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
1.2.1 Condition L . . . 9
1.2.2 Condition R . . . 13
1.3 $\delta = 2$ . . . 14
1.3.1 $2 \mid x$, $2 \perp yz$ . . . 14

1 introduction

ある三乗数を二つの三乗数の和で表すこと、あるいはある四乗数を二つの四乗数の和で表すこと、および一般に二乗より大きいべきの数を同じべきの二つの数の和で表すことは不可能である。私はこの命題の真に驚くべき証明を持っているが、余白が狭すぎるのでここに記すことはできない。

1.1 $\delta \perp xyz$

Theorem 1 (Fermat's Last Theorem)

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

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

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

Proof 3

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

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

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

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

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

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

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

また、p を除く素数に関して

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

Definition 4 $p \perp abc$

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

$$(z - x) - (x + y) = b^p - c^p$$
$$(z - y) - 2x = b^p - c^p \equiv 0 \mod p$$

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

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

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

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

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

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

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

(3) より $x = p^2 a\alpha$ と置けるので

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

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

(4) ， $p \perp \alpha^p$ より

$$p^1 \mid K \text{ でなければならない。}$$

よって

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

一般的に

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

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

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

$$p^1 \mid K$$

□

また

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

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

1.1.1 $p \mid x$

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

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

Proof 6

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

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

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

$$\delta \perp x$$

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

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

$$\delta \perp bc$$

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

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

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

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

よって $\delta \perp \beta$

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

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

よって $\delta \perp \gamma$ □

1.1.2 $p \perp x$

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

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

Proof 8

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

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

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

$$\delta \perp x$$

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

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

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

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

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

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

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

よって $\delta \perp \beta'$

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

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

よって $\delta \perp \gamma'$ □

1.2 解の条件 (Solution Conditions)

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

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

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

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

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

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 $yz \equiv UT \mod \theta$ のとき解の候補は以下の 2 通りである。

Definition 9

Condition L

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

or

Condition R

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

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

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

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

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

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

同様に

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

よって $xz \equiv U'T' \mod \theta$ のとき解の候補は以下の 2 通りである。

Definition 10

Condition L

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

or

Condition R

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

$\theta \perp xyz$ 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。

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

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

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

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

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 $xy \equiv U"T" \mod \theta$ のとき解の候補は以下の 2 通りである。

Definition 11

Condition L

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

or

Condition R

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

1.2.1 Condition L

$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \theta$ ならば、解の条件より

$$\begin{aligned} x^p \quad +y^p \equiv \quad & z^p \mod \theta \\ & \Leftrightarrow \\ x^p \quad +yz^{p-1} \quad & \equiv zy^{p-1} \mod \theta \\ -xz^{p-1} \quad +y^p \quad & \equiv -zx^{p-1} \mod \theta \\ -xy^{p-1} \quad -yx^{p-1} \quad & \equiv z^p \mod \theta \end{aligned} \tag{5}$$

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

上式を並び替える。

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

$$-xy^{p-1} + y^p \equiv zy^{p-1} \mod \delta \tag{6}$$

$$-xz^{p-1} + yz^{p-1} \equiv z^p \mod \delta \tag{7}$$

これは (5) の関係式と矛盾しない。

また、$y^{p-1} \equiv z^{p-1} \mod \delta$ ならば (6),(7) より

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

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

が一意的に定まる。よって

Proposition 12

$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \mod \delta$ と $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \delta$ は全ての条件である。

$\delta \perp xyz$ 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。

$$\begin{aligned} x^p + Uz^{p-2} &\equiv Ty^{p-2} \mod \theta \\ z^p - y^p + Uz^{p-2} &\equiv Ty^{p-2} \mod \theta \\ -y^p + Uz^{p-2} &\equiv -z^p + Ty^{p-2} \mod \theta \\ -Ty^p + UTz^{p-2} &\equiv T(-z^p + Ty^{p-2}) \mod \theta \end{aligned}$$

$UT \equiv y^2 z^2 \mod \theta$

$$\begin{aligned} -Ty^p + y^2 z^p &\equiv -T(z^p - Ty^{p-2}) \mod \theta \\ y^2(z^p - Ty^{p-2}) &\equiv -T(z^p - Ty^{p-2}) \mod \theta \\ y^p(z^p - Ty^{p-2}) &\equiv -Ty^{p-2}(z^p - Ty^{p-2}) \mod \theta \end{aligned}$$

