Fermat's Last Theorem

Hajime Mashima

Abstract

About 380 years ago, Pierre de Fermat wrote the following idea to Diophantus's "Arithmetica".

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Later, this proposition(Fermat's Last Theorem) has continued to be a presence, such as the One Ring that appeared in J·R·R·Tolkien's "Lord of the Rings". Finally in 1994, it has been proven by Sir Andrew Wiles. However, interesting Fermat's proof is still unknown. Perhaps this is assumed to algebra category.

Contents

1 introduction

最後に残った Fermat の命題が現代数学の総力を結集し"定理"と認められて以降も、微かな火が未だ燻り続けている。それは Fermat の証明が知りたいという探求心そのものである。

Theorem 1 (Fermat's Last Theorem)

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

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

これは以下と同値である。

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

1.1 位相変換

Definition 2

$$\theta \perp xyz$$

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

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta$$

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

$$\begin{aligned} tx^{p-1} \cdot uy^{p-1} &\equiv y^p z^p \mod \theta \\ tux^{p-1} &\equiv yz^p \mod \theta \end{aligned} \tag{2}$$

$$\begin{aligned} sz^{p-1} \cdot uy^{p-1} &\equiv x^p z^p \mod \theta \\ suy^{p-1} &\equiv x^p z \mod \theta \end{aligned} \tag{3}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} \cdot uy^{p-1} &\equiv x^p y^p z^p \mod \theta \\ stu &\equiv xyz \mod \theta \end{aligned} \tag{4}$$

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

(4) より

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

(2) より

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

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

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

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

$$x^p \equiv y^{p-1}(u - y) \mod \theta \tag{5}$$

同様に

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

(4) より

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

(1) より

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

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

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

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

$$x^{p-1}(t + x) \equiv z^p \mod \theta \tag{6}$$

同様に

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

(4) より

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

(3) より

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

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

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

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

$$z^{p-1}(z - s) \equiv y^p \mod \theta \tag{7}$$

項 x^p, y^p, z^p について位相変換する $k_1, k_2, k_3(\perp \theta)$ を仮定する。つまり

$$\begin{aligned} y^p - z^p &\equiv -x^p \mod \theta \\ k_1 y^p - k_2 z^p &\equiv -k_3 x^p \mod \theta \\ x^p + y^p &\equiv z^p \mod \theta \end{aligned}$$

(5)(6)(7) より

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \mod \theta \\ (u-y)y^{p-1} + (z-s)z^{p-1} &\equiv (t+x)x^{p-1} \mod \theta \end{aligned} \tag{8}$$

$$\begin{aligned} u - y &\equiv k_1 y \mod \theta \\ u &\equiv (k_1+1)y \mod \theta \\ z - s &\equiv -k_2 z \mod \theta \\ s &\equiv (k_2+1)z \mod \theta \\ t + x &\equiv -k_3 x \mod \theta \\ t &\equiv -(k_3+1)x \mod \theta \end{aligned}$$

以下、3 式の各項は合同である。

$$\begin{aligned} x^p \quad & +y^p \quad && \equiv z^p \mod \theta \\ (k_2+1)z^p \quad & -(k_3+1)x^p \quad && \equiv (k_1+1)y^p \mod \theta \\ k_1 y^p \quad & -k_2 z^p \quad && \equiv -k_3 x^p \mod \theta \end{aligned} \tag{9}$$

$$\begin{aligned} x^p &\equiv k_1 y^p \mod \theta \\ -k_3 x^p &\equiv -k_3 k_1 y^p \mod \theta \\ (k_1+1)y^p &\equiv -k_3 k_1 y^p \mod \theta \\ (k_1+1+k_1 k_3)y^p &\equiv 0 \mod \theta \\ (k_1(k_3+1)+1)y^p &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} y^p &\equiv -k_2 z^p \mod \theta \\ k_1 y^p &\equiv -k_1 k_2 z^p \mod \theta \\ (k_2+1)z^p &\equiv -k_1 k_2 z^p \mod \theta \\ (k_2+1+k_1 k_2)z^p &\equiv 0 \mod \theta \\ (k_2(k_1+1)+1)z^p &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} z^p &\equiv -k_3 x^p \mod \theta \\ -k_2 z^p &\equiv k_2 k_3 x^p \mod \theta \\ -(k_3+1)x^p &\equiv k_2 k_3 x^p \mod \theta \\ (k_3+1+k_2 k_3)x^p &\equiv 0 \mod \theta \\ (k_3(k_2+1)+1)x^p &\equiv 0 \mod \theta \end{aligned}$$

