On the algebraic symmetry of three sets

Hajime Mashima

Abstract

In this section, the symmetry is shown for two and three pairs of rings.

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 $\delta \perp xyz$

Proposition 1 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 2

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

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

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

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

$p^2 \mid R \Rightarrow p \mid y^{p-1}$ 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 3 $p \perp abc$

- (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。

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

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

(3) より $x = p^2 a\alpha$ と置けるので

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

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

(4)　, $p \perp \alpha^p$ より

$p^1 \mid K$ 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

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

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

$$\begin{aligned}
(\alpha - p^{n(p-1)-1}a^{p-1}) &\perp p \\
p^1 &\mid K
\end{aligned}$$

□

また

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

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

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 4 $x + z - y = p^n aS$, $\delta \mid S \Rightarrow \delta \perp xyz$

Proof 5

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

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

$\delta \mid S$,$\delta \mid a$ 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 $$\delta \perp \beta$$

$\delta \mid \gamma$, $\delta \mid x - y$ 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 $p \perp x$

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

Proposition 6 $x + z - y = a'S'$, $\delta \mid S'$ $\Rightarrow$ $\delta \perp xyz$

Proof 7

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

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

$\delta \mid S'$,$\delta \mid a'$ 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 $$\delta \perp \gamma'$$ □

Theorem 8 (Fermat's Last Theorem)

自然数 n の冪について, 以下の等式を満たす x, y, z の自然数解は存在しない。

$$x^n + y^n \neq z^n \quad (0 < x < y < z \ , \ n \geqq 3)$$

これは以下と同値である。

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

1.2 同値変換 (Equivalence Transformation)

Definition 9

$$\theta \perp xyz$$

$\theta \perp xyz$ 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。

$$\begin{array}{rrll} x^p & +y^p & \equiv z^p & \mod \theta \\ sz^{p-1} & +tx^{p-1} & \equiv uy^{p-1} & \mod \theta \end{array}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} &\equiv x^p y^p \mod \theta \\ stz^{p-1} &\equiv xy^p \mod \theta \end{aligned} \tag{5}$$

$$\begin{aligned} tx^{p-1} \cdot uy^{p-1} &\equiv y^p z^p \mod \theta \\ tux^{p-1} &\equiv yz^p \mod \theta \end{aligned} \tag{6}$$

$$\begin{aligned} sz^{p-1} \cdot uy^{p-1} &\equiv x^p z^p \mod \theta \\ suy^{p-1} &\equiv x^p z \mod \theta \end{aligned} \tag{7}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} \cdot uy^{p-1} &\equiv x^p y^p z^p \mod \theta \\ stu &\equiv xyz \mod \theta \end{aligned} \tag{8}$$

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta$$
$$tu \cdot sz^{p-1} + t^2ux^{p-1} \equiv tu^2y^{p-1} \mod \theta$$

(8) より

$$xyz^p + t^2ux^{p-1} \equiv tu^2y^{p-1} \mod \theta$$
$$xy(x^p + y^p) + t^2ux^{p-1} \equiv tu^2y^{p-1} \mod \theta$$
$$x^{p+1}y + xy^{p+1} + t^2ux^{p-1} \equiv tu^2y^{p-1} \mod \theta$$
$$x^{p+1}y + t^2ux^{p-1} \equiv tu^2y^{p-1} - xy^{p+1} \mod \theta$$
$$x^{p+1}y + t^2ux^{p-1} \equiv y^{p-1}(tu^2 - xy^2) \mod \theta$$
$$tx^{p-1}(x^{p+1}y + t \cdot tux^{p-1}) \equiv y^{p-1}(t^2u^2x^{p-1} - xy^2 \cdot tx^{p-1}) \mod \theta$$

(6) より

$$tx^{p-1}(x^{p+1}y + tyz^p) \equiv y^{p-1}(tu \cdot yz^p - tx^py^2) \mod \theta$$
$$tx^{p-1}(x^{p+1}y + tyz^p) \equiv y^p(tuz^p - tx^py) \mod \theta$$

$tx^{p-1} \equiv y^p$ ならば

$$x^{p+1}y + tyz^p \equiv tuz^p - tx^py \mod \theta$$
$$x^{p+1}y + tx^py \equiv tuz^p - tyz^p \mod \theta$$
$$x^p(xy + ty) \equiv z^{p-1}(tuz - tyz) \mod \theta$$
$$x^p(sxy + sty) \equiv sz^{p-1}(tuz - tyz) \mod \theta$$

