General solution conditions

Hajime Mashima

Abstract

Modulo not divisible by xyz and possible expansions.

Contents

1 introduction

フェルマーの最終定理を代数の範囲で評価を行います。

1.1 $\delta \perp xyz$ の導出

Theorem 1 (Fermat's Last Theorem)

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

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

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

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

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

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

一般的に

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

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

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

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

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

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

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

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

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

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

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

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

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

よって、少なくとも

$$p^2 \mid x$$

$x = p^2 a\alpha$ と仮定すると

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

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

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

一般的に

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

□

また

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

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

1.1.1 $p \mid x$ のとき

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

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

Proof 6

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

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

$$\delta \perp x$$

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

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

$$\delta \perp bc$$

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

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

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

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

よって $\delta \perp \beta$

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

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

よって $\delta \perp \gamma$ □

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

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

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

Proof 8

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

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

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

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

$$\delta \perp x$$

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

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

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

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

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

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

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

よって $\delta \perp \beta'$

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

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

よって $\delta \perp \gamma'$ □

1.2 解の条件 (Solution conditions)

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

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

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

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

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

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

同様に

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

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

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

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

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

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

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

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

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

同様に

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

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

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

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

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

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

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

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

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

同様に

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

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

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

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

【Solution conditions】

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

(4),(6),(8) から

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

$U = y$, $T = z$ を例とする全条件 (*This condition is not applicable here.)

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

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

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

$x - y \equiv -z \mod \delta$ より

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

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

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

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

Definition 9 以降、例として $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta$ と表記する場合、$-x^{p-1} \not\equiv z^{p-1} \mod \theta$ とも意味する。

1.3 同値変換 (Equivalence transformation)

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

Definition 10 【Equivalence transformation】

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

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

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

このとき以下を同値変換の成立条件と呼び、以降 [ ] で示す。

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

1.4 一般的解の条件 (General solution conditions)

Definition 11 同値変換の成立条件が 3 組共通な以下の関係式を
General solution conditions と呼ぶ。

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

1.4.1 $-x^{p-1}\equiv y^{p-1}\equiv z^{p-1} \mod \theta_1$ のとき

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

$\mod \theta_1$ として

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

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

【General solution conditions】

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

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

(5)、(10)、(11) より

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

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

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

(7)、(10)、(11) より

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

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

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

(9)、(10)、(11) より

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

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

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

(12)(13)(14) より

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

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

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

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

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

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

$\delta \perp 3AB$ なので

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

2 つの因数のうち、一方は δ と互いに素である。 (15)

1.4.3 $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta_2$ のとき

(13)(14) より

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

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

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

1.4.4 $-y \equiv z \equiv x \mod \theta_3$ のとき

$$\begin{aligned}s''_1 x + t''_1 y &\equiv u''_1 z \mod \theta_3 \\ s''_2 x - t''_2 y &\equiv -u''_2 z \mod \theta_3 \\ -s''_3 x - t''_3 y &\equiv u''_3 z \mod \theta_3\end{aligned}$$

$\mod \theta_3$ として

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

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

【General solution conditions】

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

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

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

(16)(17) より

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

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

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

(18)(19)(20) より

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

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

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

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

$\theta_4 = \delta$ が確定するので $\theta_2 = \theta_4$ であり $\theta_3 \neq \delta$

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

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

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

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

δ の定義に反する。

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

δ の定義に反するので $\theta_4 \neq \delta$

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

よって $\theta_1 = \delta$

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

1.5 $-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \delta$

【General solution conditions】

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

1.5.1 $x \equiv -y \equiv -2^{-1}z \mod \theta$ のとき

$\theta \neq 2$ のとき $2^{-1} \equiv 2^{\theta-2} \mod \theta$ と同値であるので便宜的に

$$\begin{aligned} s_1x &-t_2y &&\equiv -2^{-1}zu_3 \mod \theta \\ -s_3x &+t_1y &&\equiv 2^{-1}zu_2 \mod \theta \\ -2s_2x &+2t_3y &&\equiv u_1z \mod \theta \end{aligned}$$

