

General solution conditions

Hajime Mashima

Abstract

Modulo not divisible by xyz and possible expansions.

Contents

1	introduction	2
1.1	$\delta \perp xyz$	3
1.1.1	$p \mid x$	5
1.1.2	$p \perp x$	6
1.2	解の条件 (Solution conditions)	7
1.3	同値変換 (Equivalence transformation)	11
1.4	一般解の条件 (General solution conditions)	11
1.4.1	$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_{l1}}$ のとき	11
1.4.2	Common to $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_{r1}}$	12
1.4.3	$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_{r1}}$	14
1.4.4	$-y \equiv z \equiv x \pmod{\theta_{l2}}$ のとき	14
1.4.5	Common to $-y \not\equiv z \not\equiv x \pmod{\theta_{r2}}$	15
1.4.6	$x^{p-2} \equiv y^{p-2} \equiv z^{p-2} \pmod{\theta_{L1}}$ のとき	16
1.4.7	Common to $x^{p-2} \not\equiv y^{p-2} \not\equiv z^{p-2} \pmod{\theta_{R1}}$	17
1.4.8	$x^{p-2} \not\equiv y^{p-2} \not\equiv z^{p-2} \pmod{\theta_{R1}}$	18
1.4.9	$-z^2 \equiv x^2 \equiv y^2 \pmod{\theta_{L2}}$ のとき	18
1.4.10	Common to $-z^2 \not\equiv x^2 \not\equiv y^2 \pmod{\theta_{R2}}$	19
1.4.11	$-z^2 \equiv x^2 \equiv y^2 \pmod{\delta}$ or $-z^2 \not\equiv x^2 \not\equiv y^2 \pmod{\delta}$ のとき	20
1.5	$\delta = 2$	22
1.5.1	$2 \mid x$, $2 \perp yz$	22
1.6	$\delta' \perp xyz$	23
1.6.1	$p \mid z$	23
1.6.2	同値変換 (Equivalence transformation)	24
1.6.3	$-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \pmod{\theta'_{l1}}$ のとき	24
1.6.4	Common to $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\theta'_{r1}}$	25
1.6.5	$-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\theta'_{r1}}$	26
1.6.6	$z \equiv x \equiv y \pmod{\theta'_{l2}}$ のとき	26
1.6.7	Common to $z \not\equiv x \not\equiv y \pmod{\theta'_{r2}}$	27
1.6.8	$-y^{p-2} \equiv x^{p-2} \equiv z^{p-2} \pmod{\theta'_{L1}}$ のとき	28
1.6.9	Common to $-y^{p-2} \not\equiv x^{p-2} \not\equiv z^{p-2} \pmod{\theta'_{R1}}$	29
1.6.10	$-y^{p-2} \not\equiv x^{p-2} \not\equiv z^{p-2} \pmod{\theta'_{R1}}$	30

1.6.11	$-x^2 \equiv y^2 \equiv z^2 \pmod{\theta'_{L2}}$ のとき	30
1.6.12	Common to $-y^2 \not\equiv x^2 \not\equiv z^2 \pmod{\theta'_{R2}}$	31
1.6.13	$-y^2 \equiv x^2 \equiv z^2 \pmod{\delta'}$ or $-y^2 \not\equiv x^2 \not\equiv z^2 \pmod{\delta'}$ のとき	32
1.6.14	$2 \mid z$, $2 \perp xy$	34
1.7	補足 1(supplement 1)	35
1.7.1	$x^p + y^p \equiv z^p \pmod{\theta}$ が成り立つ可能性のある条件	36
1.8	補足 2(supplement 2)	37
1.8.1	$-z^{p-2} \equiv x^{p-2} \equiv y^{p-2} \pmod{\Theta_{L1}}$ のとき	37
1.8.2	Common to $-z^{p-2} \not\equiv x^{p-2} \not\equiv y^{p-2} \pmod{\Theta_{R1}}$	38
1.8.3	$-z^{p-2} \not\equiv x^{p-2} \not\equiv y^{p-2} \pmod{\Theta_{R1}}$	39
1.8.4	$x^2 \equiv y^2 \equiv z^2 \pmod{\Theta_{L2}}$ のとき	39
1.8.5	Common to $x^2 \not\equiv y^2 \not\equiv z^2 \pmod{\Theta_{R2}}$	40
1.8.6	$x^2 \equiv y^2 \equiv z^2 \pmod{\Theta_0}$ or $x^2 \not\equiv y^2 \not\equiv z^2 \pmod{\Theta_0}$ のとき	41

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 $\delta \perp xyz$

Theorem 1 (Fermat's Last Theorem)

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

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

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

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

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

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

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

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

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

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

また、 p を除く素数に関して

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

Definition 4 $p \perp abc$

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

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

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

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

よって、少なくとも

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

$$\begin{aligned} (x - (z - y))^p &= x^p - \frac{p!}{(p-1)!1!} x^{p-1}(z - y) + \frac{p!}{(p-2)!2!} x^{p-2}(z - y)^2 - \frac{p!}{(p-3)!3!} x^{p-3}(z - y)^3 + \\ &\dots + \frac{p!}{1!(p-1)!} x(z - y)^{p-1} - (z - y)^p \end{aligned}$$

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

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

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

(3) より $x = p^2 a \alpha$ と置けるので

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

(4) , $p \perp \alpha^p$ より

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

よって

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

一般的に

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

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

$$\begin{aligned} (\alpha - p^{n(p-1)-1} a^{p-1}) &\perp p \\ p^n &| K \quad , \quad (n = 1) \end{aligned}$$