$x^p \equiv sz^{p-1}$ ならば

$$sy(x + t) \equiv tz(u - y) \mod \theta$$

$$sy(x^p + tx^{p-1}) \equiv tx^{p-1}z(u - y) \mod \theta$$
$$sy(x^p + y^p) \equiv y^pz(u - y) \mod \theta$$
$$syz^p \equiv y^pz(u - y) \mod \theta$$
$$sz^{p-1} \equiv y^{p-1}(u - y) \mod \theta$$

$$x^p \equiv y^{p-1}(u - y) \mod \theta \tag{9}$$

同様に

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta$$
$$s^2uz^{p-1} + su \cdot tx^{p-1} \equiv su^2y^{p-1} \mod \theta$$

(8) より

$$s^2uz^{p-1} + yzx^p \equiv su^2y^{p-1} \mod \theta$$
$$s^2uz^{p-1} + yz(z^p - y^p) \equiv su^2y^{p-1} \mod \theta$$
$$s^2uz^{p-1} + yz^{p+1} - y^{p+1}z \equiv su^2y^{p-1} \mod \theta$$
$$s^2uz^{p-1} + yz^{p+1} \equiv su^2y^{p-1} + y^{p+1}z \mod \theta$$
$$z^{p-1}(s^2u + yz^2) \equiv su^2y^{p-1} + y^{p+1}z \mod \theta$$
$$z^{p-1}(s^2u^2y^{p-1} + uy^pz^2) \equiv uy^{p-1}(u \cdot suy^{p-1} + y^{p+1}z) \mod \theta$$

(7) より

$$z^{p-1}(sux^pz + uy^pz^2) \equiv uy^{p-1}(ux^pz + y^{p+1}z) \mod \theta$$
$$z^p(sux^p + uy^pz) \equiv uy^{p-1}(ux^pz + y^{p+1}z) \mod \theta$$

$z^p \equiv uy^{p-1}$ ならば

$$sux^p + uy^pz \equiv ux^pz + y^{p+1}z \mod \theta$$
$$sux^p - ux^pz \equiv y^{p+1}z - uy^pz \mod \theta$$
$$x^{p-1}(sux - uxz) \equiv y^p(yz - uz) \mod \theta$$
$$tx^{p-1}(sux - uxz) \equiv y^p(tyz - tuz) \mod \theta$$

$tx^{p-1} \equiv y^p$ ならば

$$ux(s - z) \equiv tz(y - u) \mod \theta$$

$$uy^{p-1}x(s - z) \equiv tz(y^p - uy^{p-1}) \mod \theta$$
$$z^px(s - z) \equiv tz(y^p - z^p) \mod \theta$$
$$z^{p-1}x(s - z) \equiv -tx^p \mod \theta$$
$$z^{p-1}(s - z) \equiv -tx^{p-1} \mod \theta$$

$$z^{p-1}(z - s) \equiv y^p \mod \theta \tag{10}$$

同様に

$$sz^{p-1}+tx^{p-1}\equiv uy^{p-1} \mod \theta$$
$$s^2tz^{p-1}+st^2x^{p-1}\equiv st\cdot uy^{p-1} \mod \theta$$

(8) より

$$s^2tz^{p-1}+st^2x^{p-1}\equiv xzy^p \mod \theta$$
$$s^2tz^{p-1}+st^2x^{p-1}\equiv xz(z^p-x^p) \mod \theta$$
$$s^2tz^{p-1}+st^2x^{p-1}\equiv xz^{p+1}-x^{p+1}z \mod \theta$$
$$x^{p+1}z+st^2x^{p-1}\equiv xz^{p+1}-s^2tz^{p-1} \mod \theta$$
$$x^{p-1}(x^2z+st^2)\equiv xz^{p+1}-s^2tz^{p-1} \mod \theta$$
$$x^{p-1}(sx^2z^p+s^2t^2z^{p-1})\equiv sz^{p-1}(xz^{p+1}-s\cdot stz^{p-1}) \mod \theta$$

(5) より

$$x^{p-1}(sx^2z^p+st\cdot xy^p)\equiv sz^{p-1}(xz^{p+1}-sxy^p) \mod \theta$$
$$x^p(sxz^p+sty^p)\equiv sz^{p-1}(xz^{p+1}-sxy^p) \mod \theta$$

