

# General solution conditions

Hajime Mashima

## Abstract

Modulo not divisible by  $xyz$  and possible expansions.

## Contents

<b>1</b>	<b>introduction</b>	<b>2</b>
1.1	$\delta \perp xyz$ の導出 . . . . .	2
1.1.1	$p \mid x$ のとき . . . . .	4
1.1.2	$p \perp x$ のとき ( $p \mid yz$ 条件は省略) . . . . .	5
1.2	解の条件 (Solution conditions) . . . . .	6
1.3	同値変換 (Equivalence transformation) . . . . .	10
1.4	一般的解の条件 (General solution conditions) . . . . .	10
1.4.1	$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1}$ のとき . . . . .	10
1.4.2	Common to $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2}$ . . . . .	11
1.4.3	$-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2}$ . . . . .	13
1.4.4	$-y \equiv z \equiv x \pmod{\theta_3}$ のとき . . . . .	13
1.4.5	Common to $-y \not\equiv z \not\equiv x \pmod{\theta_4}$ . . . . .	14
1.5	$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\delta}$ . . . . .	15
1.5.1	$x \equiv -y \equiv -2^{-1}z \pmod{\theta}$ のとき . . . . .	15
1.5.2	Common to $x \not\equiv -y \not\equiv -2^{-1}z \pmod{\theta}$ . . . . .	15
1.5.3	Common to $x^{p-1} \not\equiv -y^{p-1} \not\equiv 2z^{p-1} \pmod{\theta}$ . . . . .	16
1.6	$\delta = 2$ のとき . . . . .	18
1.6.1	$2 \mid x$ , $2 \perp yz$ . . . . .	18
1.7	補足 (supplement) . . . . .	19
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 . . . . .	19
1.7.2	まとめ . . . . .	20
1.8	$\delta' \perp xyz$ の導出 . . . . .	21
1.8.1	$p \mid z$ のとき (諸条件は省略) . . . . .	21
1.9	一般的解の条件 (General solution conditions) . . . . .	22
1.9.1	$-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \pmod{\theta'_1}$ のとき . . . . .	22
1.9.2	Common to $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\theta'_2}$ . . . . .	23
1.9.3	$-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\theta'_2}$ . . . . .	24
1.9.4	$z \equiv x \equiv y \pmod{\theta'_3}$ のとき . . . . .	24
1.9.5	Common to $z \not\equiv x \not\equiv y \pmod{\theta'_4}$ . . . . .	25
1.10	$-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \pmod{\delta'}$ . . . . .	26
1.10.1	$x \equiv z \equiv -2^{-1}y \pmod{\theta'}$ のとき . . . . .	26

1.10.2	Common to $x \not\equiv z \not\equiv -2^{-1}y \pmod{\theta'}$ . . . . .	26
1.10.3	Common to $-x^{p-1} \not\equiv z^{p-1} \not\equiv 2y^{p-1} \pmod{\theta'}$ . . . . .	27
1.11	$\delta' = 2$ のとき . . . . .	29
1.11.1	$2 \mid z$ , $2 \perp xy$ . . . . .	29

## 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 $\delta \perp xyz$ の導出

#### Theorem 1 (Fermat's Last Theorem)

$$x^p + y^p \neq z^p \quad (p \geq 3 \text{ であり } x, y, z \text{ は互いに素で一つが偶数})$$

**Proposition 2**  $p$  が奇素数で  $x^p + y^p = z^p$  を満たすとき

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

**Proof 3**  $(x + y - z)^p = x^p + y^p - z^p + p(\dots \text{省略})$

$$x^p + y^p - z^p = 0 \Rightarrow p \mid (x + y - z)^p$$

$p \mid x \Rightarrow p \mid (z - y)$  と置ける。

一般的に

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

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

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

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

$p^2 \mid R \Rightarrow p \mid y^{p-1}$  となり前提に反するので

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

また  $p$  を除く素数に関して、 $py^{p-1}$  は  $z - y$  の因数を持たないため

$$L \perp R \quad (p \text{ を除く}) \tag{2}$$

**Definition 4** (1), (2) より  $p \perp abc$  として以下のように置ける。

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

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

$b^p - c^p = (L')(R')$  と置くと  $p \mid L' \Leftrightarrow p \mid R'$  なので

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

よって、少なくとも

$$p^2 \mid x$$

$x = p^2a\alpha$  と仮定すると

$$x^p = p^{2p}a^p\alpha^p$$

(1) より  $x^p = (z - y) \cdot p\alpha^p$  なので

$$z - y = p^{2p-1}a^p$$

一般的に

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

□

また

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

$$p^n \mid x + y - z \tag{3}$$

1.1.1  $p \mid x$  のとき

$$\begin{aligned} x &= p^n a \alpha & z - y &= p^{np-1} a^p \\ y &= b \beta & z - x &= b^p \\ z &= c \gamma & x + y &= c^p \\ p &\perp a \alpha y z & \delta &= \text{奇素数 (definition)} \end{aligned}$$

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

**Proof 6**

$$\begin{aligned} x + z - y &= p^n a \alpha + p^{np-1} a^p \\ &= p^n a (\alpha + p^{(p-1)n-1} a^{p-1}) \\ p &\perp S \quad , \quad p \perp \delta \\ p \alpha^p &= R = p y^{p-1} + (z - y)(\dots) \\ R &\equiv p y^{p-1} \pmod{a} \\ p y^{p-1} &\perp a \\ \alpha &\perp a \end{aligned}$$

