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

$$p^1 \mid R \tag{1}$$

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、少なくとも $p^2 \mid b^p - c^p = L' \cdot R'$

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

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

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

$x^p = (z-y)\cdot p\alpha^p$ 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

$$p^1 \mid K \text{ でなければならない。}$$

よって

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

一般的に

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

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

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

$$p^1 \mid K$$

□

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

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

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

$\delta \mid S \quad , \delta \mid a$ 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 $p \perp x$

$$\begin{aligned} x &= a'\alpha' & z - y &= a'^p \\ y &= b'\beta' & z - x &= b'^p \\ z &= c'\gamma' & x + y &= c'^p \\ p &\perp xyzS'(※\, p \mid x - z + y) & 2 &\perp \delta \end{aligned}$$

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

Proof 8

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

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

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

$$\delta \perp x$$

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

$\delta \mid b'c'$ 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 $\delta \perp \beta'$

$\delta \mid \gamma' \quad , \ \delta \mid x - y$ 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)

$\theta \perp xyz$ 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 (5)、$yz \equiv UT \mod \theta$ を満たすとき解の候補は以下の 2 通りである。

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

$\theta \perp xyz$ 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 (6)、$xz \equiv U'T' \mod \theta$ を満たすとき解の候補は以下の 2 通りである。

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

$\theta \perp xyz$ 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 (7)、$xy \equiv U"T" \mod \theta$ を満たすとき解の候補は以下の 2 通りである。

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

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

【Solution conditions】

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

(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

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

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

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

$$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \delta \text{ は同時に成り立つ。} \tag{8}$$

$z - x \equiv 0 \mod b$, $x + y \equiv 0 \mod c$ であるから

$$\begin{aligned} z - x &\not\equiv 0 \mod \delta \\ x + y &\not\equiv 0 \mod \delta \end{aligned} \tag{9}$$

また $p - 1 = 2n$ より

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

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。

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

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

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

Definition 9 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 10 以下の関係式を General solution conditions と呼ぶ。

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

1.4.1 $-x^{p-1}\equiv y^{p-1}\equiv z^{p-1} \mod \theta$

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

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

$\mod \theta$ として

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

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

【General solution conditions】

$$\begin{aligned}x^p &\quad -yx^{p-1} &&\equiv -zx^{p-1} \mod \theta\\ -xy^{p-1} &\quad +y^p &&\equiv zy^{p-1} \mod \theta\\ -xz^{p-1} &\quad +yz^{p-1} &&\equiv z^p \mod \theta\end{aligned} \tag{10}$$

1.4.2 共通 1(Common 1)

(10) より

$$\begin{aligned} x^p \quad -yx^{p-1} \quad &\equiv -zx^{p-1} \mod \theta \\ x^p \quad +zx^{p-1} \quad &\equiv yx^{p-1} \mod \theta \end{aligned}$$

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

$$\begin{aligned} -xy^{p-1} \quad +y^p \quad &\equiv zy^{p-1} \mod \theta \\ -zy^{p-1} \quad +y^p \quad &\equiv xy^{p-1} \mod \theta \end{aligned}$$

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

$$\begin{aligned} -xz^{p-1} \quad +yz^{p-1} \quad &\equiv z^p \mod \theta \\ yz^{p-1} \quad -xz^{p-1} \quad &\equiv z^p \mod \theta \end{aligned}$$

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

(11)(12)(13) 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

2 つの因数のうち、一方は δ と互いに素である。 (14)

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

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

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

$$\begin{aligned}
x^p \quad -xy^{p-1} \quad &\equiv xz^{p-1} \mod \theta \\
-yx^{p-1} \quad +y^p \quad &\equiv -yz^{p-1} \mod \theta \\
zx^{p-1} \quad -zy^{p-1} \quad &\equiv z^p \mod \theta
\end{aligned} \tag{15}$$

1.4.4 共通 1.1(Common 1.1)

(15) より

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

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

.....

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

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

δ の定義に反する。

.....