$x^p\equiv sz^{p-1}$ ならば

$$sxz^p+sty^p\equiv xz^{p+1}-sxy^p \mod \theta$$
$$sty^p+sxy^p\equiv xz^{p+1}-sxz^p \mod \theta$$
$$y^{p-1}(sty+sxy)\equiv z^p(xz-sx) \mod \theta$$
$$uy^{p-1}(sty+sxy)\equiv z^p(uxz-sux) \mod \theta$$

$uy^{p-1}\equiv z^p$ ならば

$$sy(t+x)\equiv ux(z-s) \mod \theta$$

$$sz^{p-1}y(t+x)\equiv ux(z^p-sz^{p-1}) \mod \theta$$
$$x^py(t+x)\equiv ux(z^p-x^p) \mod \theta$$
$$x^{p-1}y(t+x)\equiv uy^p \mod \theta$$
$$x^{p-1}(t+x)\equiv uy^{p-1} \mod \theta$$

$$x^{p-1}(t+x)\equiv z^p \mod \theta \tag{11}$$

1.3 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。

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

$$\begin{aligned}
z^p - y^p + Uz^{p-1} &\equiv Ty^{p-1} \mod \theta \\
z^p + Uz^{p-1} &\equiv y^p + Ty^{p-1} \mod \theta \\
z^{p-1}(z+U) &\equiv y^{p-1}(y+T) \mod \theta \\
z^{p-1}(yz+yU) &\equiv y \cdot y^{p-1}(y+T) \mod \theta
\end{aligned} \tag{12}$$

$$yz \equiv UT \mod \theta \Rightarrow \tag{13}$$

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

同様に

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

よって解の候補は以下の 2 通りである。

$$\begin{aligned}
&Uz^{p-1} \equiv y^p \mod \theta \\
&Ty^{p-1} \equiv z^p \mod \theta \\
&\quad or \\
&Uz^{p-1} \equiv -z^p \mod \theta \\
&Ty^{p-1} \equiv -y^p \mod \theta
\end{aligned} \tag{14}$$

$\theta \perp xyz$ 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。

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

$$\begin{aligned}
-U'z^{p-1} + z^p - x^p &\equiv -T'x^{p-1} \mod \theta \\
-U'z^{p-1} + z^p &\equiv x^p - T'x^{p-1} \mod \theta \\
-z^{p-1}(U' - z) &\equiv x^{p-1}(x - T') \mod \theta \qquad (15) \\
-z^{p-1}(U'x - xz) &\equiv x \cdot x^{p-1}(x - T') \mod \theta
\end{aligned}$$

$$xz \equiv U'T' \mod \theta \Rightarrow \qquad (16)$$

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

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。

$$\begin{aligned}
&-U'z^{p-1} \equiv x^p \mod \theta \\
&-T'x^{p-1} \equiv z^p \mod \theta \\
&\quad or \qquad (17) \\
&-U'z^{p-1} \equiv -z^p \mod \theta \\
&-T'x^{p-1} \equiv -x^p \mod \theta
\end{aligned}$$

$\theta \perp xyz$ 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。

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

$$\begin{aligned} -U"y^{p-1} - T"x^{p-1} &\equiv x^p + y^p \mod \theta \\ -x^p - T"x^{p-1} &\equiv y^p + U"y^{p-1} \mod \theta \\ -x^{p-1}(x + T") &\equiv y^{p-1}(y + U") \mod \theta \\ -x^{p-1}(xy + T"y) &\equiv y \cdot y^{p-1}(y + U") \mod \theta \end{aligned} \tag{18}$$

$$xy \equiv U"T" \mod \theta \Rightarrow \tag{19}$$

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

同様に

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

よって解の候補は以下の 2 通りである。

$$\begin{gathered} -U"y^{p-1} \equiv x^p \mod \theta \\ -T"x^{p-1} \equiv y^p \mod \theta \\ or \\ -U"y^{p-1} \equiv y^p \mod \theta \\ -T"x^{p-1} \equiv x^p \mod \theta \end{gathered} \tag{20}$$

1.4 合同条件 (Congruent Conditions)

Proposition 10 $x^p + y^p \equiv z^p \mod \delta$ との合同条件は

$$\begin{aligned} xyz &\perp \theta \\ xyz &\equiv stu \mod \theta \\ xyz &\equiv (u-y)(z-s)(t+x) \mod \theta \end{aligned}$$

および解の条件を満たし、
(9)(11)(10) より以下に示す同値変換が成り立つものである。

$$\begin{gathered} sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta \\ \Leftrightarrow \\ (u-y)y^{p-1} + (z-s)z^{p-1} \equiv (t+x)x^{p-1} \mod \theta \end{gathered}$$