$\mod \theta$ として

$$\begin{aligned} s_1 &\equiv x^{p-1} \ , \ t_1 \equiv y^{p-1} \ , \ u_1 \equiv z^{p-1} \\ s_2 &\equiv -2^{-1}x^{p-1} \ , \ t_2 \equiv -y^{p-1} \ , \ u_2 \equiv 2z^{p-1} \\ s_3 &\equiv -x^{p-1} \ , \ t_3 \equiv 2^{-1}y^{p-1} \ , \ u_3 \equiv -2z^{p-1} \end{aligned}$$

$$[x^{p-1} - y^{p-1} + 2z^{p-1} \equiv 0 \mod \delta]$$

【General solution conditions】

$$\begin{aligned} x^p &-y^{p-1}x &&\equiv -2z^{p-1}x \mod \delta \\ -x^{p-1}y &+y^p &&\equiv 2z^{p-1}y \mod \delta \\ -2^{-1}x^{p-1}z &+2^{-1}y^{p-1}z &&\equiv z^p \mod \delta \end{aligned}$$

1.5.2 Common to $x \not\equiv -y \not\equiv -2^{-1}z \mod \theta$

$$\begin{aligned} -y^{p-1}x \cdot -2z^{p-1}x &\equiv y^pz^p \mod \delta \\ 2x^2 &\equiv yz \mod \delta \\ x^2 &\equiv 2^{-1}yz \mod \delta \end{aligned} \tag{21}$$

$$\begin{aligned} -x^{p-1}y \cdot 2z^{p-1}y &\equiv x^pz^p \mod \delta \\ -2y^2 &\equiv xz \mod \delta \\ y^2 &\equiv -2^{-1}xz \mod \delta \end{aligned} \tag{22}$$

$$\begin{aligned} -2^{-1}x^{p-1}z \cdot 2^{-1}y^{p-1}z &\equiv x^py^p \mod \delta \\ -2^{-2}z^2 &\equiv xy \mod \delta \\ z^2 &\equiv -2^2xy \mod \delta \end{aligned} \tag{23}$$

(21)(22)(23) より

$$-x^3 \equiv y^3 \equiv \left(2^{-1}z\right)^3 \mod \delta$$

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

$\delta \perp 3xyz2$ なので (15) より二つの因数の一方が解となる。

$x + z - y \equiv 0 \mod \delta$, $x \not\equiv -y \mod \delta$ であるから

$$x \not\equiv -y \not\equiv -2^{-1}z \mod \delta$$

よって右の因数が解となるので

$$\begin{aligned} x^2 - xy + y^2 &\equiv 0 \mod \delta \\ \text{(22) より } x^2 - xy - 2^{-1}xz &\equiv 0 \mod \delta \\ x - y &\equiv 2^{-1}z \mod \delta \end{aligned}$$

$$\begin{aligned} -z &\equiv 2^{-1}z \mod \delta \\ 0 &\not\equiv 3z \mod \delta \end{aligned}$$

であるが演算を続ける。
【General solution conditions】

$$\begin{aligned} x^p \quad -yx^{p-1} &\equiv 2^{-1}zx^{p-1} \mod \delta \\ -xy^{p-1} \quad +y^p &\equiv -2^{-1}zy^{p-1} \mod \delta \\ 2z^{p-1}x \quad -2z^{p-1}y &\equiv z^p \mod \delta \end{aligned}$$

1.5.3 Common to $x^{p-1} \not\equiv -y^{p-1} \not\equiv 2z^{p-1} \mod \theta$

$$\begin{aligned} -yx^{p-1} \cdot 2^{-1}zx^{p-1} &\equiv y^p z^p \mod \delta \\ -\left(x^{p-1}\right)^2 &\equiv 2y^{p-1}z^{p-1} \mod \delta \end{aligned} \tag{24}$$

$$\begin{aligned} -xy^{p-1} \cdot -2^{-1}zy^{p-1} &\equiv x^p z^p \mod \delta \\ \left(y^{p-1}\right)^2 &\equiv 2x^{p-1}z^{p-1} \mod \delta \end{aligned} \tag{25}$$

