

Solution Conditions

Hajime Mashima

Abstract

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

Contents

1	introduction	1
1.1	$\delta \perp xyz$	2
1.1.1	$p \mid x$	4
1.1.2	$p \perp x$	5
1.2	解の条件 (Solution Conditions)	6
1.3	解の条件 1(Solution Conditions 1)	9
1.3.1	Condition L	9
1.4	解の条件 2(Solution Conditions 2)	11
1.4.1	Condition R	12
1.4.2	Condition L and Condition R	12
1.5	$\delta = 2$	13
1.5.1	$2 \mid x$, $2 \perp yz$	13
1.5.2	$p \mid z$	14
1.5.3	Condition L	15
1.5.4	Condition R	15
1.6	$\delta' = 2$	16
1.6.1	$2 \mid z$, $2 \perp xy$	16

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)

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

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

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

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

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

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

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

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

$p^2 \mid R \Rightarrow p \mid y^{p-1}$ 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 $x + y = c^p$

$$(z - x) - (x + y) = b^p - c^p$$

$$(z - y) - 2x = b^p - c^p \equiv 0 \pmod{p}$$

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

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

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

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

$x^p = (z - y) \cdot p\alpha^p$ 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 $x = p^2a\alpha$ と置けるので

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

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

(4) , $p \perp \alpha^p$ より

$$p^1 \mid K \text{ でなければならぬ。}$$

よって

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

一般的に

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

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

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

□

また

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

1.1.1 $p \mid x$

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

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 $p \perp x$

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

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。

$$\begin{aligned}
 Uz^{p-1} &\equiv y^p \pmod{\theta} \\
 Ty^{p-1} &\equiv z^p \pmod{\theta} \\
 or \\
 Uz^{p-1} &\equiv -z^p \pmod{\theta} \\
 Ty^{p-1} &\equiv -y^p \pmod{\theta}
 \end{aligned} \tag{6}$$

Definition 9 $U = y$, $T = z$ のとき

Condition L

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

or

Condition R

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

(7)

$\theta \perp xyz$ 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。

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

$$\begin{aligned} -U'z^{p-1} + z^p - x^p &\equiv -T'x^{p-1} \pmod{\theta} \\ -U'z^{p-1} + z^p &\equiv x^p - T'x^{p-1} \pmod{\theta} \\ -z^{p-1}(U' - z) &\equiv x^{p-1}(x - T') \pmod{\theta} \\ -z^{p-1}(U'x - xz) &\equiv x \cdot x^{p-1}(x - T') \pmod{\theta} \end{aligned} \tag{8}$$

$x^p z^p \equiv -U'z^{p-1} \cdot -T'x^{p-1} \pmod{\theta}$ 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 (8)、 $xz \equiv U'T' \pmod{\theta}$ を満たすとき解の候補は以下の 2 通りである。

$$\begin{aligned} -U'z^{p-1} &\equiv x^p \pmod{\theta} \\ -T'x^{p-1} &\equiv z^p \pmod{\theta} \\ or \\ -U'z^{p-1} &\equiv -z^p \pmod{\theta} \\ -T'x^{p-1} &\equiv -x^p \pmod{\theta} \end{aligned} \tag{9}$$

Definition 10 $U' = x$, $T' = z$ のとき

Condition L

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

or

Condition R

$$x \equiv z \pmod{\theta_r}$$

(10)

$\theta \perp xyz$ 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。

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

$$\begin{aligned} -U''y^{p-1} - T'''x^{p-1} &\equiv x^p + y^p \pmod{\theta} \\ -x^p - T'''x^{p-1} &\equiv U''y^{p-1} + y^p \pmod{\theta} \\ -x^{p-1}(x + T''') &\equiv y^{p-1}(U'' + y) \pmod{\theta} \\ -x^{p-1}(xy + T'''y) &\equiv y \cdot y^{p-1}(U'' + y) \pmod{\theta} \end{aligned} \quad (11)$$

$x^py^p \equiv -U''y^{p-1} \cdot -T'''x^{p-1} \pmod{\theta}$ 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 (11)、 $xy \equiv U''T''' \pmod{\theta}$ を満たすとき解の候補は以下の 2 通りである。

$$\begin{aligned} -U''y^{p-1} &\equiv x^p \pmod{\theta} \\ -T'''x^{p-1} &\equiv y^p \pmod{\theta} \\ or \\ -U''y^{p-1} &\equiv y^p \pmod{\theta} \\ -T'''x^{p-1} &\equiv x^p \pmod{\theta} \end{aligned} \quad (12)$$

Definition 11 $U'' = x$, $T''' = y$ のとき

Condition L

$$\begin{aligned} -y^{p-1} &\equiv x^{p-1} \pmod{\theta_l} \\ or \end{aligned} \quad (13)$$

Condition R

$$-x \equiv y \pmod{\theta_r}$$

1.3 解の条件 1(Solution Conditions 1)