1.4.1 $x - y \equiv -z \mod \delta$

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

上式を並び替える。

Definition 11

$$\begin{aligned} L_1: \quad & x^p - yx^{p-1} && \equiv -zx^{p-1} \mod \delta && (21) \\ L_2: \quad & -xy^{p-1} + y^p && \equiv zy^{p-1} \mod \delta && (22) \\ L_3: \quad & -xz^{p-1} + yz^{p-1} && \equiv z^p \mod \delta && (23) \end{aligned}$$

$$\begin{aligned} x^p \quad & +tx^{p-1} && \equiv (t+x)x^{p-1} \mod \delta \\ (u-y)y^{p-1} \quad & +y^p && \equiv uy^{p-1} \mod \delta \\ sz^{p-1} \quad & +(z-s)z^{p-1} && \equiv z^p \mod \delta \end{aligned}$$

よって

$$\begin{aligned} s &\equiv -x \mod \delta \\ t &\equiv -y \mod \delta \\ u &\equiv z \mod \delta \end{aligned} \tag{24}$$

$$\begin{aligned} & xyz \perp \delta \\ & xyz \equiv stu \mod \delta \\ & xyz \equiv (u-y)(z-s)(t+x) \mod \delta \end{aligned}$$

$$
\begin{aligned}
sz^{p-1}\cdot(t+x)x^{p-1} &\equiv x^p z^p \mod \delta\\
s\cdot(t+x) &\equiv xz \mod \delta\\
-x\cdot(-z) &\equiv xz \mod \delta\\
(u-y)y^{p-1}\cdot tx^{p-1} &\equiv x^p y^p \mod \delta\\
(u-y)\cdot t &\equiv xy \mod \delta\\
(-x)\cdot -y &\equiv xy \mod \delta\\
(z-s)z^{p-1}\cdot uy^{p-1} &\equiv y^p z^p \mod \delta\\
(z-s)\cdot u &\equiv yz \mod \delta\\
(y)\cdot z &\equiv yz \mod \delta
\end{aligned}
$$

(13)(16)(19) より (24) は解の条件および同値変換を満たす。

$$
\begin{array}{cccc}
x^p & +y^p \equiv & z^p & \mod \delta\\
 & & \Leftrightarrow & \\
x^p & +yz^{p-1} & \equiv zy^{p-1} & \mod \delta\\
-xz^{p-1} & +y^p & \equiv -zx^{p-1} & \mod \delta\\
-xy^{p-1} & -yx^{p-1} & \equiv z^p & \mod \delta
\end{array}
\tag{25}
$$

1.4.2 $x+z\equiv y \mod \delta$

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

上式を並び替える。

Definition 12

$$R_1: \quad x^p+zx^{p-1} \equiv yx^{p-1} \mod \delta \tag{26}$$
$$R_2: \quad -zy^{p-1}+y^p \equiv xy^{p-1} \mod \delta \tag{27}$$
$$R_3: \quad yz^{p-1}-xz^{p-1} \equiv z^p \mod \delta \tag{28}$$

$$
\begin{array}{cccc}
x^p & +tx^{p-1} & \equiv (t+x)x^{p-1} & \mod \delta\\
(u-y)y^{p-1} & +y^p & \equiv uy^{p-1} & \mod \delta\\
sz^{p-1} & +(z-s)z^{p-1} & \equiv z^p & \mod \delta
\end{array}
$$

Proposition 13

(14)(17)(20) より、以下は (24) と 2 項の位相を交換した組である。

$$
\begin{array}{cccc}
s & \equiv & y & \mod \delta\\
t & \equiv & z & \mod \delta\\
u & \equiv & x & \mod \delta
\end{array}
$$

1.4.3 共通 (Common)

(21)(26) より

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

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

(22)(27) より

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

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

(23)(28) より

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

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

(29)(30)(31) より

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

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

Definition 14

$$\begin{aligned}
0 &\equiv \left(z^{p-1}\right)^3 - \left(y^{p-1}\right)^3 \equiv (L_1)(R_1) \mod \delta \\
0 &\equiv \left(x^{p-1}\right)^3 + \left(z^{p-1}\right)^3 \equiv (L_2)(R_2) \mod \delta \\
0 &\equiv \left(x^{p-1}\right)^3 + \left(y^{p-1}\right)^3 \equiv (L_3)(R_3) \mod \delta
\end{aligned}$$