$$
\begin{aligned}
x^p &\equiv k_1 y^p \mod \theta \\
-k_3 x^p &\equiv -k_3 k_1 y^p \mod \theta \\
z^p &\equiv -k_3 k_1 y^p \mod \theta \\
-k_2 z^p &\equiv k_3 k_2 k_1 y^p \mod \theta \\
y^p &\equiv k_1 k_2 k_3 y^p \mod \theta
\end{aligned}
$$

$$
k_1 k_2 k_3 \equiv 1 \mod \theta \tag{10}
$$

1.1.1 $k_1 \not\equiv k_2 \not\equiv k_3 \mod \theta$

個別の積 k における位相変換の考察

$$
\begin{aligned}
x^p \quad & +y^p \quad && \equiv z^p \mod \theta \\
k_1 y^p \quad & -k_2 z^p \quad && \equiv -k_3 x^p \mod \theta \\
(k_2 k_3) k_1 y^p \quad & -(k_1 k_3) k_2 z^p \quad && \equiv -(k_1 k_2) k_3 x^p \mod \theta \\
&\text{(10) より} \\
y^p \quad & -z^p \quad && \equiv -x^p \mod \theta
\end{aligned}
$$

1.1.2 $k'_1 \equiv k'_2 \equiv k'_3 \mod \theta$

共通の積 k' における位相変換の考察

$$
\begin{aligned}
x^p \quad & +y^p \quad && \equiv z^p \mod \theta \\
k_1 y^p \quad & -k_2 z^p \quad && \equiv -k_3 x^p \mod \theta \\
(k_2 k_3) k_1 y^p \quad & -k_2^2 k_3 z^p \quad && \equiv -k_2 k_3^2 x^p \mod \theta \\
&\text{(10) より} \\
y^p \quad & -k_2^2 k_3 z^p \quad && \equiv -k_2 k_3^2 x^p \mod \theta
\end{aligned}
$$

共通の積を k' と置くと

$$
\begin{aligned}
k_2'^2 k'_3 &\equiv 1 \mod \theta' \\
k'_2 k_3'^2 &\equiv 1 \mod \theta'
\end{aligned}
$$

$$
\begin{aligned}
k_2'^2 k'_3 &\equiv k'_2 k_3'^2 \mod \theta' \\
k'_2 &\equiv k'_3 \mod \theta'
\end{aligned}
$$

k'_1 も同様なので以下のようにおける。

$$
k'_1 \equiv k'_2 \equiv k'_3 \equiv k' \mod \theta'
$$

(10) より

$$
k'^3 \equiv 1 \mod \theta' \tag{11}
$$

(11) に基づいて位相変換を示す。

$$
\begin{aligned}
x^p \quad &+y^p \quad \equiv z^p \mod \theta' \\
k'y^p \quad &-k'z^p \quad \equiv -k'x^p \mod \theta' \\
&\Downarrow
\end{aligned}
$$

$$
\begin{aligned}
k'y^p &\equiv x^p \mod \theta' \\
-k'z^p &\equiv y^p \mod \theta' \\
-k'x^p &\equiv z^p \mod \theta' \\
&\circlearrowleft \\
k'x^p &\equiv -z^p \mod \theta' \\
k'y^p &\equiv x^p \mod \theta' \\
k'z^p &\equiv -y^p \mod \theta' \\
&\circlearrowleft \\
k'^2x^p &\equiv y^p \mod \theta' \\
k'^2y^p &\equiv -z^p \mod \theta' \\
k'^2z^p &\equiv -x^p \mod \theta' \\
&\circlearrowleft \\
-k' \cdot y^p &\equiv -x^p \mod \theta' \\
-k' \cdot -z^p &\equiv -y^p \mod \theta' \\
-k' \cdot -x^p &\equiv -z^p \mod \theta' \\
&\circlearrowleft \\
-k'^2 \cdot y^p &\equiv z^p \mod \theta' \\
-k'^2 \cdot -z^p &\equiv -x^p \mod \theta' \\
-k'^2 \cdot -x^p &\equiv y^p \mod \theta' \\
&\circlearrowleft \\
-k' \cdot z^p &\equiv y^p \mod \theta' \\
-k' \cdot -x^p &\equiv -z^p \mod \theta' \\
-k' \cdot y^p &\equiv -x^p \mod \theta' \\
&\circlearrowleft \\
-k'^2 \cdot z^p &\equiv x^p \mod \theta' \\
-k'^2 \cdot -x^p &\equiv y^p \mod \theta' \\
-k'^2 \cdot y^p &\equiv z^p \mod \theta'
\end{aligned}
$$