□

また

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

1.1.1 $p \mid x$

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

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

Proof 6

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

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

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

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

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

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

よって

$$\delta \perp \beta$$

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

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

よって

$$\delta \perp \gamma$$

□

1.1.2 $p \perp x$

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

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

Proof 8

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

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

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

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

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

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

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

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

よって $\delta \perp \gamma'$

□

1.2 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。

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

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

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

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

同様に

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

よって (5)、 $yz \equiv UT \pmod{\theta}$ を満たすとき解の候補は以下の 2 通りである。

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

$\theta \perp xyz$ 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。

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

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

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

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

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

同様に

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

よって (6)、 $xz \equiv U'T' \pmod{\theta}$ を満たすとき解の候補は以下の 2 通りである。

$$-U'z^{p-1} \equiv x^p \pmod{\theta}$$

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

or

$$-U'z^{p-1} \equiv -z^p \pmod{\theta}$$

$$-T'x^{p-1} \equiv -x^p \pmod{\theta}$$

$\theta \perp xyz$ 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。

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

$$\begin{aligned} -U'' y^{p-1} - T'' x^{p-1} &\equiv x^p + y^p \pmod{\theta} \\ -x^p - T'' x^{p-1} &\equiv U'' y^{p-1} + y^p \pmod{\theta} \\ -x^{p-1}(x + T'') &\equiv y^{p-1}(U'' + y) \pmod{\theta} \\ -x^{p-1}(xy + T'' y) &\equiv y \cdot y^{p-1}(U'' + y) \pmod{\theta} \end{aligned} \quad (7)$$

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

$$xy \equiv U'' T'' \pmod{\theta} \Rightarrow$$

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

同様に

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

よって (7)、 $xy \equiv U'' T'' \pmod{\theta}$ を満たすとき解の候補は以下の 2 通りである。

$$-U'' y^{p-1} \equiv x^p \pmod{\theta}$$

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

or

$$-U'' y^{p-1} \equiv y^p \pmod{\theta}$$

$$-T'' x^{p-1} \equiv x^p \pmod{\theta}$$

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

【Solution conditions】

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

(5),(6),(7) から

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

$x - y \equiv -z \pmod{\delta}$ より

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

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

なので

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

よって

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

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

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

また $p - 1 = 2n$ より

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

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

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

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

1.3 同値変換 (Equivalence transformation)

s, t, u を変数とおく。

$\theta \perp stuxyz$ ならば、その逆元が存在するので異なる文字式で同値変換できる。

Definition 10 【Equivalence transformation】

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

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

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

このとき以下を同値変換の成立条件と呼び、以降 [] で示す。

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

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

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

1.4 一般解の条件 (General solution conditions)

Definition 11 以下の関係式を General solution conditions と呼ぶ。
同値変換の成立条件が 3 組共通のときを示す。

$$\begin{aligned} (u_3 - t_2)x^{p-1} + t_2 x^{p-1} &\equiv u_3 x^{p-1} \pmod{\theta} \\ s_3 y^{p-1} + (u_2 - s_3)y^{p-1} &\equiv u_2 y^{p-1} \pmod{\theta} \\ s_2 z^{p-1} + t_3 z^{p-1} &\equiv (s_2 + t_3)z^{p-1} \pmod{\theta} \end{aligned}$$

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

$$\begin{aligned} s_1 x^{p-1} - t_2 y^{p-1} &\equiv -u_3 z^{p-1} \pmod{\theta_{l1}} \\ -s_3 x^{p-1} + t_1 y^{p-1} &\equiv u_2 z^{p-1} \pmod{\theta_{l1}} \\ -s_2 x^{p-1} + t_3 y^{p-1} &\equiv u_1 z^{p-1} \pmod{\theta_{l1}} \end{aligned}$$

mod θ_{l1} として

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

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

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

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

【General solution conditions】

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

1.4.2 Common to $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_{r_1}}$

(9) より

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\delta} \\
 &\Leftrightarrow \\
 x^p - yx^{p-1} &\equiv -zx^{p-1} \pmod{\theta_{l_1}} \\
 x^p + zx^{p-1} &\equiv yx^{p-1} \pmod{\theta_{r_1}} \\
 -yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \pmod{\delta} \\
 (x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta} \tag{10}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\delta} \\
 &\Leftrightarrow \\
 -xy^{p-1} + y^p &\equiv zy^{p-1} \pmod{\theta_{l_1}} \\
 -zy^{p-1} + y^p &\equiv xy^{p-1} \pmod{\theta_{r_1}} \\
 -xy^{p-1} \cdot zy^{p-1} &\equiv x^p z^p \pmod{\delta} \\
 (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \tag{11}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\delta} \\
 &\Leftrightarrow \\
 -xz^{p-1} + yz^{p-1} &\equiv z^p \pmod{\theta_{l_1}} \\
 yz^{p-1} - xz^{p-1} &\equiv z^p \pmod{\theta_{r_1}} \\
 -xz^{p-1} \cdot yz^{p-1} &\equiv x^p y^p \pmod{\delta} \\
 (z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \tag{12}
 \end{aligned}$$

(10)(11)(12) より

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

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

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

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

$$x^p + y^p \equiv z^p \pmod{3}$$

$$x \cdot x^{2n} + y \cdot y^{2n} \equiv z \cdot z^{2n} \pmod{3}$$

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

$$x + y \equiv z \pmod{3}$$

$$x \equiv \pm 1 \pmod{3}$$

$$y \equiv \pm 1 \pmod{3}$$

$$z \equiv \mp 1 \pmod{3}$$

$$\delta \neq 3$$

$$A^3 - B^3 = (A - B)(3AB + (A - B)^2)$$

$$A^3 + B^3 = (A + B)(-3AB + (A + B)^2)$$

$\delta \perp 3AB$ なので

2つの因数のうち、一方は δ と互いに素である。 (13)

$$\delta \mid (A - B) \quad \Rightarrow \delta \perp (3AB + (A - B)^2)$$

$$\delta \mid (3AB + (A - B)^2) \quad \Rightarrow \delta \perp (A - B)$$

【Equivalence transformation】

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

$$x^p + y^p \equiv z^p \pmod{\theta_{l_1}}$$

$$-xz^{p-1} - yx^{p-1} \equiv zy^{p-1} \pmod{\theta_{l_1}}$$

$$-xy^{p-1} + yz^{p-1} \equiv -zx^{p-1} \pmod{\theta_{l_1}}$$

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

$$x^p + y^p \equiv z^p \pmod{\theta_{r_1}}$$

$$yz^{p-1} + zx^{p-1} \equiv xy^{p-1} \pmod{\theta_{r_1}}$$

$$-zy^{p-1} - xz^{p-1} \equiv yx^{p-1} \pmod{\theta_{r_1}}$$

1.4.3 $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_{r_1}}$

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

s'', t'', u'' を変数とおく。

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

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

1.4.4 $-y \equiv z \equiv x \pmod{\theta_{l_2}}$ のとき

$$\begin{aligned}s_1''x + t_1''y &\equiv u_1''z \pmod{\theta_{l_2}} \\ s_2''x - t_2''y &\equiv -u_2''z \pmod{\theta_{l_2}} \\ -s_3''x - t_3''y &\equiv u_3''z \pmod{\theta_{l_2}}\end{aligned}$$