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

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

δ の定義に反する。
よって 3 組共通の同値変換の成立条件は成り立たない。

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

よって (14) より

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

1.4.5 $-z^{p-2} \equiv y^{p-2} \equiv x^{p-2} \mod \theta$

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。

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

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

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

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

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

$\mod \theta$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p + y^2 x^{p-2} &\equiv -z^2 x^{p-2} \mod \theta \\ x^2 y^{p-2} + y^p &\equiv -z^2 y^{p-2} \mod \theta \\ -x^2 z^{p-2} - y^2 z^{p-2} &\equiv z^p \mod \theta \end{aligned} \tag{16}$$

1.4.6 共通 2(Common 2)

(16) より

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

$$\begin{aligned} y^2x^{p-2}\cdot -z^2x^{p-2} \quad &\equiv y^pz^p \mod \delta \\ \left(x^{p-2}\right)^2 \quad &\equiv -y^{p-2}z^{p-2} \mod \delta \end{aligned} \tag{17}$$

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

$$\begin{aligned} x^2y^{p-2}\cdot -z^2y^{p-2} \quad &\equiv x^pz^p \mod \delta \\ \left(y^{p-2}\right)^2 \quad &\equiv -x^{p-2}z^{p-2} \mod \delta \end{aligned} \tag{18}$$

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

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

(17)(18)(19) より

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

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

$-x^{p-1} \equiv z^{p-1} \mod \delta$, $-x^{p-1} \equiv y^{p-1} \mod \delta$ のとき
(9) より

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

(14) より

$$(x^{p-2})^2 + (y^{p-2})^2 + (z^{p-2})^2 \equiv 0 \mod \delta$$

よって

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

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

$$z \not\equiv -y \mod \delta \tag{20}$$

1.4.7 $-y \equiv z \equiv x \mod \theta$

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。

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

$-y \equiv z \equiv x \mod \theta$ のとき

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

$\mod \theta$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p \quad -y^{p-1}x \quad &\equiv z^{p-1}x \mod \theta \\ -x^{p-1}y \quad +y^p \quad &\equiv -z^{p-1}y \mod \theta \\ x^{p-1}z \quad -y^{p-1}z \quad &\equiv z^p \mod \theta \end{aligned} \tag{21}$$

1.4.8 共通 3(Common 3)

(21) より

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

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

$$\begin{aligned} x^{p-1}z \cdot -y^{p-1}z \quad &\equiv x^p y^p \mod \delta \\ z^2 \quad &\equiv -xy \mod \delta \end{aligned} \tag{24}$$

(22)(23)(24) より

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

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

(9)(20) より

$$x^2 + y^2 + z^2 \equiv 0 \mod \delta$$

$$\begin{aligned} (x+z-y)^2 \quad &\equiv 0 \mod \delta \\ x^2 + y^2 + z^2 - 2(xy - xz + yz) \quad &\equiv 0 \mod \delta \\ x^2 + y^2 + z^2 - 2\left((22)\, or\, (23)\, or\, (24)\right) \quad &\equiv 0 \mod \delta \end{aligned}$$

1.4.9 $-z^{p-2} \not\equiv y^{p-2} \not\equiv x^{p-2} \mod \theta$

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

$$\begin{aligned} x^p \quad +x^2y^{p-2} \quad &\equiv x^2z^{p-2} \mod \theta \\ y^2x^{p-2} \quad +y^p \quad &\equiv y^2z^{p-2} \mod \theta \\ z^2x^{p-2} \quad +z^2y^{p-2} \quad &\equiv z^p \mod \theta \end{aligned} \tag{25}$$

1.4.10　共通 2.1(Common 2.1)

(25) より

$$x^2y^{p-2}\cdot x^2z^{p-2}\equiv y^pz^p \mod \delta$$
$$x^4\equiv y^2z^2 \mod \delta$$
$$x^2\equiv \pm yz \mod \delta$$

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

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

(22) より $(-yz)^{p-2}\equiv -y^{p-2}z^{p-2} \mod \delta$

$$-y^{p-2}z^{p-2}\equiv -y^{p-2}z^{p-2} \mod \delta$$

.....

$$y^2x^{p-2}\cdot y^2z^{p-2}\equiv x^pz^p \mod \delta$$
$$y^4\equiv x^2z^2 \mod \delta$$
$$y^2\equiv \pm xz \mod \delta$$