Proposition 3

$$k' \equiv 1 \mod \theta' \qquad \Rightarrow \qquad \theta' = 3 \tag{12}$$

Proof 4 $k' \equiv 1 \mod \theta' \Rightarrow$
(9) より

$$\begin{aligned} x^p &\equiv y^p \mod \theta' \\ y^p &\equiv -z^p \mod \theta' \\ z^p &\equiv -x^p \mod \theta' \end{aligned} \tag{13}$$

$$\begin{aligned} x^p + y^p &\equiv z^p \mod \theta' \\ y^p + y^p &\equiv z^p \mod \theta' \\ 2y^p &\equiv z^p \mod \theta' \end{aligned}$$

(13) より

$$2y^p \equiv -2z^p \mod \theta'$$

$$\begin{aligned} 2y^p - 2y^p &\equiv z^p + 2z^p \mod \theta' \\ 0 &\equiv 3z^p \mod \theta' \end{aligned}$$

□

(11) より以下、3 式の各項は合同である。

$$\begin{aligned} x^p \quad & +y^p \quad && \equiv z^p \mod \theta' \\ k'y^p \quad & -k'z^p \quad && \equiv -k'x^p \mod \theta' \\ k'^{3n+1}y^p \quad & -k'^{3n+1}z^p \quad && \equiv -k'^{3n+1}x^p \mod \theta' \end{aligned}$$

$$\begin{aligned} 3n + 1 &= \theta'' - 1 \Rightarrow \\ k' &\equiv 1 \mod \theta'' \end{aligned}$$

これは (12) に反する。
よって $\theta'' = 3n + 2$ の位相変換は、$k_1 \not\equiv k_2 \not\equiv k_3$ のみである。

$$3n = \theta''' - 1$$

$\theta''' = 3n + 1$ の位相変換は、$k_1 \not\equiv k_2 \not\equiv k_3$ または $k_1 \equiv k_2 \equiv k_3$ があり得る。
ただし $k' \not\equiv 1 \mod \theta'''$

1.2 $\delta \perp xyz$

Proposition 5

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

Proof 6

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

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

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

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

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

$$p^1 \mid R$$

※また p を除いた素数に関して

$$L \perp R$$

Definition 7 $p \perp abc$

- $z - y = a^p p^{p-1}$
- $z - x = b^p$
- $x + y = c^p$

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

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

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

$$p^2 \mid x \tag{14}$$

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

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

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

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \qquad (15)$$

(14) より $x = ap^2\alpha$ と置けるので

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

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

(15) ， $p \perp \alpha^p$ より

$p^1 \mid K$ でなければならない。

よって

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

一般的に

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

□

また

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

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

1.2.1 $p \mid x$

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

Proposition 8 $x + z - y = p^n aS \quad , \ \delta \mid S \ \Rightarrow \ \delta \perp xyz$

Proof 9

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

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

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

1.2.2 $p \perp x$

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

Proposition 10 $x + z - y = aS' \quad , \ \delta \mid S' \ \Rightarrow \ \delta \perp xyz$

Proof 11

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

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

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

項 x, y, z について位相変換する $m_1, m_2, m_3 (\perp \delta)$ を仮定する。つまり

$$\begin{aligned} -y \quad +z \quad &\equiv -x \mod \delta \\ -m_1 y \quad +m_2 z \quad &\equiv -m_3 x \mod \delta \\ x \quad -y \quad &\equiv -z \mod \delta \end{aligned}$$

(8) を参考にすると

$$\begin{aligned} x \quad -y \quad &\equiv -z \mod \delta \\ s'z \quad -t'x \quad &\equiv -u'y \mod \delta \\ (-u'+1)y \quad +(-1-s')z \quad &\equiv (1-t')x \mod \delta \end{aligned}$$

$$\begin{aligned} -u'+1 &\equiv -m_1 \mod \delta \\ u' &\equiv m_1 + 1 \mod \delta \\ -1-s' &\equiv m_2 \mod \delta \\ s' &\equiv -m_2 - 1 \mod \delta \\ 1-t' &\equiv -m_3 \mod \delta \\ t' &\equiv m_3 + 1 \mod \delta \end{aligned}$$