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

$$\begin{aligned}
x^p + y^p &\equiv z^p \mod 3 \\
3 \perp xyz &\Rightarrow x + y \equiv z \mod 3 \qquad \text{(Fermat's little theorem)} \\
x &\equiv \pm 1 \mod 3 \\
y &\equiv \pm 1 \mod 3 \\
z &\equiv \mp 1 \mod 3 \\
\delta &\neq 3
\end{aligned}$$

R_1, R_2, R_3 と L_1, L_2, L_3 は少なくとも 1 つの式が成立しない場合、
同値変換は成り立たない。

$$\begin{gathered}
sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \delta \\
\not\Leftrightarrow \\
(u - y)y^{p-1} + (z - s)z^{p-1} \equiv (t + x)x^{p-1} \mod \delta
\end{gathered}$$

よって

$$\begin{gathered}
L \equiv 0 \mod \delta \qquad R \not\equiv 0 \mod \delta \\
or \\
L \not\equiv 0 \mod \delta \qquad R \equiv 0 \mod \delta
\end{gathered}$$

1.4.4 $R \equiv 0 \mod \delta$

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

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

$$x^p - xy^{p-1} \equiv xz^{p-1} \mod \delta$$

$$
\begin{aligned}
-xy^{p-1} &\equiv y^p \mod \delta \\
xz^{p-1} &\equiv z^p \mod \delta \Rightarrow
\end{aligned}
$$

$z^p y^p \perp \delta$ なので

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

. . . .

$$-yx^{p-1} + y^p \equiv -yz^{p-1} \mod \delta$$

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

$z^p \perp \delta$ なので

$$-y \not\equiv x \mod \delta$$

. . . .

$$zx^{p-1} - zy^{p-1} \equiv z^p \mod \delta$$

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

$y^p \perp \delta$ なので

$$z \not\equiv x \mod \delta$$

. . . .

よって

$$
\begin{aligned}
& x^p \quad + y^p && \equiv z^p \mod \delta \\
& && \Leftrightarrow \\
R_3, R_2: \quad & x^p \quad - xz^{p-1} && \equiv xy^{p-1} \mod \delta && (32) \\
R_3, R_1: \quad & yz^{p-1} + y^p && \equiv yx^{p-1} \mod \delta && (33) \\
R_2, R_1: \quad & -zy^{p-1} + zx^{p-1} && \equiv z^p \mod \delta && (34)
\end{aligned}
$$

1.4.5 $R \not\equiv 0 \mod \delta$

Definition 15

$$\begin{aligned} zx^{p-1} &= R_1^1 \quad , \quad yx^{p-1} = R_1^2 \\ -zy^{p-1} &= R_2^1 \quad , \quad xy^{p-1} = R_2^2 \\ yz^{p-1} &= R_3^1 \quad , \quad -xz^{p-1} = R_3^2 \end{aligned}$$

$$\begin{aligned} (32) \text{ より } -xz^{p-1} \cdot xy^{p-1} &\equiv y^p z^p \mod \delta \\ -x^2 &\equiv yz \mod \delta \\ x^2 &\equiv -yz \mod \delta \end{aligned}$$

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

$$R_3^2 \cdot R_2^2 \equiv y^p z^p \mod \delta$$

....

$$\begin{aligned} (33) \text{ より } yz^{p-1} \cdot yx^{p-1} &\equiv x^p z^p \mod \delta \\ y^2 &\equiv xz \mod \delta \end{aligned}$$

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

$$R_3^1 \cdot R_1^2 \not\equiv x^p z^p \mod \delta$$

....

$$\begin{aligned} (34) \text{ より } -zy^{p-1} \cdot zx^{p-1} &\equiv x^p y^p \mod \delta \\ -z^2 &\equiv xy \mod \delta \\ z^2 &\equiv -xy \mod \delta \end{aligned}$$

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

$$R_2^1 \cdot R_1^1 \not\equiv x^p y^p \mod \delta$$

よって $R \not\equiv 0 \mod \delta$

1.4.6 $L \equiv 0 \mod \delta$

(12)(15)(18) と (25) より $-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \delta$

Proposition 16

$e, d = odd$、$e \perp d$　, $xz \perp \theta$

$$\begin{aligned} x^d &\equiv z^d \mod \theta \qquad (35)\\ x^e &\equiv z^e \mod \theta \\ &\Rightarrow \\ x &\equiv z \mod \theta \qquad (36) \end{aligned}$$