$\pmod{\theta_{l_2}}$ として

$$\begin{aligned}s_1'' &\equiv x^{p-1} \quad , \quad t_1'' \equiv y^{p-1} \quad , \quad u_1'' \equiv z^{p-1} \\ s_2'' &\equiv x^{p-1} \quad , \quad t_2'' \equiv -y^{p-1} \quad , \quad u_2'' \equiv -z^{p-1} \\ s_3'' &\equiv -x^{p-1} \quad , \quad t_3'' \equiv -y^{p-1} \quad , \quad u_3'' \equiv z^{p-1} \\ [x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_{r_1}}]\end{aligned}$$

【General solution conditions】

$$\begin{aligned}x^p - y^{p-1}x &\equiv z^{p-1}x \pmod{\theta_{l_2}} \\ -x^{p-1}y + y^p &\equiv -z^{p-1}y \pmod{\theta_{l_2}} \\ x^{p-1}z - y^{p-1}z &\equiv z^p \pmod{\theta_{l_2}}\end{aligned} \tag{14}$$

1.4.5 Common to $-y \not\equiv z \not\equiv x \pmod{\theta_{r_2}}$

(14) より

$$\begin{aligned} -xy^{p-1} \cdot xz^{p-1} &\equiv y^p z^p \pmod{\theta_{r_1}} \\ -x^2 &\equiv yz \pmod{\theta_{r_1}} \\ x^2 &\equiv -yz \pmod{\theta_{r_1}} \end{aligned} \quad (15)$$

$$\begin{aligned} (10) \text{ より } (x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\theta_{r_1}} \\ (x^2)^{p-1} &\equiv y^{p-1} z^{p-1} \pmod{\theta_{r_1}} \\ (-yz)^{p-1} &\equiv y^{p-1} z^{p-1} \pmod{\theta_{r_1}} \\ y^{p-1} z^{p-1} &\equiv y^{p-1} z^{p-1} \pmod{\theta_{r_1}} \end{aligned}$$

$$\begin{aligned} -yx^{p-1} \cdot -yz^{p-1} &\equiv x^p z^p \pmod{\theta_{r_1}} \\ y^2 &\equiv xz \pmod{\theta_{r_1}} \end{aligned} \quad (16)$$

$$\begin{aligned} (11) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\theta_{r_1}} \\ (y^2)^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\theta_{r_1}} \\ (xz)^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\theta_{r_1}} \\ x^{p-1} z^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\theta_{r_1}} \end{aligned}$$

δ の定義に反する。

$$\begin{aligned} zx^{p-1} \cdot -zy^{p-1} &\equiv x^p y^p \pmod{\theta_{r_1}} \\ -z^2 &\equiv xy \pmod{\theta_{r_1}} \\ z^2 &\equiv -xy \pmod{\theta_{r_1}} \end{aligned} \quad (17)$$

$$\begin{aligned} (12) \text{ より } (z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\theta_{r_1}} \\ (z^2)^{p-1} &\equiv -x^{p-1} y^{p-1} \pmod{\theta_{r_1}} \\ (-xy)^{p-1} &\equiv -x^{p-1} y^{p-1} \pmod{\theta_{r_1}} \\ x^{p-1} y^{p-1} &\equiv -x^{p-1} y^{p-1} \pmod{\theta_{r_1}} \end{aligned}$$

δ の定義に反するので $\theta_{r_1} \neq \delta$

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

よって $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\delta}$ のとき
 $-y \equiv z \equiv x \pmod{\delta}$ or $-y \not\equiv z \not\equiv x \pmod{\delta}$ は成り立たないので $\theta_{l_1} = \delta$