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

(24)(25)(26) より

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

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

$$
\begin{aligned}
\left(x^{p-1}\right)^3+\left(y^{p-1}\right)^3 &\equiv (x^{p-1}+y^{p-1})\left(\left(x^{p-1}\right)^2-x^{p-1}y^{p-1}+\left(y^{p-1}\right)^2\right)\equiv 0 \mod \delta\\
\text{(25) より}\qquad &\equiv (x^{p-1}+y^{p-1})\left(\left(x^{p-1}\right)^2-x^{p-1}y^{p-1}+2x^{p-1}z^{p-1}\right)\equiv 0 \mod \delta\\
&\equiv (x^{p-1}+y^{p-1})(x^{p-1}-y^{p-1}+2z^{p-1})x^{p-1}\equiv 0 \mod \delta
\end{aligned}
$$

$$x^{p-1}+y^{p-1}\equiv 0 \mod \delta \quad \wedge \quad x^{p-1}-y^{p-1}+2z^{p-1}\equiv 0 \mod \delta$$

(15) より $3xy \perp \delta$ なので矛盾する。また

$$
\begin{aligned}
\text{(12) より}\ \left(x^{p-1}\right)^2 &\equiv y^{p-1}z^{p-1} \mod \delta\\
\left(x^2\right)^{p-1} &\equiv y^{p-1}z^{p-1} \mod \delta\\
\text{(21) より}\ \left(2^{-1}yz\right)^{p-1} &\equiv y^{p-1}z^{p-1} \mod \delta\\
2^{-(p-1)}y^{p-1}z^{p-1} &\equiv y^{p-1}z^{p-1} \mod \delta\\
1 &\equiv 2^{p-1} \mod \delta
\end{aligned}
$$

$$
\begin{aligned}
\text{(13) より}\ \left(y^{p-1}\right)^2 &\equiv -x^{p-1}z^{p-1} \mod \delta\\
\left(y^2\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \delta\\
\text{(22) より}\ \left(-2^{-1}xz\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \delta\\
2^{-(p-1)}x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \delta\\
-1 &\equiv 2^{p-1} \mod \delta
\end{aligned}
$$

$$
\begin{aligned}
\text{(14) より}\ \left(z^{p-1}\right)^2 &\equiv -x^{p-1}y^{p-1} \mod \delta\\
\left(z^2\right)^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \delta\\
\text{(23) より}\ \left(-2^2xy\right)^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \delta\\
2^{2(p-1)}x^{p-1}y^{p-1} &\equiv -x^{p-1}y^{p-1} \mod \delta\\
\left(2^{p-1}\right)^2 &\equiv -1 \mod \delta
\end{aligned}
$$

上式を満たす δ は存在しない。
よって

$$\delta \neq odd$$

1.6 $\delta = 2$ のとき

1.6.1 $2 \mid x$, $2 \perp yz$

$S = 2^k$ のとき

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

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

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

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

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

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

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

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

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

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

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

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。

1.6.2 まとめ

【General solution conditions】

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

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

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

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

【Equivalence transformation】

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

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

or

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

$$
\begin{aligned}
xx^{p-1} \quad &+yy^{p-1} \quad &&\equiv zz^{p-1} \mod \theta_2 \\
yz^{p-1} \quad &+zx^{p-1} \quad &&\equiv xy^{p-1} \mod \theta_2 \\
-zy^{p-1} \quad &-xz^{p-1} \quad &&\equiv yx^{p-1} \mod \theta_2
\end{aligned}
$$

1.7 $\delta' \perp xyz$ の導出

1.7.1 $p \mid z$ のとき (諸条件は省略)

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

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

Proof 13

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

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

$$\delta' \perp z$$

$$2z = -(x + y - z) + (z + x + y)$$
$$ab \mid x + y - z$$
$$z \perp ab$$

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

$$z \equiv -x \mod \delta'$$
$$z^p \equiv -x^p \mod \delta'$$
$$z^p + x^p \equiv 0 \mod \delta'$$

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

$$z^p + x^p + (z^p - x^p) \equiv 0 \mod \delta'$$
$$2z^p \not\equiv 0 \mod \delta'$$

よって $\delta' \perp \beta$

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

$$z^p + y^p + (z^p - y^p) \equiv 0 \mod \delta'$$
$$2z^p \not\equiv 0 \mod \delta'$$

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

$$\begin{aligned} -z^{p-1} \equiv & x^{p-1} \equiv y^{p-1} \mod \delta' \\ & or \\ -z^{p-1} \not\equiv & x^{p-1} \not\equiv y^{p-1} \mod \delta' \end{aligned} \tag{27}$$