1.3.1 Condition L

(5),(8),(11) から

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

$$\begin{aligned} z^{p-1} &\equiv y^{p-1} \pmod{\theta_l} \implies y \not\equiv -z \pmod{\theta_l} \\ -z^{p-1} &\equiv x^{p-1} \pmod{\theta_l} \implies x \not\equiv z \pmod{\theta_l} \\ -x^{p-1} &\equiv y^{p-1} \pmod{\theta_l} \implies -x \not\equiv y \pmod{\theta_l} \end{aligned}$$

合同式 (14) を満たすので解の条件を展開できる。

(7),(10),(13) から

$$\begin{aligned} y &\equiv -z \pmod{\theta_r} \implies z^{p-1} \not\equiv y^{p-1} \pmod{\theta_r} \\ x &\equiv z \pmod{\theta_r} \implies -z^{p-1} \not\equiv x^{p-1} \pmod{\theta_r} \\ -x &\equiv y \pmod{\theta_r} \implies -x^{p-1} \not\equiv y^{p-1} \pmod{\theta_r} \end{aligned}$$

もし以下の関係が成り立つと仮定すると

$$\begin{aligned} y &\not\equiv -z \pmod{\theta_r} \implies z^{p-1} \not\equiv y^{p-1} \pmod{\theta_r} \\ x &\not\equiv z \pmod{\theta_r} \implies -z^{p-1} \not\equiv x^{p-1} \pmod{\theta_r} \\ -x &\not\equiv y \pmod{\theta_r} \implies -x^{p-1} \not\equiv y^{p-1} \pmod{\theta_r} \end{aligned}$$

Condition R に相反する条件が存在するので矛盾する。

$$\begin{aligned} y &\equiv -z \pmod{\theta_r} \perp y \not\equiv -z \pmod{\theta_r} \\ x &\equiv z \pmod{\theta_r} \perp x \not\equiv z \pmod{\theta_r} \\ -x &\equiv y \pmod{\theta_r} \perp -x \not\equiv y \pmod{\theta_r} \end{aligned}$$

よって以下の関係が成り立つ。

$$\begin{aligned} z^{p-1} &\equiv y^{p-1} \pmod{\theta_l} \iff y \not\equiv -z \pmod{\theta_l} \\ -z^{p-1} &\equiv x^{p-1} \pmod{\theta_l} \iff x \not\equiv z \pmod{\theta_l} \\ -x^{p-1} &\equiv y^{p-1} \pmod{\theta_l} \iff -x \not\equiv y \pmod{\theta_l} \end{aligned}$$

また他に、もし以下の関係が成り立つと仮定すると

$$\begin{aligned} z^{p-1} &\not\equiv y^{p-1} \pmod{\theta_l} \implies y \not\equiv -z \pmod{\theta_l} \\ -z^{p-1} &\not\equiv x^{p-1} \pmod{\theta_l} \implies x \not\equiv z \pmod{\theta_l} \\ -x^{p-1} &\not\equiv y^{p-1} \pmod{\theta_l} \implies -x \not\equiv y \pmod{\theta_l} \end{aligned}$$

Condition L に相反する条件が存在するので矛盾する。

$$\begin{aligned} z^{p-1} &\equiv y^{p-1} \pmod{\theta_l} \perp z^{p-1} \not\equiv y^{p-1} \pmod{\theta_l} \\ -z^{p-1} &\equiv x^{p-1} \pmod{\theta_l} \perp -z^{p-1} \not\equiv x^{p-1} \pmod{\theta_l} \\ -x^{p-1} &\equiv y^{p-1} \pmod{\theta_l} \perp -x^{p-1} \not\equiv y^{p-1} \pmod{\theta_l} \end{aligned}$$

よって以下の関係が成り立つ。

$$\begin{aligned} y &\equiv -z \pmod{\theta_r} \iff z^{p-1} \not\equiv y^{p-1} \pmod{\theta_r} \\ x &\equiv z \pmod{\theta_r} \iff -z^{p-1} \not\equiv x^{p-1} \pmod{\theta_r} \\ -x &\equiv y \pmod{\theta_r} \iff -x^{p-1} \not\equiv y^{p-1} \pmod{\theta_r} \end{aligned} \quad (15)$$

Proposition 12

Condition L の 3 組 $-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\delta}$ は同時に成り立つ。 (16)

Proof 13 $x - y \equiv -z \pmod{\delta}$ より

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

上式を並び替える。

$$\begin{aligned} x^p - yx^{p-1} &\equiv -zx^{p-1} \pmod{\delta} \\ -xy^{p-1} + y^p &\equiv zy^{p-1} \pmod{\delta} \\ -xz^{p-1} + yz^{p-1} &\equiv z^p \pmod{\delta} \end{aligned} \quad (17)$$

解の条件より

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{\delta} \\ \iff \\ x^p + yz^{p-1} &\equiv zy^{p-1} \pmod{\delta} \\ -xz^{p-1} + y^p &\equiv -zx^{p-1} \pmod{\delta} \\ -xy^{p-1} - yx^{p-1} &\equiv z^p \pmod{\delta} \end{aligned} \quad (18)$$