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

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

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

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

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

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

$$s'_1 x^{p-2} + t'_1 y^{p-2} \equiv u'_1 z^{p-2} \pmod{\theta_{L1}}$$

$$s'_2 x^{p-2} + t'_2 y^{p-2} \equiv u'_2 z^{p-2} \pmod{\theta_{L1}}$$

$$s'_3 x^{p-2} + t'_3 y^{p-2} \equiv u'_3 z^{p-2} \pmod{\theta_{L1}}$$

$\pmod{\theta_{L1}}$ として

$$s'_1 \equiv x^2, \quad t'_1 \equiv y^2, \quad u'_1 \equiv z^2$$

$$s'_2 \equiv x^2, \quad t'_2 \equiv y^2, \quad u'_2 \equiv z^2$$

$$s'_3 \equiv x^2, \quad t'_3 \equiv y^2, \quad u'_3 \equiv z^2$$

$$[x^2 + y^2 - z^2 \equiv 0 \pmod{\theta_0}]$$

【General solution conditions】

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

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

(18) より

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_0} \\
 &\Leftrightarrow \\
 x^p + y^2 x^{p-2} &\equiv z^2 x^{p-2} \pmod{\theta_{L1}} \\
 x^p - z^2 x^{p-2} &\equiv -y^2 x^{p-2} \pmod{\theta_{R1}} \\
 \\
 y^2 x^{p-2} \cdot z^2 x^{p-2} &\equiv y^p z^p \pmod{\theta_0} \\
 (x^{p-2})^2 &\equiv y^{p-2} z^{p-2} \pmod{\theta_0} \tag{19}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_0} \\
 &\Leftrightarrow \\
 x^2 y^{p-2} + y^p &\equiv z^2 y^{p-2} \pmod{\theta_{L1}} \\
 -z^2 y^{p-2} + y^p &\equiv -x^2 y^{p-2} \pmod{\theta_{R1}} \\
 \\
 x^2 y^{p-2} \cdot z^2 y^{p-2} &\equiv x^p z^p \pmod{\theta_0} \\
 (y^{p-2})^2 &\equiv x^{p-2} z^{p-2} \pmod{\theta_0} \tag{20}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_0} \\
 &\Leftrightarrow \\
 x^2 z^{p-2} + y^2 z^{p-2} &\equiv z^p \pmod{\theta_{L1}} \\
 y^2 z^{p-2} + x^2 z^{p-2} &\equiv z^p \pmod{\theta_{R1}} \\
 \\
 x^2 z^{p-2} \cdot y^2 z^{p-2} &\equiv x^p y^p \pmod{\theta_0} \\
 (z^{p-2})^2 &\equiv x^{p-2} y^{p-2} \pmod{\theta_0} \tag{21}
 \end{aligned}$$

(19)(20)(21) より

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

$$(z^{p-2})^3 - (y^{p-2})^3 \equiv (z^{p-2} - y^{p-2})((z^{p-2})^2 + y^{p-2}z^{p-2} + (y^{p-2})^2) \equiv 0 \pmod{\theta_0}$$

$$(x^{p-2})^3 - (z^{p-2})^3 \equiv (x^{p-2} - z^{p-2})((x^{p-2})^2 + x^{p-2}z^{p-2} + (z^{p-2})^2) \equiv 0 \pmod{\theta_0}$$

$$(x^{p-2})^3 - (y^{p-2})^3 \equiv (x^{p-2} - y^{p-2})((x^{p-2})^2 + x^{p-2}y^{p-2} + (y^{p-2})^2) \equiv 0 \pmod{\theta_0}$$

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

$$(x^{p-2})^2 + (z^{p-2})^2 + (y^{p-2})^2 \equiv 0 \pmod{\theta_{R1}}$$

$$(x^{p-2})^2 + x^{p-2}y^{p-2} + x^{p-2}z^{p-2} \equiv 0 \pmod{\theta_{R1}}$$

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

$$x^{p-2} + y^{p-2} \equiv -z^{p-2} \pmod{\theta_{R1}}$$

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。

$$s_1''x^2 + t_1''y^2 \equiv u_1''z^2 \pmod{\theta}$$

$$s_2''z^2 + t_2''x^2 \equiv u_2''y^2 \pmod{\theta}$$

$$s_3''y^2 + t_3''z^2 \equiv u_3''x^2 \pmod{\theta}$$

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

$$s_1''x^2 + t_1''y^2 \equiv u_1''z^2 \pmod{\theta_{L2}}$$

$$-s_2''x^2 + t_2''y^2 \equiv -u_2''z^2 \pmod{\theta_{L2}}$$

$$s_3''x^2 - t_3''y^2 \equiv -u_3''z^2 \pmod{\theta_{L2}}$$

$\pmod{\theta_{L2}}$ として

$$s_1'' \equiv x^{p-2}, \quad t_1'' \equiv y^{p-2}, \quad u_1'' \equiv z^{p-2}$$

$$s_2'' \equiv -x^{p-2}, \quad t_2'' \equiv y^{p-2}, \quad u_2'' \equiv -z^{p-2}$$

$$s_3'' \equiv x^{p-2}, \quad t_3'' \equiv -y^{p-2}, \quad u_3'' \equiv -z^{p-2}$$

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

【General solution conditions】

$$\begin{aligned} x^p + x^2y^{p-2} &\equiv -x^2z^{p-2} \pmod{\theta_{L2}} \\ y^2x^{p-2} + y^p &\equiv -y^2z^{p-2} \pmod{\theta_{L2}} \\ -z^2x^{p-2} - z^2y^{p-2} &\equiv z^p \pmod{\theta_{L2}} \end{aligned} \quad (22)$$

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

(22) より

$$\begin{aligned} x^2 y^{p-2} \cdot -x^2 z^{p-2} &\equiv y^p z^p \pmod{\theta_0} \\ x^4 &\equiv -y^2 z^2 \pmod{\theta_0} \end{aligned} \quad (23)$$

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

これは δ の定義に反する。

.....

$$\begin{aligned} y^2 x^{p-2} \cdot -y^2 z^{p-2} &\equiv x^p z^p \pmod{\theta_0} \\ y^4 &\equiv -x^2 z^2 \pmod{\theta_0} \end{aligned} \quad (24)$$

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

これは δ の定義に反する。

.....

$$\begin{aligned} -z^2 x^{p-2} \cdot -z^2 y^{p-2} &\equiv x^p y^p \pmod{\theta_0} \\ z^4 &\equiv x^2 y^2 \pmod{\theta_0} \end{aligned} \quad (25)$$

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

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

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

また

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

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

1.4.11 $-z^2 \equiv x^2 \equiv y^2 \pmod{\delta}$ or $-z^2 \not\equiv x^2 \not\equiv y^2 \pmod{\delta}$ のとき

(23)(24)(25) より

$$x^6 \equiv y^6 \equiv -z^6 \pmod{\delta}$$

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

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

が成り立つならば、 $\theta_{R1} = \theta_{R2}$

(23)(24)(25) より

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

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

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

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

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

$x^2 + z^2 \equiv 0 \pmod{\delta}$ のとき

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

$z^2 + y^2 \equiv 0 \pmod{\delta}$ のとき

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

これは δ の定義を満たすが、 $x^2 - y^2 \not\equiv 0 \pmod{\delta}$ に反するので $\delta \neq \theta_{L2}$