Proof 17

d_N を d の素因数とすると、$d = d_1 d_2 d_3 \cdots$

Fermat's little theorem より

$$e^{d_1-1} \equiv 1 \mod d_1$$
$$(e^{d_1-1})^{d_2-1} \equiv 1 \mod d_2$$

$(e^{d_1-1})^{d_2-1} = d_1 d_2 m + 1$ とおけるので

$$(e^{d_1-1})^{d_2-1} \equiv 1 \mod d_1 d_2$$

$$((e^{d_1-1})^{d_2-1})^{d_3-1} \equiv 1 \mod d_1 d_2 d_3$$
$$\vdots$$
$$e^n \equiv 1 \mod d$$

よって $e^n = dm + 1$ が存在する。($dm + 1 = odd$　, $dm = even$)

$$(x^e)^{e\cdots} \equiv (z^e)^{e\cdots} \mod \theta$$
$$x^{e^n} \equiv z^{e^n} \mod \theta$$
$$x^{dm+1} \equiv z^{dm+1} \mod \theta$$

(35) より

$$x^{dm} \equiv z^{dm} \mod \theta$$
$$x \equiv z \mod \theta$$

□

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

Fermat's little theorem より

$$x^{\delta-1} \equiv z^{\delta-1} \mod \delta$$
$$(x^{\delta-1})^2 \equiv (z^{\delta-1})^2 \mod \delta$$
$$x^{2\delta-2} \equiv z^{2\delta-2} \mod \delta$$

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

$p-\delta = 2^{n-1}d$ $(d \perp 2 \quad , \ n > 1)$ とおくと

$$(x^{2^n})^d \equiv (z^{2^n})^d \mod \delta$$

$\delta - 1 = 2k$ とおくと

$$x^{2k} \equiv z^{2k} \mod \delta$$
$$(x^{2^n})^{2kj} \equiv (z^{2^n})^{2kj} \mod \delta$$

j は $2kj - d = e \quad , \ e \perp d$ となるものと仮定すると

$$(x^{2^n})^e \equiv (z^{2^n})^e \mod \delta$$

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

$$z^{2^n} \equiv y^{2^n} \mod \delta$$
$$x^{2^n} \equiv z^{2^n} \mod \delta$$
$$x^{2^n} \equiv y^{2^n} \mod \delta$$

$d_p = odd$ と仮定する。

$p-1 = 2^n d_p$ ならば、$z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \mod \delta$

$d_\delta = odd$ と仮定する。

$p-1 = 2^{n-2} d_p$ ならば $\delta - 1 = 2^{n-2} d_\delta$ と置けるので

$$\begin{aligned}(p-1)-(\delta-1) &= 2^{n-2}d_p - 2^{n-2}d_\delta \\ p-\delta &= 2^{n-2}(d_p - d_\delta) \\ p-\delta &= 2^{n-2}\cdot 2d\end{aligned}$$

$$\begin{aligned}-x^{2^{n-2}} &\equiv z^{2^{n-2}} \mod \delta \\ (-x^{2^{n-2}})^{d_\delta} &\equiv (z^{2^{n-2}})^{d_\delta} \mod \delta \\ -x^{\delta-1} &\not\equiv z^{\delta-1} \mod \delta\end{aligned}$$

$p-1 = 2^{n-1} d_p$ ならば、$k' > 0$ として

$$\begin{aligned}(p-1)-(\delta-1) &= 2^{n-1}d_p - 2^{n-1+k'}d_\delta \\ p-\delta &= 2^{n-1}(d_p - 2^{k'}d_\delta) \\ p-\delta &= 2^{n-1}d\end{aligned}$$

よって

$$\begin{aligned}z^{2^{n-1}} &\equiv y^{2^{n-1}} \mod \delta \\ -x^{2^{n-1}} &\equiv z^{2^{n-1}} \mod \delta \\ -x^{2^{n-1}} &\equiv y^{2^{n-1}} \mod \delta\end{aligned} \tag{37}$$