$\delta \mid S$  のとき  $\delta \mid a$  または  $\delta \mid \alpha$  ならば矛盾するので

$$\delta \perp x$$

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

$\delta \mid bc$  ならば  $\delta \mid 2x$  でなければならず矛盾するので

$$\delta \perp bc$$

$\delta \mid \beta$  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  $p \perp x$  のとき ( $p \mid yz$  条件は省略)

$$\begin{aligned} x &= a'\alpha' & z - y &= a'^p \\ y &= b'\beta' & z - x &= b'^p \\ z &= c'\gamma' & x + y &= c'^p \\ p &\perp xyz & \delta &= \text{奇素数 (definition)} \end{aligned}$$

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

**Proof 8**

$$\begin{aligned} x + z - y &= a'\alpha' + a'^p \\ &= a'(\alpha' + a'^{p-1}) \\ (3) \text{ より } p &\perp S' \text{ , } p \perp \delta \\ \alpha'^p &= R = py^{p-1} + (z - y)(\dots) \\ R &\equiv py^{p-1} \pmod{a'} \\ py^{p-1} &\perp a' \\ \alpha' &\perp a' \end{aligned}$$

$\delta \mid S'$  のとき  $\delta \mid a'$  または  $\delta \mid \alpha'$  ならば矛盾するので

$$\delta \perp x$$

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

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

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

$\delta \mid \beta'$  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。

$$\begin{aligned}
 x^p + Uz^{p-1} &\equiv Ty^{p-1} \pmod{\theta} \\
 z^p - y^p + Uz^{p-1} &\equiv Ty^{p-1} \pmod{\theta} \\
 z^p + Uz^{p-1} &\equiv Ty^{p-1} + y^p \pmod{\theta} \\
 z^{p-1}(z + U) &\equiv y^{p-1}(T + y) \pmod{\theta} \\
 z^{p-1}(yz + yU) &\equiv y \cdot y^{p-1}(T + y) \pmod{\theta}
 \end{aligned} \tag{4}$$

$Uz^{p-1} \cdot Ty^{p-1} \equiv y^p z^p \pmod{\theta}$  ならば

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

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

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 (4)、 $Uz^{p-1} \cdot Ty^{p-1} \equiv y^p z^p \pmod{\theta}$  を満たすとき解の候補は以下の 2 通りである。

$$\begin{aligned}
 Uz^{p-1} &\equiv y^p \pmod{\theta} \\
 Ty^{p-1} &\equiv z^p \pmod{\theta} \\
 &or \\
 Uz^{p-1} &\equiv -z^p \pmod{\theta} \\
 Ty^{p-1} &\equiv -y^p \pmod{\theta}
 \end{aligned} \tag{5}$$

$\theta \perp xyz$  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。

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

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

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

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

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

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

$$\begin{aligned} -U'z^{p-1} &\equiv x^p \pmod{\theta} \\ -T'x^{p-1} &\equiv z^p \pmod{\theta} \\ &or \\ -U'z^{p-1} &\equiv -z^p \pmod{\theta} \\ -T'x^{p-1} &\equiv -x^p \pmod{\theta} \end{aligned} \quad (7)$$

$\theta \perp xyz$  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。

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

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

$$-U''y^{p-1} \cdot -T''x^{p-1} \equiv x^p y^p \pmod{\theta} \text{ ならば}$$

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

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

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

$$\begin{aligned} -U''y^{p-1} &\equiv x^p \pmod{\theta} \\ -T''x^{p-1} &\equiv y^p \pmod{\theta} \\ &or \\ -U''y^{p-1} &\equiv y^p \pmod{\theta} \\ -T''x^{p-1} &\equiv x^p \pmod{\theta} \end{aligned} \quad (9)$$



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

【Solution conditions】

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

(4),(6),(8) 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

$$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\delta} \text{ は同時に成り立つ。} \quad (10)$$

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

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

$U = y$  ,  $T = z$  を例とする全条件 (\*This condition is not applicable here.)

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

**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** 以下の関係式における同値変換の成立条件が3組共通であるとき General solution conditions と呼ぶ。

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

**1.4.1**  $-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1}$  のとき

$$\begin{aligned} s_1x^{p-1} - t_2y^{p-1} &\equiv -u_3z^{p-1} \pmod{\theta_1} \\ -s_3x^{p-1} + t_1y^{p-1} &\equiv u_2z^{p-1} \pmod{\theta_1} \\ -s_2x^{p-1} + t_3y^{p-1} &\equiv u_1z^{p-1} \pmod{\theta_1} \end{aligned}$$

mod  $\theta_1$  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】

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

**1.4.2 Common to  $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2}$**

(11)、(5) より

$$\begin{aligned}
Uz^{p-1} &\equiv -yx^{p-1} \pmod{\delta} \\
Ty^{p-1} &\equiv -zx^{p-1} \pmod{\delta} \\
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
x^p - yx^{p-1} &\equiv -zx^{p-1} \pmod{\theta_1} \\
x^p + zx^{p-1} &\equiv yx^{p-1} \pmod{\theta_2} \\
-yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \pmod{\delta} \\
(x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta} \tag{12}
\end{aligned}$$