以下、3 式の各項は合同である。

$$\begin{aligned} x \quad -y \quad &\equiv -z \mod \delta \\ (-m_2-1)z \quad -(m_3+1)x \quad &\equiv -(m_1+1)y \mod \delta \\ -m_1 y \quad +m_2 z \quad &\equiv -m_3 x \mod \delta \end{aligned}$$

$$\begin{aligned} x &\equiv -m_1 y \mod \delta \\ m_3 x &\equiv -m_3 m_1 y \mod \delta \\ (m_1+1)y &\equiv -m_1 m_3 y \mod \delta \\ (m_1+1+m_1 m_3)y &\equiv 0 \mod \delta \end{aligned}$$

$$\begin{aligned} -y &\equiv m_2 z \mod \delta \\ -m_1 y &\equiv m_1 m_2 z \mod \delta \\ (-m_2-1)z &\equiv m_1 m_2 z \mod \delta \\ (m_2+1+m_1 m_2)z &\equiv 0 \mod \delta \end{aligned} \tag{16}$$

$$\begin{aligned} -z &\equiv -m_3 x \mod \delta \\ -m_2 z &\equiv -m_2 m_3 x \mod \delta \\ (m_3+1)x &\equiv -m_2 m_3 x \mod \delta \\ (m_3+1+m_2 m_3)x &\equiv 0 \mod \delta \end{aligned}$$

(16) より

$$\begin{aligned} -y &\equiv m_2 z \mod \delta \\ -m_3 m_1 y &\equiv m_1 m_2 m_3 z \mod \delta \\ m_3 x &\equiv m_1 m_2 m_3 z \mod \delta \\ z &\equiv m_1 m_2 m_3 z \mod \delta \end{aligned}$$

$$m_1 m_2 m_3 \equiv 1 \mod \delta \tag{17}$$

1.2.3 $m_1 \equiv m_2 \equiv m_3 \mod \delta$

共通の積 m' による位相変換が可能とすると (17) より

$$\begin{aligned} m'_1 \equiv m'_2 \equiv m'_3 \equiv m' \mod \delta' \\ m'^3 \equiv 1 \mod \delta \end{aligned} \tag{18}$$

(16) より

$$\begin{aligned} m'x &\equiv -m'^2 y \mod \delta \\ -m'y &\equiv m'^2 z \mod \delta \\ -m'z &\equiv -m'^2 x \mod \delta \end{aligned}$$

であるから (18) より

$$\begin{aligned} m'x &\equiv m'^3 z \equiv z \mod \delta \\ -m'y &\equiv m'^3 x \equiv x \mod \delta \\ -m'z &\equiv m'^3 y \equiv y \mod \delta \end{aligned}$$

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

(16) より

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

(9) より

$$\begin{aligned} m'^p \equiv k' \mod \delta' \Rightarrow \\ x^p \equiv k' y^p \equiv -k' y^p \mod \delta' \end{aligned}$$

$$\begin{aligned} m'^p \equiv -k' \mod \delta' \Rightarrow \\ y^p \equiv -k' z^p \equiv k' z^p \mod \delta' \end{aligned}$$

これは前提に反する。よって共通の積 m' による位相変換はできない。

1.3 解の条件

1.3.1 $m_1 \not\equiv m_2 \not\equiv m_3 \mod \delta$

U , T について満たすべき解を考察する。

$$x^p + Uz^{p-1} \equiv Ty^{p-1} \mod \theta \tag{19}$$

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

$$\begin{aligned}
Uz^{p-1} \cdot Ty^{p-1} &\equiv y^p z^p \mod \theta \\
UT &\equiv yz \mod \theta
\end{aligned} \tag{20}$$

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

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 (19)(20) $\Rightarrow$

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

U' , T' について満たすべき解を考察する。

$$U'y^{p-1} + T'x^{p-1} \equiv z^p \mod \theta \tag{21}$$

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

$$\begin{aligned} U'y^{p-1} \cdot T'x^{p-1} &\equiv x^p y^p \mod \theta \\ U'T' &\equiv xy \mod \theta \end{aligned} \tag{22}$$