1.8 一般的解の条件 (General solution conditions)

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

1.8.1 $-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \mod \theta_1'$ のとき

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

$\mod \theta_1'$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p + yx^{p-1} &\equiv -zx^{p-1} \mod \delta' \\ xy^{p-1} + y^p &\equiv -zy^{p-1} \mod \delta' \\ -xz^{p-1} - yz^{p-1} &\equiv z^p \mod \delta' \end{aligned} \tag{28}$$

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

(27)(28) より

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

$$\begin{aligned} xy^{p-1} \cdot -zy^{p-1} &\equiv x^p z^p \mod \delta' \\ \left(y^{p-1}\right)^2 &\equiv -x^{p-1} z^{p-1} \mod \delta' \end{aligned} \tag{30}$$

$$\begin{aligned} -xz^{p-1} \cdot -yz^{p-1} &\equiv x^p y^p \mod \delta' \\ \left(z^{p-1}\right)^2 &\equiv x^{p-1} y^{p-1} \mod \delta' \end{aligned} \tag{31}$$

(29)(30)(31) より

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

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

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

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

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

$\delta' \perp 3AB$ なので

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

2 つの因数のうち、一方は δ' と互いに素である。 (32)

1.8.3 $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \mod \theta'_2$ のとき

(30)(31) より

$$\begin{aligned}(x^{p-1})^2 + (z^{p-1})^2 + (y^{p-1})^2 &\equiv 0 \mod \theta'_2 \\ (x^{p-1})^2 + x^{p-1}y^{p-1} - x^{p-1}z^{p-1} &\equiv 0 \mod \theta'_2 \\ x^{p-1} + y^{p-1} - z^{p-1} &\equiv 0 \mod \theta'_2\end{aligned}$$

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

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

1.8.4 $z \equiv x \equiv y \mod \theta'_3$ のとき

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

$\mod \theta'_3$ として

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

$$[x^{p-1} + y^{p-1} - z^{p-1} \equiv 0 \mod \theta'_2]$$

【General solution conditions】

$$\begin{aligned}x^p &+ xy^{p-1} &&\equiv xz^{p-1} \mod \theta'_2 \\ yx^{p-1} &+ y^p &&\equiv yz^{p-1} \mod \theta'_2 \\ zx^{p-1} &+ zy^{p-1} &&\equiv z^p \mod \theta'_2\end{aligned} \tag{33}$$

$$\begin{aligned}z \equiv & x \equiv y \mod \theta'_2 \\ & or \\ z \not\equiv & x \not\equiv y \mod \theta'_2\end{aligned} \tag{34}$$

1.8.5 Common to $z \not\equiv x \not\equiv y \mod \theta_4'$

(33)(34) より

$$\begin{aligned} xy^{p-1} \cdot xz^{p-1} &\equiv y^p z^p \mod \theta_2' \\ x^2 &\equiv yz \mod \theta_2' \end{aligned} \tag{35}$$

$$\begin{aligned} \text{(29) より } \left(x^{p-1}\right)^2 &\equiv -y^{p-1}z^{p-1} \mod \theta_4' \\ \left(x^2\right)^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta_4' \\ \text{(35) より } (yz)^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta_4' \\ y^{p-1}z^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \theta_4' \end{aligned}$$

δ' の定義に反する。

.....

$$\begin{aligned} yx^{p-1} \cdot yz^{p-1} &\equiv x^p z^p \mod \theta_2' \\ y^2 &\equiv xz \mod \theta_2' \end{aligned} \tag{36}$$

$$\begin{aligned} \text{(30) より } \left(y^{p-1}\right)^2 &\equiv -x^{p-1}z^{p-1} \mod \theta_4' \\ \left(y^2\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_4' \\ \text{(36) より } (xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_4' \\ x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \theta_4' \end{aligned}$$

δ' の定義に反する。

.....

$$\begin{aligned} zx^{p-1} \cdot zy^{p-1} &\equiv x^p y^p \mod \theta_2' \\ z^2 &\equiv xy \mod \theta_2' \end{aligned} \tag{37}$$

$$\begin{aligned} \text{(31) より } \left(z^{p-1}\right)^2 &\equiv x^{p-1}y^{p-1} \mod \theta_4' \\ \left(z^2\right)^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta_4' \\ \text{(37) より } (xy)^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta_4' \\ x^{p-1}y^{p-1} &\equiv x^{p-1}y^{p-1} \mod \theta_4' \end{aligned}$$