(11)、(7) より

$$\begin{aligned}
-U'z^{p-1} &\equiv -xy^{p-1} \pmod{\delta} \\
-T'x^{p-1} &\equiv zy^{p-1} \pmod{\delta} \\
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
-xy^{p-1} + y^p &\equiv zy^{p-1} \pmod{\theta_1} \\
-zy^{p-1} + y^p &\equiv xy^{p-1} \pmod{\theta_2} \\
-xy^{p-1} \cdot zy^{p-1} &\equiv x^p z^p \pmod{\delta} \\
(y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \tag{13}
\end{aligned}$$

(11)、(9) より

$$\begin{aligned}
-U''y^{p-1} &\equiv -xz^{p-1} \pmod{\delta} \\
-T''x^{p-1} &\equiv yz^{p-1} \pmod{\delta} \\
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
-xz^{p-1} + yz^{p-1} &\equiv z^p \pmod{\theta_1} \\
yz^{p-1} - xz^{p-1} &\equiv z^p \pmod{\theta_2} \\
-xz^{p-1} \cdot yz^{p-1} &\equiv x^p y^p \pmod{\delta} \\
(z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \tag{14}
\end{aligned}$$

(12)(13)(14) より

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

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

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{3} \\ x \cdot x^{2n} + y \cdot y^{2n} &\equiv z \cdot z^{2n} \pmod{3} \end{aligned}$$

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

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

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

$\delta \perp 3AB$  なので

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

2つの因数のうち、一方は  $\delta$  と互いに素である。 (15)

1.4.3  $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2}$

(13)(14) より

$$\begin{aligned}(x^{p-1})^2 + (z^{p-1})^2 + (y^{p-1})^2 &\equiv 0 \pmod{\theta_2} \\ (x^{p-1})^2 - x^{p-1}y^{p-1} - x^{p-1}z^{p-1} &\equiv 0 \pmod{\theta_2} \\ x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_2}\end{aligned}$$

$s'', t'', u''$  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。

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

同値変換の成立条件

$$\begin{aligned}[s_1'' &\equiv u_3'' - t_2'' \pmod{\theta}] \\ [t_1'' &\equiv u_2'' - s_3'' \pmod{\theta}] \\ [u_1'' &\equiv s_2'' + t_3'' \pmod{\theta}]\end{aligned}$$

1.4.4  $-y \equiv z \equiv x \pmod{\theta_3}$  のとき

$$\begin{aligned}s_1''x + t_1''y &\equiv u_1''z \pmod{\theta_3} \\ s_2''x - t_2''y &\equiv -u_2''z \pmod{\theta_3} \\ -s_3''x - t_3''y &\equiv u_3''z \pmod{\theta_3}\end{aligned}$$

$\pmod{\theta_3}$  として

$$\begin{aligned}s_1'' &\equiv x^{p-1}, \quad t_1'' \equiv y^{p-1}, \quad u_1'' \equiv z^{p-1} \\ s_2'' &\equiv x^{p-1}, \quad t_2'' \equiv -y^{p-1}, \quad u_2'' \equiv -z^{p-1} \\ s_3'' &\equiv -x^{p-1}, \quad t_3'' \equiv -y^{p-1}, \quad u_3'' \equiv z^{p-1} \\ [x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_2}]\end{aligned}$$

【General solution conditions】

$$\begin{aligned}x^p - y^{p-1}x &\equiv z^{p-1}x \pmod{\theta_2} \\ -x^{p-1}y + y^p &\equiv -z^{p-1}y \pmod{\theta_2} \\ x^{p-1}z - y^{p-1}z &\equiv z^p \pmod{\theta_2}\end{aligned} \tag{16}$$

1.4.5 Common to  $-y \not\equiv z \not\equiv x \pmod{\theta_4}$

(16) より

$$\begin{aligned} -y^{p-1}x \cdot z^{p-1}x &\equiv y^p z^p \pmod{\theta_2} \\ -x^2 &\equiv yz \pmod{\theta_2} \\ x^2 &\equiv -yz \pmod{\theta_2} \end{aligned} \quad (17)$$

$$\begin{aligned} (12) \text{ より } (x^{p-1})^2 &\equiv y^{p-1}z^{p-1} \pmod{\theta_2} \\ (x^2)^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\theta_2} \\ (-yz)^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\theta_2} \\ y^{p-1}z^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\theta_2} \end{aligned}$$

---


$$\begin{aligned} -x^{p-1}y \cdot -z^{p-1}y &\equiv x^p z^p \pmod{\theta_2} \\ y^2 &\equiv xz \pmod{\theta_2} \end{aligned} \quad (18)$$

$$\begin{aligned} (13) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1}z^{p-1} \pmod{\theta_2} \\ (y^2)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\theta_2} \\ (xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\theta_2} \\ x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\theta_2} \end{aligned}$$

$\delta$  の定義に反する。

---


$$\begin{aligned} x^{p-1}z \cdot -y^{p-1}z &\equiv x^p y^p \pmod{\theta_2} \\ -z^2 &\equiv xy \pmod{\theta_2} \\ z^2 &\equiv -xy \pmod{\theta_2} \end{aligned} \quad (19)$$

$$\begin{aligned} (14) \text{ より } (z^{p-1})^2 &\equiv -x^{p-1}y^{p-1} \pmod{\theta_2} \\ (z^2)^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\theta_2} \\ (-xy)^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\theta_2} \\ x^{p-1}y^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\theta_2} \end{aligned}$$