以上より

$$\delta \neq odd$$

1.5 $\delta = 2$

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

$S = 2^k$ のとき

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

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

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

$$2 \mid a$$

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

$$2 \perp \alpha$$

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

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

$$2^0 = 1$$

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

$S' = 2^k$ のとき

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

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

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

$$2 \mid a'$$

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

$$2 \perp \alpha'$$

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

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

$$2^0 = 1$$

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

よって $2 \mid x$ のとき成り立たない。

1.6 $\delta' \perp xyz$

1.6.1 $p \mid z$

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

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

Proof 13

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

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

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

$$\delta' \perp z$$

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

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

$$\delta' \perp ab$$

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

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

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

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

よって

$$\delta' \perp \beta$$

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

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

よって

$$\delta' \perp \alpha$$

□

$x + y \equiv -z \pmod{\delta'}$ より

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

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

なので

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

よって

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

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

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

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

1.6.2 同値変換 (Equivalence transformation)

【Equivalence transformation】

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

1.6.3 $-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \pmod{\theta'_{11}}$ のとき

$$\begin{aligned} s_1x^{p-1} + t_2y^{p-1} &\equiv -u_3z^{p-1} \pmod{\theta'_{11}} \\ s_3x^{p-1} + t_1y^{p-1} &\equiv -u_2z^{p-1} \pmod{\theta'_{11}} \\ -s_2x^{p-1} - t_3y^{p-1} &\equiv u_1z^{p-1} \pmod{\theta'_{11}} \end{aligned}$$

$\pmod{\theta'_{11}}$ として

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

【General solution conditions】

$$\begin{aligned} x^p + yx^{p-1} &\equiv -zx^{p-1} \pmod{\theta'_{11}} \\ xy^{p-1} + y^p &\equiv -zy^{p-1} \pmod{\theta'_{11}} \\ -xz^{p-1} - yz^{p-1} &\equiv z^p \pmod{\theta'_{11}} \end{aligned} \tag{26}$$

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

(26) より

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

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

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

(27)(28)(29) より

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

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

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

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

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

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

(13) と同様

2つの因数のうち、一方は δ' と互いに素である。 (30)

【Equivalence transformation】

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

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

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

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

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

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

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

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

$$1.6.6 \quad z \equiv x \equiv y \pmod{\theta'_{l2}} \text{ のとき}$$

$$\begin{aligned} s''_1x + t''_1y &\equiv u''_1z \pmod{\theta'_{l2}} \\ s''_2x + t''_2y &\equiv u''_2z \pmod{\theta'_{l2}} \\ s''_3x + t''_3y &\equiv u''_3z \pmod{\theta'_{l2}} \end{aligned}$$

$\pmod{\theta'_{l2}}$ として

$$\begin{aligned} s''_1 &\equiv x^{p-1}, \quad t''_1 \equiv y^{p-1}, \quad u''_1 \equiv z^{p-1} \\ s''_2 &\equiv x^{p-1}, \quad t''_2 \equiv y^{p-1}, \quad u''_2 \equiv z^{p-1} \\ s''_3 &\equiv x^{p-1}, \quad t''_3 \equiv y^{p-1}, \quad u''_3 \equiv z^{p-1} \\ [x^{p-1} + y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta'_{r1}}] \end{aligned}$$

【General solution conditions】

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

1.6.7 Common to $z \not\equiv x \not\equiv y \pmod{\theta'_{r_2}}$

(31) より

$$\begin{aligned} xy^{p-1} \cdot xz^{p-1} &\equiv y^p z^p \pmod{\theta'_{r_1}} \\ x^2 &\equiv yz \pmod{\theta'_{r_1}} \end{aligned} \quad (32)$$

$$(27) \text{ より } (x^{p-1})^2 \equiv -y^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

$$(x^2)^{p-1} \equiv -y^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

$$(32) \text{ より } (yz)^{p-1} \equiv -y^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

$$y^{p-1} z^{p-1} \equiv -y^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

δ' の定義に反する。

$$\begin{aligned} yx^{p-1} \cdot yz^{p-1} &\equiv x^p z^p \pmod{\theta'_{r_1}} \\ y^2 &\equiv xz \pmod{\theta'_{r_1}} \end{aligned} \quad (33)$$

$$(28) \text{ より } (y^{p-1})^2 \equiv -x^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

$$(y^2)^{p-1} \equiv -x^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

$$(33) \text{ より } (xz)^{p-1} \equiv -x^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

$$x^{p-1} z^{p-1} \equiv -x^{p-1} z^{p-1} \pmod{\theta'_{r_1}}$$

δ' の定義に反する。

$$\begin{aligned} zx^{p-1} \cdot zy^{p-1} &\equiv x^p y^p \pmod{\theta'_{r_1}} \\ z^2 &\equiv xy \pmod{\theta'_{r_1}} \end{aligned} \quad (34)$$

$$(29) \text{ より } (z^{p-1})^2 \equiv x^{p-1} y^{p-1} \pmod{\theta'_{r_1}}$$

$$(z^2)^{p-1} \equiv x^{p-1} y^{p-1} \pmod{\theta'_{r_1}}$$

$$(34) \text{ より } (xy)^{p-1} \equiv x^{p-1} y^{p-1} \pmod{\theta'_{r_1}}$$

$$x^{p-1} y^{p-1} \equiv x^{p-1} y^{p-1} \pmod{\theta'_{r_1}}$$

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

よって $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\delta'}$ のとき

$z \equiv x \equiv y \pmod{\delta'}$ or $z \not\equiv x \not\equiv y \pmod{\delta'}$ は成り立たないので $\theta'_{11} = \delta'$