同様に

$$\begin{aligned} -y^p + Uz^{p-2} &\equiv -z^p + Ty^{p-2} \mod \theta \\ U(-y^p + Uz^{p-2}) &\equiv -Uz^p + UTy^{p-2} \mod \theta \end{aligned}$$

$UT \equiv y^2 z^2 \mod \theta$

$$\begin{aligned} U(Uz^{p-2} - y^p) &\equiv -Uz^p + z^2 y^p \mod \theta \\ U(Uz^{p-2} - y^p) &\equiv -z^2(Uz^{p-2} - y^p) \mod \theta \\ -Uz^{p-2}(Uz^{p-2} - y^p) &\equiv z^p(Uz^{p-2} - y^p) \mod \theta \end{aligned}$$

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

$z \not\equiv y \mod \delta$ より

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

$T = z^2$, $U = y^2$ とおくと

$$\begin{aligned} z^p - Ty^{p-2} &\not\equiv 0 \mod \delta \\ Uz^{p-2} - y^p &\not\equiv 0 \mod \delta \end{aligned}$$

であるから

$$\begin{aligned} y^p &\equiv -Ty^{p-2} \mod \delta \\ -Uz^{p-2} &\equiv z^p \mod \delta \end{aligned}$$

$$y^2 \equiv -z^2 \mod \delta$$

$\delta \perp xyz$ 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。

$$\begin{aligned} U'z^{p-2}+y^p &\equiv T'x^{p-2} \mod \theta \\ U'z^{p-2}+z^p-x^p &\equiv T'x^{p-2} \mod \theta \\ U'z^{p-2}-x^p &\equiv T'x^{p-2}-z^p \mod \theta \\ U'T'z^{p-2}-T'x^p &\equiv T'(T'x^{p-2}-z^p) \mod \theta \end{aligned}$$

$U'T' \equiv x^2z^2 \mod \theta$

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

同様に

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

$U'T' \equiv x^2z^2 \mod \theta$

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

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

$z \not\equiv -x \mod \delta$ より

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

$U' = x^2$, $T' = z^2$ とおくと

$$\begin{aligned} z^p-T'x^{p-2} &\not\equiv 0 \mod \delta \\ U'z^{p-2}-x^p &\not\equiv 0 \mod \delta \end{aligned}$$

であるから

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

$$x^2 \equiv -z^2 \mod \delta$$

$\delta \perp xyz$ 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。

$$\begin{aligned} U"y^{p-2} + T"x^{p-2} &\equiv z^p \mod \theta \\ U"y^{p-2} + T"x^{p-2} &\equiv x^p + y^p \mod \theta \\ U"y^{p-2} - x^p &\equiv y^p - T"x^{p-2} \mod \theta \\ U"T"y^{p-2} - T"x^p &\equiv T"(y^p - T"x^{p-2}) \mod \theta \end{aligned}$$

$U"T" \equiv x^2y^2 \mod \theta$

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

同様に

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

$U"T" \equiv x^2y^2 \mod \theta$

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

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

$y \not\equiv -x \mod \delta$ より

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

$U" = x^2$, $T" = y^2$ とおくと

$$\begin{aligned} y^p - T"x^{p-2} &\not\equiv 0 \mod \delta \\ U"y^{p-2} - x^p &\not\equiv 0 \mod \delta \end{aligned}$$

であるから

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

$$x^2 \equiv y^2 \mod \delta$$

しかし、$z \not\equiv 0 \mod \delta$ なので

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

これは矛盾する。

1.2.2 Condition R

$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \mod \theta$ ならば、解の条件より

$$\begin{aligned} x^p \quad +y^p \equiv \quad & z^p \mod \theta \\ & \Leftrightarrow \\ x^p \quad -zy^{p-1} \quad & \equiv -yz^{p-1} \mod \theta \\ zx^{p-1} \quad +y^p \quad & \equiv xz^{p-1} \mod \theta \\ -yx^{p-1} \quad -xy^{p-1} \quad & \equiv z^p \mod \theta \end{aligned} \tag{8}$$

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

(8) の関係式を上式へ代入する。

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

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

$$\begin{aligned} & x + z \not\equiv y \mod 3 \\ & \delta \neq 3 \end{aligned}$$

$$\begin{aligned} 3x^p \quad & \equiv 0 \mod \delta \\ 3y^p \quad & \equiv 0 \mod \delta \\ 3z^p \quad & \equiv 0 \mod \delta \end{aligned}$$

これは $\delta \perp xyz$ と矛盾する。

1.3 $\delta = 2$

1.3.1 $2 \mid x$, $2 \perp yz$

$S = 2^k$ 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

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