$\delta$  の定義に反するので  $\theta_2 \neq \delta$

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

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  $\theta_1 = \delta$

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

$$1.5 \quad -x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\delta}$$

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

1.5.1  $x \equiv -y \equiv -2^{-1}z \pmod{\theta}$  のとき

$\theta \neq 2$  のとき  $2^{-1} \equiv 2^{\theta-2} \pmod{\theta}$  と置けるので計算上差し障りない。

$$\begin{aligned} s_1x - t_2y &\equiv -2^{-1}zu_3 \pmod{\theta} \\ -s_3x + t_1y &\equiv 2^{-1}zu_2 \pmod{\theta} \\ -2s_2x + 2t_3y &\equiv u_1z \pmod{\theta} \end{aligned}$$

$\pmod{\theta}$  として

$$\begin{aligned} s_1 &\equiv x^{p-1}, \quad t_1 \equiv y^{p-1}, \quad u_1 \equiv z^{p-1} \\ s_2 &\equiv -2^{-1}x^{p-1}, \quad t_2 \equiv -y^{p-1}, \quad u_2 \equiv 2z^{p-1} \\ s_3 &\equiv -x^{p-1}, \quad t_3 \equiv 2^{-1}y^{p-1}, \quad u_3 \equiv -2z^{p-1} \\ [x^{p-1} - y^{p-1} + 2z^{p-1} &\equiv 0 \pmod{\delta}] \end{aligned}$$

【General solution conditions】

$$\begin{aligned} x^p - y^{p-1}x &\equiv -2z^{p-1}x \pmod{\delta} \\ -x^{p-1}y + y^p &\equiv 2z^{p-1}y \pmod{\delta} \\ -2^{-1}x^{p-1}z + 2^{-1}y^{p-1}z &\equiv z^p \pmod{\delta} \end{aligned}$$

1.5.2 Common to  $x \not\equiv -y \not\equiv -2^{-1}z \pmod{\theta}$

$$\begin{aligned} -y^{p-1}x \cdot -2z^{p-1}x &\equiv y^p z^p \pmod{\delta} \\ 2x^2 &\equiv yz \pmod{\delta} \\ x^2 &\equiv 2^{-1}yz \pmod{\delta} \end{aligned} \tag{20}$$

$$\begin{aligned} -x^{p-1}y \cdot 2z^{p-1}y &\equiv x^p z^p \pmod{\delta} \\ -2y^2 &\equiv xz \pmod{\delta} \\ y^2 &\equiv -2^{-1}xz \pmod{\delta} \end{aligned} \tag{21}$$

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

(20)(21)(22) より

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

$$\begin{aligned} x^3 + y^3 &\equiv (x+y)(x^2 - xy + y^2) \equiv 0 \pmod{\delta} \\ (2^{-1}z)^3 - y^3 &\equiv (2^{-1}z - y)((2^{-1}z)^2 + 2^{-1}zy + y^2) \equiv 0 \pmod{\delta} \\ (2^{-1}z)^3 + x^3 &\equiv (2^{-1}z + x)((2^{-1}z)^2 - 2^{-1}zx + x^2) \equiv 0 \pmod{\delta} \end{aligned}$$

$x + z - y \equiv 0 \pmod{\delta}$  ,  $x \not\equiv -y \pmod{\delta}$  であるから

$$x \not\equiv -y \not\equiv -2^{-1}z \pmod{\delta}$$

よって

$$\begin{aligned} x^2 - xy + y^2 &\equiv 0 \pmod{\delta} \\ (21) \text{ より } x^2 - xy - 2^{-1}xz &\equiv 0 \pmod{\delta} \\ x - y &\equiv 2^{-1}z \pmod{\delta} \end{aligned}$$

$-z \not\equiv 2^{-1}z \pmod{\delta}$  であるが演算を続ける。

【General solution conditions】

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

**1.5.3 Common to  $x^{p-1} \not\equiv -y^{p-1} \not\equiv 2z^{p-1} \pmod{\theta}$**

$$\begin{aligned} -yx^{p-1} \cdot 2^{-1}zx^{p-1} &\equiv y^p z^p \pmod{\delta} \\ -(x^{p-1})^2 &\equiv 2y^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \quad (23)$$

$$\begin{aligned} -xy^{p-1} \cdot -2^{-1}zy^{p-1} &\equiv x^p z^p \pmod{\delta} \\ (y^{p-1})^2 &\equiv 2x^{p-1}z^{p-1} \pmod{\delta} \end{aligned} \quad (24)$$

$$\begin{aligned} 2z^{p-1}x \cdot -2z^{p-1}y &\equiv x^p y^p \pmod{\delta} \\ -2^2 (z^{p-1})^2 &\equiv x^{p-1}y^{p-1} \pmod{\delta} \end{aligned} \quad (25)$$

(23)(24)(25) より

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



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

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

$$x^{p-1} + y^{p-1} \equiv 0 \pmod{\delta} \quad \wedge \quad x^{p-1} - y^{p-1} + 2z^{p-1} \equiv 0 \pmod{\delta}$$