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

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

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

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

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

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

$$s'_1 x^{p-2} + t'_1 y^{p-2} \equiv u'_1 z^{p-2} \pmod{\theta'_{L1}}$$

$$s'_2 x^{p-2} - t'_2 y^{p-2} \equiv -u'_2 z^{p-2} \pmod{\theta'_{L1}}$$

$$-s'_3 x^{p-2} - t'_3 y^{p-2} \equiv u'_3 z^{p-2} \pmod{\theta'_{L1}}$$

$\pmod{\theta'_{L1}}$ として

$$s'_1 \equiv x^2, \quad t'_1 \equiv y^2, \quad u'_1 \equiv z^2$$

$$s'_2 \equiv x^2, \quad t'_2 \equiv -y^2, \quad u'_2 \equiv -z^2$$

$$s'_3 \equiv -x^2, \quad t'_3 \equiv -y^2, \quad u'_3 \equiv z^2$$

$$[x^2 - y^2 - z^2 \equiv 0 \pmod{\theta'_0}]$$

【General solution conditions】

$$\begin{aligned} x^p - y^2 x^{p-2} &\equiv z^2 x^{p-2} \pmod{\theta'_{L1}} \\ -x^2 y^{p-2} + y^p &\equiv -z^2 y^{p-2} \pmod{\theta'_{L1}} \\ x^2 z^{p-2} - y^2 z^{p-2} &\equiv z^p \pmod{\theta'_{L1}} \end{aligned} \quad (35)$$

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

(35) より

$$\begin{aligned}
x^p + y^p &\equiv z^p \pmod{\theta'_0} \\
&\Leftrightarrow \\
x^p - y^2 x^{p-2} &\equiv z^2 x^{p-2} \pmod{\theta'_{L1}} \\
x^p - z^2 x^{p-2} &\equiv y^2 x^{p-2} \pmod{\theta'_{R1}} \\
-y^2 x^{p-2} \cdot z^2 x^{p-2} &\equiv y^p z^p \pmod{\theta'_0} \\
(x^{p-2})^2 &\equiv -y^{p-2} z^{p-2} \pmod{\theta'_0} \tag{36}
\end{aligned}$$

$$\begin{aligned}
x^p + y^p &\equiv z^p \pmod{\theta'_0} \\
&\Leftrightarrow \\
-x^2 y^{p-2} + y^p &\equiv -z^2 y^{p-2} \pmod{\theta'_{L1}} \\
z^2 y^{p-2} + y^p &\equiv x^2 y^{p-2} \pmod{\theta'_{R1}} \\
-x^2 y^{p-2} \cdot -z^2 y^{p-2} &\equiv x^p z^p \pmod{\theta'_0} \\
(y^{p-2})^2 &\equiv x^{p-2} z^{p-2} \pmod{\theta'_0} \tag{37}
\end{aligned}$$

$$\begin{aligned}
x^p + y^p &\equiv z^p \pmod{\theta'_0} \\
&\Leftrightarrow \\
x^2 z^{p-2} - y^2 z^{p-2} &\equiv z^p \pmod{\theta'_{L1}} \\
-y^2 z^{p-2} + x^2 z^{p-2} &\equiv z^p \pmod{\theta'_{R1}} \\
x^2 z^{p-2} \cdot -y^2 z^{p-2} &\equiv x^p y^p \pmod{\theta'_0} \\
(z^{p-2})^2 &\equiv -x^{p-2} y^{p-2} \pmod{\theta'_0} \tag{38}
\end{aligned}$$

(36)(37)(38) より

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

$$(z^{p-2})^3 + (y^{p-2})^3 \equiv (z^{p-2} + y^{p-2})((z^{p-2})^2 - y^{p-2}z^{p-2} + (y^{p-2})^2) \equiv 0 \pmod{\theta'_0}$$

$$(x^{p-2})^3 - (z^{p-2})^3 \equiv (x^{p-2} - z^{p-2})((x^{p-2})^2 + x^{p-2}z^{p-2} + (z^{p-2})^2) \equiv 0 \pmod{\theta'_0}$$

$$(x^{p-2})^3 + (y^{p-2})^3 \equiv (x^{p-2} + y^{p-2})((x^{p-2})^2 - x^{p-2}y^{p-2} + (y^{p-2})^2) \equiv 0 \pmod{\theta'_0}$$

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

$$(x^{p-2})^2 + (z^{p-2})^2 + (y^{p-2})^2 \equiv 0 \pmod{\theta'_{R1}}$$

$$(x^{p-2})^2 - x^{p-2}y^{p-2} + x^{p-2}z^{p-2} \equiv 0 \pmod{\theta'_{R1}}$$

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

$$x^{p-2} - y^{p-2} \equiv -z^{p-2} \pmod{\theta'_{R1}}$$

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。

$$s''_1x^2 + t''_1y^2 \equiv u''_1z^2 \pmod{\theta'}$$

$$s''_2z^2 + t''_2x^2 \equiv u''_2y^2 \pmod{\theta'}$$

$$s''_3y^2 + t''_3z^2 \equiv u''_3x^2 \pmod{\theta'}$$

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

$$s''_1x^2 + t''_1y^2 \equiv u''_1z^2 \pmod{\theta'_{L2}}$$

$$-s''_2x^2 - t''_2y^2 \equiv u''_2z^2 \pmod{\theta'_{L2}}$$

$$-s''_3x^2 + t''_3y^2 \equiv -u''_3z^2 \pmod{\theta'_{L2}}$$

$\pmod{\theta'_{L2}}$ として

$$s''_1 \equiv x^{p-2}, \quad t''_1 \equiv y^{p-2}, \quad u''_1 \equiv z^{p-2}$$

$$s''_2 \equiv -x^{p-2}, \quad t''_2 \equiv -y^{p-2}, \quad u''_2 \equiv z^{p-2}$$

$$s''_3 \equiv -x^{p-2}, \quad t''_3 \equiv y^{p-2}, \quad u''_3 \equiv -z^{p-2}$$

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

【General solution conditions】

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

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

(39) より

$$\begin{aligned} -x^2 y^{p-2} \cdot -x^2 z^{p-2} &\equiv y^p z^p \pmod{\theta'_0} \\ x^4 &\equiv y^2 z^2 \pmod{\theta'_0} \end{aligned} \quad (40)$$

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

.....

$$\begin{aligned} -y^2 x^{p-2} \cdot y^2 z^{p-2} &\equiv x^p z^p \pmod{\theta'_0} \\ y^4 &\equiv -x^2 z^2 \pmod{\theta'_0} \end{aligned} \quad (41)$$