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

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

(23) より $(xz)^{p-2}\equiv -x^{p-2}z^{p-2} \mod \delta$

$$x^{p-2}z^{p-2}\equiv -x^{p-2}z^{p-2} \mod \delta$$

これは δ の定義に反する。

.....

$$z^2x^{p-2}\cdot z^2y^{p-2}\equiv x^py^p \mod \delta$$
$$z^4\equiv x^2y^2 \mod \delta$$
$$z^2\equiv \pm xy \mod \delta$$

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

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

(24) より $(-xy)^{p-2}\equiv x^{p-2}y^{p-2} \mod \delta$

$$-x^{p-2}y^{p-2}\equiv x^{p-2}y^{p-2} \mod \delta$$

これは δ の定義に反する。
よって

$$[x^{p-2}+y^{p-2}-z^{p-2}\not\equiv 0 \mod \delta]$$

これは (8) と矛盾するので

$$\delta\neq odd$$

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 $p \mid z$

$$x = a\alpha \qquad y = b\beta \qquad z = p^n c\gamma$$
$$z - y = a^p \qquad z - x = b^p \qquad x + y = p^{pn-1}c^p$$
$$p \perp xyc\gamma S\text{”} \qquad 2 \perp \delta'$$

Proposition 11 $z + x + y = p^n cS\text{”} \quad , \ \delta' \mid S\text{”} \ \Rightarrow \ \delta' \perp xyz$

Proof 12

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

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

$\delta' \mid S\text{”} \quad , \delta' \mid c$ 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 $\delta' \perp \beta$

$\delta' \mid \alpha \quad , \ \delta' \mid z + y$ 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

$$-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \mod \delta' \text{ は同時に成り立つ。} \tag{26}$$

$z-x \equiv 0 \mod b$, $z-y \equiv 0 \mod a$ であるから

$$\begin{aligned} z-x &\not\equiv 0 \mod \delta' \\ z-y &\not\equiv 0 \mod \delta' \end{aligned} \tag{27}$$

また

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

1.6.2 同値変換 (Equivalence transformation)

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

1.6.3 $-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \mod \theta$

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

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

$\mod \theta$ として

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

$$[x+y+z \equiv 0 \mod \theta]$$

【General solution conditions】

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

1.6.4 共通 4(Common 4)

(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

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

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

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

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

(14) より

2 つの因数のうち、一方は δ' と互いに素である。 (32)

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

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

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

1.6.6　共通 4.1(Common 4.1)

(33) より

$$xy^{p-1} \cdot xz^{p-1} \equiv y^p z^p \mod \delta'$$
$$x^2 \equiv yz \mod \delta'$$

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

δ' の定義に反する。

.....

$$yx^{p-1} \cdot yz^{p-1} \equiv x^p z^p \mod \delta'$$
$$y^2 \equiv xz \mod \delta'$$

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

δ' の定義に反する。

.....

$$zx^{p-1} \cdot zy^{p-1} \equiv x^p y^p \mod \delta'$$
$$z^2 \equiv xy \mod \delta'$$

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

よって 3 組共通の同値変換の成立条件は成り立たない。

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

よって (32) より

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

1.6.7 $-z^{p-2} \equiv y^{p-2} \equiv x^{p-2} \mod \theta$

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。

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

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

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

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

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

$\mod \theta$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p + y^2 x^{p-2} &\equiv -z^2 x^{p-2} \mod \theta \\ x^2 y^{p-2} + y^p &\equiv -z^2 y^{p-2} \mod \theta \\ -x^2 z^{p-2} - y^2 z^{p-2} &\equiv z^p \mod \theta \end{aligned} \tag{34}$$

1.6.8 共通 5(Common 5)

(34) より

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

$$\begin{aligned} y^2x^{p-2}\cdot -z^2x^{p-2} \quad &\equiv y^pz^p \mod \delta' \\ \left(x^{p-2}\right)^2 \quad &\equiv -y^{p-2}z^{p-2} \mod \delta' \end{aligned} \tag{35}$$

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

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

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

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

(35)(36)(37) より

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

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

$-z^{p-1} \equiv x^{p-1} \mod \delta'$, $-z^{p-1} \equiv y^{p-1} \mod \delta'$ のとき
(27) より