これは (15) と矛盾する。また

$$\begin{aligned}
(12) \text{ より } (x^{p-1})^2 &\equiv y^{p-1}z^{p-1} \pmod{\delta} \\
(x^2)^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\delta} \\
(20) \text{ より } (2^{-1}yz)^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\delta} \\
2^{-(p-1)}y^{p-1}z^{p-1} &\equiv y^{p-1}z^{p-1} \pmod{\delta} \\
1 &\equiv 2^{p-1} \pmod{\delta}
\end{aligned}$$

.....

$$\begin{aligned}
(13) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1}z^{p-1} \pmod{\delta} \\
(y^2)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\delta} \\
(21) \text{ より } (-2^{-1}xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\delta} \\
2^{-(p-1)}x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\delta} \\
-1 &\equiv 2^{p-1} \pmod{\delta}
\end{aligned}$$

.....

$$\begin{aligned}
(14) \text{ より } (z^{p-1})^2 &\equiv -x^{p-1}y^{p-1} \pmod{\delta} \\
(z^2)^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\delta} \\
(22) \text{ より } (-2^2xy)^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\delta} \\
2^{2(p-1)}x^{p-1}y^{p-1} &\equiv -x^{p-1}y^{p-1} \pmod{\delta} \\
(2^{p-1})^2 &\equiv -1 \pmod{\delta}
\end{aligned}$$

上式を満たす  $\delta$  は存在しない。  
よって

$$\delta \neq odd$$

## 1.6 $\delta = 2$ のとき

1.6.1  $2 \mid x$  ,  $2 \perp yz$

$S = 2^k$  のとき

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

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

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

$$2 \mid a$$

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

$$2 \perp \alpha$$

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

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

$$2^0 = 1$$

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。

## 1.7 補足 (supplement)

### 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

- $-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1}$  のとき

$$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1}$$

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

$$\theta_1 = \delta$$

.....  
(17)(18)(19) より

$$-y^3 \equiv z^3 \equiv x^3 \pmod{\theta_2}$$

$$z^3 + y^3 \equiv (z + y)(z^2 - yz + y^2) \equiv 0 \pmod{\theta_2}$$

$$x^3 - z^3 \equiv (x - z)(x^2 + xz + z^2) \equiv 0 \pmod{\theta_2}$$

$$x^3 + y^3 \equiv (x + y)(x^2 - xy + y^2) \equiv 0 \pmod{\theta_2}$$

- $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2} \quad \wedge \quad -y \equiv z \equiv x \pmod{\theta_3}$  のとき

$$[x^{p-1} - y^{p-1} - z^{p-1} \equiv 0 \pmod{\theta_2}]$$

$$-y \equiv z \equiv x \pmod{\theta_3}$$

$$\theta_2 = \theta_3$$

※ただし  $\delta = \theta_2$  ならば

$$x^2 + xz + z^2 \equiv 0 \pmod{\theta_4}$$

$$(19) \text{ より } x^2 + xz - xy \equiv 0 \pmod{\theta_4}$$

$$x + z - y \equiv 0 \pmod{\theta_4}$$

と成り、 $\delta = \theta_4$  が確定するので  $\delta \neq \theta_3$

- $-x^{p-1} \not\equiv y^{p-1} \not\equiv z^{p-1} \pmod{\theta_2} \quad \wedge \quad -y \not\equiv z \not\equiv x \pmod{\theta_4}$  のとき

$$[x^{p-1} - y^{p-1} - z^{p-1} \equiv 0 \pmod{\theta_2}]$$

$$x^2 + xz + z^2 \equiv 0 \pmod{\theta_4}$$

$$\theta_2 = \theta_4$$

※ただし  $\delta = \theta_1$  のときは  $\delta \neq \theta_2$  であり (17)(18)(19) は成り立たない。この場合

$$[x + z - y \not\equiv 0 \pmod{\theta_4}]$$

### 1.7.2 まとめ

【General solution conditions】

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_1} \\
 &\Leftrightarrow \\
 x^p - yx^{p-1} &\equiv -zx^{p-1} \pmod{\theta_1} \\
 -xy^{p-1} + y^p &\equiv zy^{p-1} \pmod{\theta_1} \\
 -xz^{p-1} + yz^{p-1} &\equiv z^p \pmod{\theta_1}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_4} \\
 &\Leftrightarrow \\
 x^p + zx^{p-1} &\equiv yx^{p-1} \pmod{\theta_4} \\
 -zy^{p-1} + y^p &\equiv xy^{p-1} \pmod{\theta_4} \\
 yz^{p-1} - xz^{p-1} &\equiv z^p \pmod{\theta_4}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_3} \\
 &\Leftrightarrow \\
 x^p - y^{p-1}x &\equiv z^{p-1}x \pmod{\theta_3} \\
 -x^{p-1}y + y^p &\equiv -z^{p-1}y \pmod{\theta_3} \\
 x^{p-1}z - y^{p-1}z &\equiv z^p \pmod{\theta_3}
 \end{aligned}$$

$$\begin{aligned}
 x^p + y^p &\equiv z^p \pmod{\theta_4} \\
 &\Leftrightarrow \\
 x^p - z^{p-1}x &\equiv y^{p-1}x \pmod{\theta_4} \\
 z^{p-1}y + y^p &\equiv x^{p-1}y \pmod{\theta_4} \\
 -y^{p-1}z + x^{p-1}z &\equiv z^p \pmod{\theta_4}
 \end{aligned}$$