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

これは δ' の定義に反する。

.....

$$\begin{aligned} -z^2 x^{p-2} \cdot z^2 y^{p-2} &\equiv x^p y^p \pmod{\theta'_0} \\ z^4 &\equiv -x^2 y^2 \pmod{\theta'_0} \end{aligned} \quad (42)$$

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

これは δ' の定義に反する。

$-z^{p-1} \equiv x^{p-1} \pmod{\delta'}$, $-y^{p-1} \equiv z^{p-1} \pmod{\delta'}$, $y^{p-1} \equiv x^{p-1} \pmod{\delta'}$
 のとき (8) の δ 同様であるのと , $-z \not\equiv x \pmod{\delta'}$ より

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

また

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

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

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

(40)(41)(42) より

$$-x^6 \equiv y^6 \equiv z^6 \pmod{\delta'}$$

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

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

が成り立つならば、 $\theta'_{R1} = \theta'_{R2}$

(40)(41)(42) より

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

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

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

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

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

$x^2 + z^2 \equiv 0 \pmod{\delta'}$ のとき

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

$x^2 + y^2 \equiv 0 \pmod{\delta'}$ のとき

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

これは δ' の定義を満たすが、 $z^2 - y^2 \not\equiv 0 \pmod{\delta'}$ に反するので $\delta' \neq \theta'_{L_2}$

以上より

$$\delta' \neq \text{odd}$$

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

$S^n = 2^k$ のとき

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

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

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

$$2 \mid c$$

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

$$2 \nmid \gamma$$

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

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

$$2^0 = 1$$

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

よって $2 \mid z$ のとき成り立たない。

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

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

1.7 補足 1(supplement 1)

$$\begin{aligned} -y &\equiv z \equiv x \pmod{\theta_{l_2}} \\ [x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_{r_1}}] \end{aligned}$$

【General solution conditions】

$$\begin{aligned} x^p - y^{p-1}x &\equiv z^{p-1}x \pmod{\theta_{l_2}} \\ -x^{p-1}y + y^p &\equiv -z^{p-1}y \pmod{\theta_{l_2}} \\ x^{p-1}z - y^{p-1}z &\equiv z^p \pmod{\theta_{l_2}} \end{aligned}$$

Common to $-y \not\equiv z \not\equiv x \pmod{\theta_{r_2}}$

$$\begin{aligned} -y^{p-1}x \cdot z^{p-1}x &\equiv y^p z^p \pmod{\theta_{r_1}} \\ x^2 &\equiv -yz \pmod{\theta_{r_1}} \end{aligned} \quad (43)$$

$$\begin{aligned} -x^{p-1}y \cdot -z^{p-1}y &\equiv x^p z^p \pmod{\theta_{r_1}} \\ y^2 &\equiv xz \pmod{\theta_{r_1}} \end{aligned} \quad (44)$$

$$\begin{aligned} x^{p-1}z \cdot -y^{p-1}z &\equiv x^p y^p \pmod{\theta_{r_1}} \\ z^2 &\equiv -xy \pmod{\theta_{r_1}} \end{aligned} \quad (45)$$

(43)(44)(45) より

$$-y^3 \equiv z^3 \equiv x^3 \pmod{\theta_{r_1}}$$

$$\begin{aligned} z^3 + y^3 &\equiv (z+y)(z^2 - yz + y^2) \equiv 0 \pmod{\theta_{r_1}} \\ x^3 - z^3 &\equiv (x-z)(x^2 + xz + z^2) \equiv 0 \pmod{\theta_{r_1}} \\ x^3 + y^3 &\equiv (x+y)(x^2 - xy + y^2) \equiv 0 \pmod{\theta_{r_1}} \end{aligned}$$

(45) より

$$\begin{aligned} x^2 + xz + z^2 &\equiv 0 \pmod{\theta_{r_1}} \\ x^2 + xz - xy &\equiv 0 \pmod{\theta_{r_1}} \\ x + z - y &\equiv 0 \pmod{\theta_{r_1}} \end{aligned}$$

1.7.1 $x^p + y^p \equiv z^p \pmod{\theta}$ が成り立つ可能性のある条件

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

$$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_{l1}}$$

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

$$\theta_{l1} = \delta$$

$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_{r1}} \quad \wedge \quad -y \equiv z \equiv x \pmod{\theta_{l2}}$ のとき

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

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

$$\theta_{r1} = \theta_{l2}$$

$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_{r1}} \quad \wedge \quad -y \not\equiv z \not\equiv x \pmod{\theta_{r2}}$ のとき

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

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

$$\delta = \theta_{r1}$$

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

【Equivalence transformation】

$$\begin{array}{rcl} x^p & +y^p & \not\equiv z^p \pmod{\theta_{r2}} \\ -y^{p-1}z & -z^{p-1}x & \not\equiv x^{p-1}y \pmod{\theta_{r2}} \\ z^{p-1}y & +x^{p-1}z & \not\equiv y^{p-1}x \pmod{\theta_{r2}} \end{array}$$

1.8 補足 2(supplement 2)

s', t', u' を変数とおく。

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

【Equivalence transformation】

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

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

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

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

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

$\pmod{\Theta_{L1}}$ として

$$\begin{aligned} s'_1 &\equiv x^2, & t'_1 &\equiv y^2, & u'_1 &\equiv z^2 \\ s'_2 &\equiv -x^2, & t'_2 &\equiv y^2, & u'_2 &\equiv -z^2 \\ s'_3 &\equiv x^2, & t'_3 &\equiv -y^2, & u'_3 &\equiv -z^2 \\ [x^2 + y^2 + z^2 &\equiv 0 \pmod{\Theta_0}] \end{aligned}$$

【General solution conditions】

$$\begin{aligned} x^p + y^2 x^{p-2} &\equiv -z^2 x^{p-2} \pmod{\Theta_{L1}} \\ x^2 y^{p-2} + y^p &\equiv -z^2 y^{p-2} \pmod{\Theta_{L1}} \\ -x^2 z^{p-2} - y^2 z^{p-2} &\equiv z^p \pmod{\Theta_{L1}} \end{aligned} \tag{46}$$