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

(32) より

$$(x^{p-2})^2 + (y^{p-2})^2 + (z^{p-2})^2 \equiv 0 \mod \delta'$$

よって

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

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

$$x \not\equiv y \mod \delta' \tag{38}$$

1.6.9 $z \equiv x \equiv y \mod \theta$

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。

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

$z \equiv x \equiv y \mod \theta$ のとき

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

$\mod \theta$ として

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

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

【General solution conditions】

$$\begin{aligned} x^p \quad +y^{p-1}x \quad &\equiv z^{p-1}x \mod \theta \\ x^{p-1}y \quad +y^p \quad &\equiv z^{p-1}y \mod \theta \\ x^{p-1}z \quad +y^{p-1}z \quad &\equiv z^p \mod \theta \end{aligned} \tag{39}$$

1.6.10 共通 6(Common 6)

(39) より

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

$$\begin{aligned} x^{p-1}y \cdot z^{p-1}y \quad &\equiv x^p z^p \mod \delta' \\ y^2 \quad &\equiv xz \mod \delta' \end{aligned} \tag{41}$$

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

(40)(41)(42) より

$$y^3 \equiv z^3 \equiv x^3 \mod \delta'$$

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

(27)(38) より

$$x^2 + y^2 + z^2 \equiv 0 \mod \delta'$$

$$\begin{aligned} (x+z+y)^2 \quad &\equiv 0 \mod \delta' \\ x^2+y^2+z^2+2(xy+xz+yz) \quad &\equiv 0 \mod \delta' \\ x^2+y^2+z^2+2\left((40)\,or\,(41)\,or\,(42)\right) \quad &\equiv 0 \mod \delta' \end{aligned}$$

1.6.11 $-z^{p-2} \not\equiv y^{p-2} \not\equiv x^{p-2} \mod \theta$

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

$$\begin{aligned} x^p \quad +x^2y^{p-2} \quad &\equiv x^2z^{p-2} \mod \theta \\ y^2x^{p-2} \quad +y^p \quad &\equiv y^2z^{p-2} \mod \theta \\ z^2x^{p-2} \quad +z^2y^{p-2} \quad &\equiv z^p \mod \theta \end{aligned} \tag{43}$$

1.6.12　共通 5.1(Common 5.1)

(43) より

$$x^2y^{p-2}\cdot x^2z^{p-2}\equiv y^pz^p \mod \delta'$$
$$x^4\equiv y^2z^2 \mod \delta'$$
$$x^2\equiv \pm yz \mod \delta'$$

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

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

(40) より $(yz)^{p-2}\equiv -y^{p-2}z^{p-2} \mod \delta'$

$$y^{p-2}z^{p-2}\equiv -y^{p-2}z^{p-2} \mod \delta'$$

これは δ' の定義に反する。

.....

$$y^2x^{p-2}\cdot y^2z^{p-2}\equiv x^pz^p \mod \delta'$$
$$y^4\equiv x^2z^2 \mod \delta'$$
$$y^2\equiv \pm xz \mod \delta'$$

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

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

(41) より $(xz)^{p-2}\equiv -x^{p-2}z^{p-2} \mod \delta'$

$$x^{p-2}z^{p-2}\equiv -x^{p-2}z^{p-2} \mod \delta'$$

これは δ' の定義に反する。

.....

$$z^2x^{p-2}\cdot z^2y^{p-2}\equiv x^py^p \mod \delta'$$
$$z^4\equiv x^2y^2 \mod \delta'$$
$$z^2\equiv \pm xy \mod \delta'$$

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

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

(42) より $(xy)^{p-2}\equiv x^{p-2}y^{p-2} \mod \delta'$

$$x^{p-2}y^{p-2}\equiv x^{p-2}y^{p-2} \mod \delta'$$

よって

$$[x^{p-2}+y^{p-2}-z^{p-2}\not\equiv 0 \mod \delta']$$

これは (26) と矛盾するので

$$\delta'\neq odd$$

1.7 $\delta' = 2$

1.7.1 $2 \mid z$, $2 \perp xy$

$S" = 2^k$ のとき

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

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

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

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

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

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

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