【Equivalence transformation】

$$\begin{aligned}
 -x^{p-1} &\equiv y^{p-1} \equiv z^{p-1} \pmod{\theta_1} \\
 xx^{p-1} + yy^{p-1} &\equiv zz^{p-1} \pmod{\theta_1} \\
 -xz^{p-1} - yx^{p-1} &\equiv zy^{p-1} \pmod{\theta_1} \\
 -xy^{p-1} + yz^{p-1} &\equiv -zx^{p-1} \pmod{\theta_1}
 \end{aligned}$$

or

$$\begin{aligned}
 [x^{p-1} - y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta_2}] \\
 xx^{p-1} + yy^{p-1} &\equiv zz^{p-1} \pmod{\theta_2} \\
 yz^{p-1} + zx^{p-1} &\equiv xy^{p-1} \pmod{\theta_2} \\
 -zy^{p-1} - xz^{p-1} &\equiv yx^{p-1} \pmod{\theta_2}
 \end{aligned}$$

## 1.8 $\delta' \perp xyz$ の導出

### 1.8.1 $p \mid z$ のとき (諸条件は省略)

$$\begin{array}{lll} x = a\alpha & y = b\beta & z = p^n c\gamma \\ z - y = a^p & z - x = b^p & x + y = p^{np-1} c^p \\ p \perp xyc\gamma & & \delta' = \text{奇素数 (definition)} \end{array}$$

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

**Proof 13**

$$\begin{aligned} z + x + y &= p^n c\gamma + p^{np-1} c^p \\ &= p^n c(\gamma + p^{(p-1)n-1} c^{p-1}) \\ p &\perp S'' \quad , \quad p \perp \delta' \\ p\gamma^p &= R = py^{p-1} + (x+y)(\dots) \\ R &\equiv py^{p-1} \pmod{c} \\ py^{p-1} &\perp c \\ \gamma &\perp c \end{aligned}$$

$\delta' \mid S''$  のとき  $\delta' \mid c$  または  $\delta' \mid \gamma$  ならば矛盾するので

$$\delta' \perp z$$

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

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

$$\delta' \perp ab$$

$\delta' \mid \beta$  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

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

$U = -y$  ,  $T = -z$  を例とする全条件 (\*This condition is not applicable here.)

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

## 1.9 一般解の条件 (General solution conditions)

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

### 1.9.1 $-z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \pmod{\theta'_1}$ のとき

$$\begin{aligned} s_1x^{p-1} + t_2y^{p-1} &\equiv -u_3z^{p-1} \pmod{\theta'_1} \\ s_3x^{p-1} + t_1y^{p-1} &\equiv -u_2z^{p-1} \pmod{\theta'_1} \\ -s_2x^{p-1} - t_3y^{p-1} &\equiv u_1z^{p-1} \pmod{\theta'_1} \end{aligned}$$

$\pmod{\theta'_1}$  として

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

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

【General solution conditions】

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

**1.9.2 Common to  $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\theta'_2}$**

(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

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

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

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

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

(15) と同様

$$2 \text{ つの因数のうち、一方は } \delta' \text{ と互いに素である。} \quad (30)$$

**1.9.3**  $-z^{p-1} \not\equiv x^{p-1} \not\equiv y^{p-1} \pmod{\theta'_2}$

(28)(29) より

$$\begin{aligned} (x^{p-1})^2 + (z^{p-1})^2 + (y^{p-1})^2 &\equiv 0 \pmod{\theta'_2} \\ (x^{p-1})^2 + x^{p-1}y^{p-1} - x^{p-1}z^{p-1} &\equiv 0 \pmod{\theta'_2} \\ x^{p-1} + y^{p-1} - z^{p-1} &\equiv 0 \pmod{\theta'_2} \end{aligned}$$

$s'', t'', u''$  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。

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

同値変換の成立条件

$$\begin{aligned} [s''_1 &\equiv u''_3 - t''_2 \pmod{\theta'}] \\ [t''_1 &\equiv u''_2 - s''_3 \pmod{\theta'}] \\ [u''_1 &\equiv s''_2 + t''_3 \pmod{\theta'}] \end{aligned}$$

**1.9.4**  $z \equiv x \equiv y \pmod{\theta'_3}$  のとき

$$\begin{aligned} s''_1x + t''_1y &\equiv u''_1z \pmod{\theta'_3} \\ s''_2x + t''_2y &\equiv u''_2z \pmod{\theta'_3} \\ s''_3x + t''_3y &\equiv u''_3z \pmod{\theta'_3} \end{aligned}$$

$\pmod{\theta'_3}$  として

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

【General solution conditions】

$$\begin{aligned} x^p + xy^{p-1} &\equiv xz^{p-1} \pmod{\theta'_2} \\ yx^{p-1} + y^p &\equiv yz^{p-1} \pmod{\theta'_2} \\ zx^{p-1} + zy^{p-1} &\equiv z^p \pmod{\theta'_2} \end{aligned} \tag{31}$$