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

(46) より

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\Theta_0} \\
 &\Leftrightarrow \\
 x^p + y^2 x^{p-2} &\equiv -z^2 x^{p-2} \pmod{\Theta_{L1}} \\
 x^p + z^2 x^{p-2} &\equiv -y^2 x^{p-2} \pmod{\Theta_{R1}} \\
 \\
 y^2 x^{p-2} \cdot -z^2 x^{p-2} &\equiv y^p z^p \pmod{\Theta_0} \\
 (x^{p-2})^2 &\equiv -y^{p-2} z^{p-2} \pmod{\Theta_0} \tag{47}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\Theta_0} \\
 &\Leftrightarrow \\
 x^2 y^{p-2} + y^p &\equiv -z^2 y^{p-2} \pmod{\Theta_{L1}} \\
 z^2 y^{p-2} + y^p &\equiv -x^2 y^{p-2} \pmod{\Theta_{R1}} \\
 \\
 x^2 y^{p-2} \cdot -z^2 y^{p-2} &\equiv x^p z^p \pmod{\Theta_0} \\
 (y^{p-2})^2 &\equiv -x^{p-2} z^{p-2} \pmod{\Theta_0} \tag{48}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\Theta_0} \\
 &\Leftrightarrow \\
 -x^2 z^{p-2} - y^2 z^{p-2} &\equiv z^p \pmod{\Theta_{L1}} \\
 -y^2 z^{p-2} - x^2 z^{p-2} &\equiv z^p \pmod{\Theta_{R1}} \\
 \\
 -x^2 z^{p-2} \cdot -y^2 z^{p-2} &\equiv x^p y^p \pmod{\Theta_0} \\
 (z^{p-2})^2 &\equiv x^{p-2} y^{p-2} \pmod{\Theta_0} \tag{49}
 \end{aligned}$$

(47)(48)(49) より

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

$$(z^{p-2})^3 + (y^{p-2})^3 \equiv (z^{p-2} + y^{p-2})((z^{p-2})^2 - y^{p-2}z^{p-2} + (y^{p-2})^2) \equiv 0 \pmod{\Theta_0}$$

$$(x^{p-2})^3 + (z^{p-2})^3 \equiv (x^{p-2} + z^{p-2})((x^{p-2})^2 - x^{p-2}z^{p-2} + (z^{p-2})^2) \equiv 0 \pmod{\Theta_0}$$

$$(x^{p-2})^3 - (y^{p-2})^3 \equiv (x^{p-2} - y^{p-2})((x^{p-2})^2 + x^{p-2}y^{p-2} + (y^{p-2})^2) \equiv 0 \pmod{\Theta_0}$$

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

$$(x^{p-2})^2 + (z^{p-2})^2 + (y^{p-2})^2 \equiv 0 \pmod{\Theta_{R1}}$$

$$(x^{p-2})^2 + x^{p-2}y^{p-2} - x^{p-2}z^{p-2} \equiv 0 \pmod{\Theta_{R1}}$$

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

$$x^{p-2} + y^{p-2} \equiv z^{p-2} \pmod{\Theta_{R1}}$$

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。

$$s_1''x^2 + t_1''y^2 \equiv u_1''z^2 \pmod{\Theta}$$

$$s_2''z^2 + t_2''x^2 \equiv u_2''y^2 \pmod{\Theta}$$

$$s_3''y^2 + t_3''z^2 \equiv u_3''x^2 \pmod{\Theta}$$

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

$$s_1''x^2 + t_1''y^2 \equiv u_1''z^2 \pmod{\Theta_{L2}}$$

$$s_2''x^2 + t_2''y^2 \equiv u_2''z^2 \pmod{\Theta_{L2}}$$

$$s_3''x^2 + t_3''y^2 \equiv u_3''z^2 \pmod{\Theta_{L2}}$$

$\pmod{\Theta_{L2}}$ として

$$s_1'' \equiv x^{p-2}, \quad t_1'' \equiv y^{p-2}, \quad u_1'' \equiv z^{p-2}$$

$$s_2'' \equiv x^{p-2}, \quad t_2'' \equiv y^{p-2}, \quad u_2'' \equiv z^{p-2}$$

$$s_3'' \equiv x^{p-2}, \quad t_3'' \equiv y^{p-2}, \quad u_3'' \equiv z^{p-2}$$

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

【General solution conditions】

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

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

(50) より

$$\begin{aligned} x^2 y^{p-2} \cdot x^2 z^{p-2} &\equiv y^p z^p \pmod{\Theta_0} \\ x^4 &\equiv y^2 z^2 \pmod{\Theta_0} \end{aligned} \quad (51)$$

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

$$\begin{aligned} y^2 x^{p-2} \cdot y^2 z^{p-2} &\equiv x^p z^p \pmod{\Theta_0} \\ y^4 &\equiv x^2 z^2 \pmod{\Theta_0} \end{aligned} \quad (52)$$

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

$$\begin{aligned} z^2 x^{p-2} \cdot z^2 y^{p-2} &\equiv x^p y^p \pmod{\Theta_0} \\ z^4 &\equiv x^2 y^2 \pmod{\Theta_0} \end{aligned} \quad (53)$$

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

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

1.8.6 $x^2 \equiv y^2 \equiv z^2 \pmod{\Theta_0}$ or $x^2 \not\equiv y^2 \not\equiv z^2 \pmod{\Theta_0}$ のとき

(51)(52)(53) より

$$x^6 \equiv y^6 \equiv z^6 \pmod{\Theta_0}$$

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

(51)(52)(53) より

$$x^4 + x^2y^2 + y^4 \equiv x^2 + y^2 + z^2 \pmod{\Theta_0}$$

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

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

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

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

よって、 δ は上記三組の合同式に対する共通の法に該当しない。

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

$$-z \equiv y \pmod{\delta}$$

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