1.4.7 $L \not\equiv 0 \mod \delta$

$\delta \perp xyz$ 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。

$$x^p + Uz^{p-2^{n-1}} \equiv Ty^{p-2^{n-1}} \mod \delta$$

$$\begin{aligned}
z^p - y^p + Uz^{p-2^{n-1}} &\equiv Ty^{p-2^{n-1}} \mod \delta \\
z^p + Uz^{p-2^{n-1}} &\equiv y^p + Ty^{p-2^{n-1}} \mod \delta \\
z^{p-2^{n-1}}(z^{2^{n-1}} + U) &\equiv y^{p-2^{n-1}}(y^{2^{n-1}} + T) \mod \delta \\
z^{p-2^{n-1}}(y^{2^{n-1}}z^{2^{n-1}} + y^{2^{n-1}}U) &\equiv y^{2^{n-1}} \cdot y^{p-2^{n-1}}(y^{2^{n-1}} + T) \mod \delta
\end{aligned}$$

$$y^{2^{n-1}}z^{2^{n-1}} \equiv UT \mod \delta \Rightarrow$$

$$\begin{aligned}
z^{p-2^{n-1}}(UT + y^{2^{n-1}}U) &\equiv y^p(y^{2^{n-1}} + T) \mod \delta \\
Uz^{p-2^{n-1}}(T + y^{2^{n-1}}) &\equiv y^p(T + y^{2^{n-1}}) \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
z^{2^{n-1}} \cdot z^{p-2^{n-1}}(z^{2^{n-1}} + U) &\equiv y^{p-2^{n-1}}(y^{2^{n-1}}z^{2^{n-1}} + z^{2^{n-1}}T) \mod \delta \\
z^p(z^{2^{n-1}} + U) &\equiv y^{p-2^{n-1}}(UT + z^{2^{n-1}}T) \mod \delta \\
z^p(U + z^{2^{n-1}}) &\equiv Ty^{p-2^{n-1}}(U + z^{2^{n-1}}) \mod \delta
\end{aligned}$$

$$x^p + y^{2^{n-1}}z^{p-2^{n-1}} \equiv z^{2^{n-1}}y^{p-2^{n-1}} \mod \delta$$
$$z^{p-2^{n-1}}(z^{2^{n-1}} + y^{2^{n-1}}) \equiv y^{p-2^{n-1}}(z^{2^{n-1}} + y^{2^{n-1}}) \mod \delta$$

(37) より $z^{2^{n-1}} + y^{2^{n-1}} \not\equiv 0 \mod \delta$ なので

$$z^{p-2^{n-1}} \equiv y^{p-2^{n-1}} \mod \delta$$

$p - 2^{n-1} = odd$ なので、(36) より

$$z \not\equiv y \mod \delta$$

$\delta \perp xyz$ 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。

$$-U'z^{p-2^{n-1}} + y^p \equiv -T'x^{p-2^{n-1}} \mod \delta$$

$$\begin{aligned}
-U'z^{p-2^{n-1}} + z^p - x^p &\equiv -T'x^{p-2^{n-1}} \mod \delta \\
-U'z^{p-2^{n-1}} + z^p &\equiv x^p - T'x^{p-2^{n-1}} \mod \delta \\
-z^{p-2^{n-1}}(U' - z^{2^{n-1}}) &\equiv x^{p-2^{n-1}}(x^{2^{n-1}} - T') \mod \delta \\
-z^{p-2^{n-1}}(U'x^{2^{n-1}} - x^{2^{n-1}}z^{2^{n-1}}) &\equiv x^{2^{n-1}} \cdot x^{p-2^{n-1}}(x^{2^{n-1}} - T') \mod \delta
\end{aligned}$$

$$x^{2^{n-1}}z^{2^{n-1}} \equiv U'T' \mod \delta \Rightarrow$$

$$\begin{aligned}
-z^{p-2^{n-1}}(U'x^{2^{n-1}} - U'T') &\equiv x^p(x^{2^{n-1}} - T') \mod \delta \\
-U'z^{p-2^{n-1}}(x^{2^{n-1}} - T') &\equiv x^p(x^{2^{n-1}} - T') \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
-z^{2^{n-1}} \cdot z^{p-2^{n-1}}(U' - z^{2^{n-1}}) &\equiv x^{p-2^{n-1}}(x^{2^{n-1}}z^{2^{n-1}} - T'z^{2^{n-1}}) \mod \delta \\
-z^p(U' - z^{2^{n-1}}) &\equiv x^{p-2^{n-1}}(U'T' - T'z^{2^{n-1}}) \mod \delta \\
z^p(U' - z^{2^{n-1}}) &\equiv -T'x^{p-2^{n-1}}(U' - z^{2^{n-1}}) \mod \delta
\end{aligned}$$

$$-x^{2^{n-1}}z^{p-2^{n-1}} + y^p \equiv -z^{2^{n-1}}x^{p-2^{n-1}} \mod \delta$$
$$-z^{p-2^{n-1}}(x^{2^{n-1}} - z^{2^{n-1}}) \equiv x^{p-2^{n-1}}(x^{2^{n-1}} - z^{2^{n-1}}) \mod \delta$$