少なくとも δ' の定義に反するので $\theta_4' \neq \delta'$

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

よって $\theta_1' = \delta'$

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

1.9 $-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \mod \delta'$

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

1.9.1 $x \equiv z \equiv -2^{-1}y \mod \theta'$ のとき

$\theta' \neq 2$ のとき $2^{-1} \equiv 2^{\theta'-2} \mod \theta'$ と同値であるので便宜的に

$$\begin{aligned} s_1 x \quad -2^{-1} y t_2 \quad &\equiv u_3 z \mod \theta' \\ -2 s_3 x \quad +t_1 y \quad &\equiv -2 u_2 z \mod \theta' \\ s_2 x \quad -2^{-1} y t_3 \quad &\equiv u_1 z \mod \theta' \end{aligned}$$

$\mod \theta'$ として

$$\begin{aligned} s_1 \quad &\equiv x^{p-1} \quad , \ t_1 \equiv y^{p-1} \quad , \ u_1 \equiv z^{p-1} \\ s_2 \quad &\equiv x^{p-1} \quad , \ t_2 \equiv -2y^{p-1} \quad , \ u_2 \equiv -2^{-1} z^{p-1} \\ s_3 \quad &\equiv -2^{-1} x^{p-1} \quad , \ t_3 \equiv -2y^{p-1} \quad , \ u_3 \equiv z^{p-1} \end{aligned}$$

$$[x^{p-1} - 2y^{p-1} - z^{p-1} \equiv 0 \mod \delta']$$

【General solution conditions】

$$\begin{aligned} x^p \quad -2y^{p-1} x \quad &\equiv z^{p-1} x \mod \delta' \\ -2^{-1} x^{p-1} y \quad +y^p \quad &\equiv -2^{-1} z^{p-1} y \mod \delta' \\ x^{p-1} z \quad -2y^{p-1} z \quad &\equiv z^p \mod \delta' \end{aligned}$$

1.9.2 Common to $x \not\equiv z \not\equiv -2^{-1}y \mod \theta'$

$$\begin{aligned} -2y^{p-1} x \cdot z^{p-1} x \quad &\equiv y^p z^p \mod \delta' \\ -2x^2 \quad &\equiv yz \mod \delta' \\ x^2 \quad &\equiv -2^{-1} yz \mod \delta' \end{aligned} \tag{38}$$

$$\begin{aligned} -2^{-1} x^{p-1} y \cdot -2^{-1} z^{p-1} y \quad &\equiv x^p z^p \mod \delta' \\ 2^{-2} y^2 \quad &\equiv xz \mod \delta' \\ y^2 \quad &\equiv 2^2 xz \mod \delta' \end{aligned} \tag{39}$$

$$\begin{aligned} x^{p-1} z \cdot -2y^{p-1} z \quad &\equiv x^p y^p \mod \delta' \\ -2z^2 \quad &\equiv xy \mod \delta' \\ z^2 \quad &\equiv -2^{-1} xy \mod \delta' \end{aligned} \tag{40}$$

(38)(39)(40) より

$$x^3 \equiv z^3 \equiv -\left(2^{-1}y\right)^3 \mod \delta'$$

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

$\delta' \perp 3xyz2$ なので (32) より二つの因数の一方が解となる。

$x+y+z \equiv 0 \mod \delta'$, $x \not\equiv z \mod \delta'$ であるから

$$x \not\equiv z \not\equiv -2^{-1}y \mod \delta'$$

よって右の因数が解となるので

$$\begin{aligned} x^2+xz+z^2 &\equiv 0 \mod \delta' \\ \text{(40) より } x^2+xz-2^{-1}xy &\equiv 0 \mod \delta' \\ x-2^{-1}y &\equiv -z \mod \delta' \end{aligned}$$

$$\begin{aligned} y &\equiv -2^{-1}y \mod \delta' \\ 0 &\not\equiv 3y \mod \delta' \end{aligned}$$