1.9.5 Common to  $z \not\equiv x \not\equiv y \pmod{\theta'_4}$

(31) より

$$\begin{aligned} xy^{p-1} \cdot xz^{p-1} &\equiv y^p z^p \pmod{\theta'_2} \\ x^2 &\equiv yz \pmod{\theta'_2} \end{aligned} \quad (32)$$

$$(27) \text{ より } (x^{p-1})^2 \equiv -y^{p-1} z^{p-1} \pmod{\theta'_2}$$

$$(x^2)^{p-1} \equiv -y^{p-1} z^{p-1} \pmod{\theta'_2}$$

$$(32) \text{ より } (yz)^{p-1} \equiv -y^{p-1} z^{p-1} \pmod{\theta'_2}$$

$$y^{p-1} z^{p-1} \equiv -y^{p-1} z^{p-1} \pmod{\theta'_2}$$

$\delta'$  の定義に反する。

$$\begin{aligned} yx^{p-1} \cdot yz^{p-1} &\equiv x^p z^p \pmod{\theta'_2} \\ y^2 &\equiv xz \pmod{\theta'_2} \end{aligned} \quad (33)$$

$$(28) \text{ より } (y^{p-1})^2 \equiv -x^{p-1} z^{p-1} \pmod{\theta'_2}$$

$$(y^2)^{p-1} \equiv -x^{p-1} z^{p-1} \pmod{\theta'_2}$$

$$(33) \text{ より } (xz)^{p-1} \equiv -x^{p-1} z^{p-1} \pmod{\theta'_2}$$

$$x^{p-1} z^{p-1} \equiv -x^{p-1} z^{p-1} \pmod{\theta'_2}$$

$\delta'$  の定義に反する。

$$\begin{aligned} zx^{p-1} \cdot zy^{p-1} &\equiv x^p y^p \pmod{\theta'_2} \\ z^2 &\equiv xy \pmod{\theta'_2} \end{aligned} \quad (34)$$

$$(29) \text{ より } (z^{p-1})^2 \equiv x^{p-1} y^{p-1} \pmod{\theta'_2}$$

$$(z^2)^{p-1} \equiv x^{p-1} y^{p-1} \pmod{\theta'_2}$$

$$(34) \text{ より } (xy)^{p-1} \equiv x^{p-1} y^{p-1} \pmod{\theta'_2}$$

$$x^{p-1} y^{p-1} \equiv x^{p-1} y^{p-1} \pmod{\theta'_2}$$

2条件が  $\delta'$  の定義に反するので  $\theta'_2 \neq \delta'$

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

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  $\theta'_1 = \delta'$

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

$$1.10 \quad -z^{p-1} \equiv x^{p-1} \equiv y^{p-1} \pmod{\delta'}$$

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

1.10.1  $x \equiv z \equiv -2^{-1}y \pmod{\theta'}$  のとき

$\theta' \neq 2$  のとき  $2^{-1} \equiv 2^{\theta'-2} \pmod{\theta'}$  と置けるので計算上差し障りない。

$$\begin{aligned} s_1x - 2^{-1}yt_2 &\equiv u_3z \pmod{\theta'} \\ -2s_3x + t_1y &\equiv -2u_2z \pmod{\theta'} \\ s_2x - 2^{-1}yt_3 &\equiv u_1z \pmod{\theta'} \end{aligned}$$

$\pmod{\theta'}$  として

$$\begin{aligned} s_1 &\equiv x^{p-1}, \quad t_1 \equiv y^{p-1}, \quad u_1 \equiv z^{p-1} \\ s_2 &\equiv x^{p-1}, \quad t_2 \equiv -2y^{p-1}, \quad u_2 \equiv -2^{-1}z^{p-1} \\ s_3 &\equiv -2^{-1}x^{p-1}, \quad t_3 \equiv -2y^{p-1}, \quad u_3 \equiv z^{p-1} \\ [x^{p-1} - 2y^{p-1} - z^{p-1} &\equiv 0 \pmod{\delta'}] \end{aligned}$$

【General solution conditions】

$$\begin{aligned} x^p - 2y^{p-1}x &\equiv z^{p-1}x \pmod{\delta'} \\ -2^{-1}x^{p-1}y + y^p &\equiv -2^{-1}z^{p-1}y \pmod{\delta'} \\ x^{p-1}z - 2y^{p-1}z &\equiv z^p \pmod{\delta'} \end{aligned}$$

1.10.2 Common to  $x \not\equiv z \not\equiv -2^{-1}y \pmod{\theta'}$

$$\begin{aligned} -2y^{p-1}x \cdot z^{p-1}x &\equiv y^p z^p \pmod{\delta'} \\ -2x^2 &\equiv yz \pmod{\delta'} \\ x^2 &\equiv -2^{-1}yz \pmod{\delta'} \end{aligned} \tag{35}$$

$$\begin{aligned} -2^{-1}x^{p-1}y \cdot -2^{-1}z^{p-1}y &\equiv x^p z^p \pmod{\delta'} \\ 2^{-2}y^2 &\equiv xz \pmod{\delta'} \\ y^2 &\equiv 2^2xz \pmod{\delta'} \end{aligned} \tag{36}$$

$$\begin{aligned} x^{p-1}z \cdot -2y^{p-1}z &\equiv x^p y^p \pmod{\delta'} \\ -2z^2 &\equiv xy \pmod{\delta'} \\ z^2 &\equiv -2^{-1}xy \pmod{\delta'} \end{aligned} \tag{37}$$