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

同様に

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

よって (21)(22) $\Rightarrow$

$$\begin{aligned} U'y^{p-1} &\equiv x^p \mod \theta \\ T'x^{p-1} &\equiv y^p \mod \theta \\ &or \\ U'y^{p-1} &\equiv y^p \mod \theta \\ T'x^{p-1} &\equiv x^p \mod \theta \end{aligned}$$

$$\begin{aligned} x \quad -y \quad &\equiv -z \mod \delta \\ -m_1 y \quad +m_2 z \quad &\equiv -m_3 x \mod \delta \end{aligned}$$

$$\begin{aligned} -m_1^p y^p &\equiv x^p \mod \delta \\ -m_2^p z^p &\equiv y^p \mod \delta \\ m_3^p x^p &\equiv z^p \mod \delta \end{aligned}$$

$$\begin{aligned} -m_1^p y^p x^{-(p-1)} &\equiv x \mod \delta \\ -m_2^p z^p y^{-(p-1)} &\equiv y \mod \delta \\ m_3^p x^p z^{-(p-1)} &\equiv z \mod \delta \end{aligned}$$

$$\begin{aligned} x \quad &+z \quad &&\equiv y \mod \delta \\ -m_1^p y^p x^{-(p-1)} \quad &+m_3^p x^p z^{-(p-1)} \quad &&\equiv -m_2^p z^p y^{-(p-1)} \mod \delta \\ -m_1^p y^p \quad &+m_3^p x^p z^{-(p-1)} \cdot x^{p-1} \quad &&\equiv -m_2^p z^p y^{-(p-1)} \cdot x^{p-1} \mod \delta \\ x^p \quad &+z^p z^{-(p-1)} \cdot x^{p-1} \quad &&\equiv y^p y^{-(p-1)} \cdot x^{p-1} \mod \delta \\ x^p \quad &+(z \cdot z^{-(p-1)} \cdot x^{p-1}) z^{p-1} \quad &&\equiv (y \cdot y^{-(p-1)} \cdot x^{p-1}) y^{p-1} \mod \delta \end{aligned}$$

(19)(20) より

$$\begin{aligned} (y \cdot y^{-(p-1)} \cdot x^{p-1})(z \cdot z^{-(p-1)} \cdot x^{p-1}) &\equiv yz \mod \delta \\ y^{-(p-1)} z^{-(p-1)} x^{2(p-1)} &\equiv 1 \mod \delta \\ \left(x^{p-1}\right)^2 &\equiv y^{p-1} z^{p-1} \mod \delta \quad (23) \end{aligned}$$

$$\begin{aligned} x \quad &+z \quad &&\equiv y \mod \delta \\ -m_1^p y^p x^{-(p-1)} \quad &+m_3^p x^p z^{-(p-1)} \quad &&\equiv -m_2^p z^p y^{-(p-1)} \mod \delta \\ -m_1^p y^p x^{-(p-1)} \cdot y^{p-1} \quad &+m_3^p x^p z^{-(p-1)} \cdot y^{p-1} \quad &&\equiv -m_2^p z^p \mod \delta \\ x^p x^{-(p-1)} \cdot y^{p-1} \quad &+z^p z^{-(p-1)} \cdot y^{p-1} \quad &&\equiv y^p \mod \delta \\ (x \cdot x^{-(p-1)} \cdot y^{p-1}) x^{p-1} \quad &+(z \cdot z^{-(p-1)} \cdot y^{p-1}) z^{p-1} \quad &&\equiv y^p \mod \delta \end{aligned}$$

(19)(20) を参考に

$$\begin{aligned} -(z \cdot z^{-(p-1)} \cdot y^{p-1})(x \cdot x^{-(p-1)} \cdot y^{p-1}) &\equiv zx \mod \delta \\ -z^{-(p-1)} x^{-(p-1)} \cdot y^{2(p-1)} &\equiv 1 \mod \delta \\ \left(y^{p-1}\right)^2 &\equiv -x^{p-1} z^{p-1} \mod \delta \quad (24) \end{aligned}$$

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

(23)(24)(25) より

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

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

よって

$$L \equiv 0 \mod \delta \quad or \quad R \equiv 0 \mod \delta$$

1.3.2 $R \equiv 0 \mod \delta$

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

(21)(22) より

$$\begin{aligned}
-z^2 &\equiv xy \mod \delta \\
z^2 &\equiv -xy \mod \delta
\end{aligned}$$

(25) より

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

これは前提に反する。

1.3.3 $L \equiv 0 \mod \delta$

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

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

$$
zx^{p-1} + 2zy^{p-1} \equiv z^p \mod \delta
$$

(21)(22) より

$$
2z^2 \equiv xy \mod \delta
$$

(25) より

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

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

(19)(20) より

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

(23) より

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

よって

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

これは前提に反する。