\not\equiv y^{p-2} \mod \Theta_0 \\ -x^{p-2} &\not\equiv z^{p-2} \mod \Theta_0 \\ x^{p-2} &\not\equiv y^{p-2} \mod \Theta_0 \end{aligned}$$

よって、δ は上記三組の合同式に対する共通の法に該当しない。

$z^{p-1} \equiv y^{p-1} \mod \delta$, $-x^{p-1} \equiv z^{p-1} \mod \delta$, $-x^{p-1} \equiv y^{p-1} \mod \delta$
$x \not\equiv z \mod \delta$, $-x \not\equiv y \mod \delta$ なので

$$-z \equiv y \mod \delta$$

$$\begin{aligned} -z^{p-2} &\equiv y^{p-2} \mod \delta \\ -x^{p-2} &\not\equiv z^{p-2} \mod \delta \\ x^{p-2} &\not\equiv y^{p-2} \mod \delta \end{aligned}$$