であるが演算を続ける。
【General solution conditions】

$$\begin{aligned} x^p \quad -2^{-1}yx^{p-1} &\equiv -zx^{p-1} \mod \delta' \\ -2xy^{p-1} \quad +y^p &\equiv 2zy^{p-1} \mod \delta' \\ -xz^{p-1} \quad +2^{-1}yz^{p-1} &\equiv z^p \mod \delta' \end{aligned}$$

1.9.3 Common to $-x^{p-1} \not\equiv z^{p-1} \not\equiv 2y^{p-1} \mod \theta'$

$$\begin{aligned} -2^{-1}yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \mod \delta' \\ \left(x^{p-1}\right)^2 &\equiv 2y^{p-1}z^{p-1} \mod \delta' \end{aligned} \tag{41}$$

$$\begin{aligned} -2xy^{p-1} \cdot 2zy^{p-1} &\equiv x^p z^p \mod \delta' \\ -2^2\left(y^{p-1}\right)^2 &\equiv x^{p-1}z^{p-1} \mod \delta' \end{aligned} \tag{42}$$

$$\begin{aligned} -xz^{p-1} \cdot 2^{-1}yz^{p-1} &\equiv x^p y^p \mod \delta' \\ \left(z^{p-1}\right)^2 &\equiv -2x^{p-1}y^{p-1} \mod \delta' \end{aligned} \tag{43}$$

(41)(42)(43) より

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

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

$$
\begin{aligned}
\left(x^{p-1}\right)^3+\left(z^{p-1}\right)^3 &\equiv (x^{p-1}+z^{p-1})\left(\left(x^{p-1}\right)^2-x^{p-1}z^{p-1}+\left(z^{p-1}\right)^2\right)\equiv 0 \mod \delta' \\
\text{(43) より} \qquad &\equiv (x^{p-1}+z^{p-1})\left(\left(x^{p-1}\right)^2-x^{p-1}z^{p-1}-2x^{p-1}y^{p-1}\right)\equiv 0 \mod \delta' \\
&\equiv (x^{p-1}+z^{p-1})(x^{p-1}-z^{p-1}-2y^{p-1})x^{p-1}\equiv 0 \mod \delta'
\end{aligned}
$$

$$
x^{p-1}+z^{p-1}\equiv 0 \mod \delta' \quad \wedge \quad x^{p-1}-2y^{p-1}-z^{p-1}\equiv 0 \mod \delta'
$$

(32) より $3xz \perp \delta'$ なので矛盾する。また

$$
\begin{aligned}
\text{(29) より } \left(x^{p-1}\right)^2 &\equiv -y^{p-1}z^{p-1} \mod \delta' \\
\left(x^2\right)^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \delta' \\
\text{(38) より } \left(-2^{-1}yz\right)^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \delta' \\
2^{-(p-1)}y^{p-1}z^{p-1} &\equiv -y^{p-1}z^{p-1} \mod \delta' \\
-1 &\equiv 2^{p-1} \mod \delta'
\end{aligned}
$$

.....

$$
\begin{aligned}
\text{(30) より } \left(y^{p-1}\right)^2 &\equiv -x^{p-1}z^{p-1} \mod \delta' \\
\left(y^2\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \delta' \\
\text{(39) より } \left(2^2xz\right)^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \delta' \\
2^{2(p-1)}x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \mod \delta' \\
\left(2^{p-1}\right)^2 &\equiv -1 \mod \delta'
\end{aligned}
$$

.....

$$
\begin{aligned}
\text{(31) より } \left(z^{p-1}\right)^2 &\equiv x^{p-1}y^{p-1} \mod \delta' \\
\left(z^2\right)^{p-1} &\equiv x^{p-1}y^{p-1} \mod \delta' \\
\text{(40) より } \left(-2^{-1}xy\right)^{p-1} &\equiv x^{p-1}y^{p-1} \mod \delta' \\
2^{-(p-1)}x^{p-1}y^{p-1} &\equiv x^{p-1}y^{p-1} \mod \delta' \\
1 &\equiv 2^{p-1} \mod \delta'
\end{aligned}
$$

上式を満たす δ' は存在しない。
よって

$$
\delta' \neq odd
$$

1.10 $\delta' = 2$ のとき

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

$S\text{”} = 2^k$ のとき

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

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

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

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

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

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

よって $2 \mid z$ のとき成り立たない。

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

以上より

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