(35)(36)(37) より

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

$$\begin{aligned} x^3 - z^3 &\equiv (x - z)(x^2 + xz + z^2) \equiv 0 \pmod{\delta'} \\ (2^{-1}y)^3 + z^3 &\equiv (2^{-1}y + z)((2^{-1}y)^2 - 2^{-1}yz + z^2) \equiv 0 \pmod{\delta'} \\ (2^{-1}y)^3 + x^3 &\equiv (2^{-1}y + x)((2^{-1}y)^2 - 2^{-1}xy + x^2) \equiv 0 \pmod{\delta'} \end{aligned}$$

$x + y + z \equiv 0 \pmod{\delta'}$  ,  $x \not\equiv z \pmod{\delta'}$  であるから

$$x \not\equiv z \not\equiv -2^{-1}y \pmod{\delta'}$$

よって

$$\begin{aligned} x^2 + xz + z^2 &\equiv 0 \pmod{\delta'} \\ (37) \text{ より } x^2 + xz - 2^{-1}xy &\equiv 0 \pmod{\delta'} \\ x - 2^{-1}y &\equiv -z \pmod{\delta'} \end{aligned}$$

$y \not\equiv -2^{-1}y \pmod{\delta'}$  であるが演算を続ける。

【General solution conditions】

$$\begin{aligned} x^p - 2^{-1}yx^{p-1} &\equiv -zx^{p-1} \pmod{\delta'} \\ -2xy^{p-1} + y^p &\equiv 2zy^{p-1} \pmod{\delta'} \\ -xz^{p-1} + 2^{-1}yz^{p-1} &\equiv z^p \pmod{\delta'} \end{aligned}$$

**1.10.3 Common to**  $-x^{p-1} \not\equiv z^{p-1} \not\equiv 2y^{p-1} \pmod{\theta'}$

$$\begin{aligned} -2^{-1}yx^{p-1} \cdot -zx^{p-1} &\equiv y^p z^p \pmod{\delta'} \\ (x^{p-1})^2 &\equiv 2y^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (38)$$

$$\begin{aligned} -2xy^{p-1} \cdot 2zy^{p-1} &\equiv x^p z^p \pmod{\delta'} \\ -2^2 (y^{p-1})^2 &\equiv x^{p-1} z^{p-1} \pmod{\delta'} \end{aligned} \quad (39)$$

$$\begin{aligned} -xz^{p-1} \cdot 2^{-1}yz^{p-1} &\equiv x^p y^p \pmod{\delta'} \\ -(z^{p-1})^2 &\equiv 2x^{p-1} y^{p-1} \pmod{\delta'} \end{aligned} \quad (40)$$

(38)(39)(40) より

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

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

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

$$x^{p-1} + z^{p-1} \equiv 0 \pmod{\delta'} \quad \wedge \quad x^{p-1} - 2y^{p-1} - z^{p-1} \equiv 0 \pmod{\delta'}$$

これは (30) と矛盾する。また

$$\begin{aligned}
(27) \text{ より } (x^{p-1})^2 &\equiv -y^{p-1}z^{p-1} \pmod{\delta'} \\
(x^2)^{p-1} &\equiv -y^{p-1}z^{p-1} \pmod{\delta'} \\
(35) \text{ より } (-2^{-1}yz)^{p-1} &\equiv -y^{p-1}z^{p-1} \pmod{\delta'} \\
2^{-(p-1)}y^{p-1}z^{p-1} &\equiv -y^{p-1}z^{p-1} \pmod{\delta'} \\
-1 &\equiv 2^{p-1} \pmod{\delta'}
\end{aligned}$$

.....

$$\begin{aligned}
(28) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1}z^{p-1} \pmod{\delta'} \\
(y^2)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\delta'} \\
(36) \text{ より } (2^2xz)^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\delta'} \\
2^{2(p-1)}x^{p-1}z^{p-1} &\equiv -x^{p-1}z^{p-1} \pmod{\delta'} \\
(2^{p-1})^2 &\equiv -1 \pmod{\delta'}
\end{aligned}$$

.....

$$\begin{aligned}
(29) \text{ より } (z^{p-1})^2 &\equiv x^{p-1}y^{p-1} \pmod{\delta'} \\
(z^2)^{p-1} &\equiv x^{p-1}y^{p-1} \pmod{\delta'} \\
(37) \text{ より } (-2^{-1}xy)^{p-1} &\equiv x^{p-1}y^{p-1} \pmod{\delta'} \\
2^{-(p-1)}x^{p-1}y^{p-1} &\equiv x^{p-1}y^{p-1} \pmod{\delta'} \\
1 &\equiv 2^{p-1} \pmod{\delta'}
\end{aligned}$$

上式を満たす  $\delta'$  は存在しない。  
よって

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

## 1.11 $\delta' = 2$ のとき

1.11.1  $2 \mid z$  ,  $2 \perp xy$

$S^n = 2^k$  のとき

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

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

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

$$2 \mid c$$

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

$$2 \perp \gamma$$

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

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

$$2^0 = 1$$

しかし、 $\gamma + p^{(p-1)n-1} c^{p-1} > 1$  なので矛盾する。 $p \perp z$  も同様である。

よって  $2 \mid z$  のとき成り立たない。

$y + z - x$  は  $x, y$  について  $x + z - y$  と対称のため  $2 \mid y$  のときも成り立たない。  
以上より

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