(18) より $yz^{p-1} \equiv y^p \pmod{\delta} \Rightarrow$ (17) より $-xz^{p-1} \equiv x^p \pmod{\delta} \Rightarrow$
(18) より $-zx^{p-1} \equiv z^p \pmod{\delta} \Rightarrow$ (17) より $-yx^{p-1} \equiv y^p \pmod{\delta} \Rightarrow$
(18) より $-xy^{p-1} \equiv x^p \pmod{\delta} \Rightarrow$ (17) より $zy^{p-1} \equiv z^p \pmod{\delta}$ □

1.4 解の条件 2(Solution Conditions 2)

$\theta \perp xyz$ 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。

$$\begin{aligned} u'z^2 + y^p &\equiv t'x^2 \pmod{\theta} \\ u'z^2 + z^p - x^p &\equiv t'x^2 \pmod{\theta} \\ z^2(u' + z^{p-2}) &\equiv x^2(x^{p-2} + t') \pmod{\theta} \\ z^2(x^{p-2} + z^{p-2}) &\equiv x^2(x^{p-2} + z^{p-2}) \pmod{\theta} \end{aligned}$$

$x^2 \equiv z^2 \pmod{\theta}$, $-z^{p-2} \not\equiv x^{p-2} \pmod{\theta}$ のとき上記合同式を満たすので解の条件 1 と同様に以下の関係が成り立つ。

Definition 14

Condition M

$$x^2 \equiv z^2 \pmod{\theta_m}$$

or

Condition N

$$-z^{p-2} \equiv x^{p-2} \pmod{\theta_n}$$

$$-z^{p-2} \not\equiv x^{p-2} \pmod{\theta_m} \iff x^2 \equiv z^2 \pmod{\theta_m} \quad (19)$$

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

$z \not\equiv x \pmod{\delta}$ より $-z^{p-2} \not\equiv x^{p-2} \pmod{\delta}$ なので (19) より

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

$x+z \equiv y \pmod{\delta}$ より矛盾するので

$$-z^{p-1} \not\equiv x^{p-1} \pmod{\delta}$$

(16) より

$$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\delta} \quad (20)$$

1.4.1 Condition R

$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\delta}$ ならば (15) より

$$\begin{aligned} z + y &\equiv 0 \pmod{\delta} \\ x - z &\equiv 0 \pmod{\delta} \end{aligned} \tag{21}$$

$$x + y \equiv 0 \pmod{\delta} \tag{22}$$

(21),(22) は $\delta \perp yz$ と矛盾する。

また、Condition L と Condition R どちらも成り立たないのは解の条件に反する。

1.4.2 Condition L and Condition R

$\delta \perp yz$ の前提から Condition L と Condition R がともに成り立つ可能性があるのは

Condition L

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

and

Condition R

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

しかし (20) より Condition L の組は全て成り立たないので、Condition R とともに成り立つことはない。よって

$$\delta \neq odd$$

1.5 $\delta = 2$

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

$S = 2^k$ のとき

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

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

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

$$2 \mid a$$

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

$$2 \nmid \alpha$$

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

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

$$2^0 = 1$$

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

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

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

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

$$2 \mid a'$$

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

$$2 \nmid \alpha'$$

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

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

$$2^0 = 1$$

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。

1.5.2 $p \mid z$

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

Proposition 15 $z + x + y = p^n cS''$, $\delta' \mid S'' \Rightarrow \delta' \perp xyz$

Proof 16

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

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

$\delta' \mid S''$, $\delta' \mid c$ 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

$$\delta' \perp \alpha$$

□

1.5.3 Condition L

$x + y \equiv -z \pmod{\delta'}$ より

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

解の条件より

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

(5),(8),(11) と同様に

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

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

$x \not\equiv z \pmod{\delta'}$ より $x^{p-2} \not\equiv -z^{p-2} \pmod{\delta'}$ なので (19) より

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

$x + z \equiv -y \pmod{\delta'}$ より矛盾するので

$$x^{p-1} \not\equiv -z^{p-1} \pmod{\delta'}$$

(16) と同様に

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

1.5.4 Condition R

$x^{p-1} \not\equiv y^{p-1} \not\equiv -z^{p-1} \pmod{\delta'}$ ならば

$$z - y \equiv 0 \pmod{\delta'} \tag{23}$$

$$x - z \equiv 0 \pmod{\delta'} \tag{24}$$

$$x - y \equiv 0 \pmod{\delta'}$$

(23),(24) は $\delta' \mid xy$ と矛盾する。よって

$$\delta' \neq odd$$

1.6 $\delta' = 2$

1.6.1 $2 \mid z$, $2 \perp xy$

$S'' = 2^k$ のとき

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

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

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

$$2 \mid c$$

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

$$2 \perp \gamma$$

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

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

$$2^0 = 1$$

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

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