(37) より $x^{2^{n-1}} - z^{2^{n-1}} \not\equiv 0 \mod \delta$ なので

$$-z^{p-2^{n-1}} \equiv x^{p-2^{n-1}} \mod \delta$$

$p - 2^{n-1} = odd$ なので、(36) より

$$\begin{aligned}
x^{2^n j} &\equiv z^{2^n j} \mod \delta \\
&or \\
-x^{2^{n-1} j} &\equiv z^{2^{n-1} j} \mod \delta
\end{aligned}$$

$z \not\equiv x \mod \delta$ であるから

$$-z \equiv x \mod \delta \tag{38}$$

$\delta \perp xyz$ 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。

$$U"y^{p-2^{n-1}} + T"x^{p-2^{n-1}} \equiv z^p \mod \delta$$

$$\begin{aligned}
U"y^{p-2^{n-1}} + T"x^{p-2^{n-1}} &\equiv x^p + y^p \mod \delta \\
-x^p + T"x^{p-2^{n-1}} &\equiv y^p - U"y^{p-2^{n-1}} \mod \delta \\
-x^{p-2^{n-1}}(x^{2^{n-1}} - T") &\equiv y^{p-2^{n-1}}(y^{2^{n-1}} - U") \mod \delta \\
-x^{p-2^{n-1}}(x^{2^{n-1}}y^{2^{n-1}} - T"y^{2^{n-1}}) &\equiv y^{2^{n-1}} \cdot y^{p-2^{n-1}}(y^{2^{n-1}} - U") \mod \delta
\end{aligned}$$

$$x^{2^{n-1}}y^{2^{n-1}} \equiv U"T" \mod \delta \Rightarrow$$

$$\begin{aligned}
-x^{p-2^{n-1}}(U"T" - T"y^{2^{n-1}}) &\equiv y^p(y^{2^{n-1}} - U") \mod \delta \\
T"x^{p-2^{n-1}}(U" - y^{2^{n-1}}) &\equiv y^p(U" - y^{2^{n-1}}) \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
-x^{2^{n-1}} \cdot x^{p-2^{n-1}}(x^{2^{n-1}} - T") &\equiv y^{p-2^{n-1}}(x^{2^{n-1}}y^{2^{n-1}} - x^{2^{n-1}}U") \mod \delta \\
-x^p(x^{2^{n-1}} - T") &\equiv y^{p-2^{n-1}}(U"T" - x^{2^{n-1}}U") \mod \delta \\
x^p(x^{2^{n-1}} - T") &\equiv U"y^{p-2^{n-1}}(x^{2^{n-1}} - T") \mod \delta
\end{aligned}$$

$$x^{2^{n-1}}y^{p-2^{n-1}} + y^{2^{n-1}}x^{p-2^{n-1}} \equiv z^p \mod \delta$$
$$x^{p-2^{n-1}}(x^{2^{n-1}} - y^{2^{n-1}}) \equiv y^{p-2^{n-1}}(x^{2^{n-1}} - y^{2^{n-1}}) \mod \delta$$

(37) より $x^{2^{n-1}} - y^{2^{n-1}} \not\equiv 0 \mod \delta$ なので

$$x^{p-2^{n-1}} \equiv y^{p-2^{n-1}} \mod \delta$$

$p - 2^{n-1} = odd$ なので、(36) より

$$\begin{aligned}
x^{2^n j} &\equiv y^{2^n j} \mod \delta \\
&or \\
-x^{2^{n-1} j} &\equiv y^{2^{n-1} j} \mod \delta
\end{aligned}$$

$-x \not\equiv y \mod \delta$ であるから

$$x \equiv y \mod \delta$$
$$x^p \equiv y^p \mod \delta$$

(38) より

$$x^p \equiv -z^p \mod \delta$$
$$x^p \equiv -x^p - y^p \mod \delta$$
$$3x^p \not\equiv 0 \mod \delta$$

よって $L \not\equiv 0 \mod \delta$

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。

・$2 \mid y$　,　$2 \perp xz$ のときは $y + z - x$
・$2 \mid z$　,　$2 \perp xy$ のときは $z + x + y$ にて同様の結果を得る。

よって $\delta = 2$ のとき

$$x^p + y^p \not\equiv z^p \mod \delta$$