Fermat's Last Theorem

Hajime Mashima

January 20, 2019

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。

1.1 Fermat's Last Theorem

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。

$$x^p + y^p \neq z^p \quad (p \text{ は } 3 \text{ 以上の素数で } x \ , \ y \ , \ z \text{ は互いに素})$$

1.2 Structure of the product

Theorem 2 (Fermat's little theorem) A を自然数、p が素数で $p \perp A$ のとき

$$A^{p-1} \equiv 1 \pmod{p} \tag{1}$$

$$\begin{aligned} x^p + y^p - z^p &\equiv 0 \mod p \\ x^{p-1}x + y^{p-1}y - z^{p-1}z &\equiv 0 \mod p \\ (1) \text{ より} \qquad x + y - z &\equiv 0 \mod p \end{aligned}$$

Definition 3 $p \perp xyz$ における The Barlow-Abel Equations[1, p.45]。

- $x^p + y^p = (x + y) \cdot \gamma^p$
- $z^p - y^p = (z - y) \cdot \alpha^p$
- $z^p - x^p = (z - x) \cdot \beta^p$

$$L = \{(x + y), (z - y), (z - x)\} \quad , \quad R = \{\gamma^p, \alpha^p, \beta^p\}$$

以降用いる k は適当な整数とする。

Proposition 4 $p \perp xyz$ のとき

$$R \equiv 1 \mod p$$

Proof 5 $p = 5$ を例とする。

$$\begin{aligned} (y + (z - y))^5 &= y^5 + 5y^4(z - y) + 10y^3(z - y)^2 + 10y^2(z - y)^3 + 5y(z - y)^4 + (z - y)^5 \\ z^5 &= y^5 + 5y^4(z - y) + 10y^3(z - y)^2 + 10y^2(z - y)^3 + 5y(z - y)^4 + (z - y)^5 \end{aligned}$$

$$z^5 - y^5 = (z - y)(5y^4 + 10y^3(z - y) + 10y^2(z - y)^2 + 5y(z - y)^3 + (z - y)^4) \tag{2}$$

$$\begin{aligned} (-y + (x + y))^5 &= -y^5 + 5y^4(x + y) - 10y^3(x + y)^2 + 10y^2(x + y)^3 - 5y(x + y)^4 + (x + y)^5 \\ x^5 &= -y^5 + 5y^4(x + y) - 10y^3(x + y)^2 + 10y^2(x + y)^3 - 5y(x + y)^4 + (x + y)^5 \end{aligned}$$

$$x^5 + y^5 = (x + y)(5y^4 - 10y^3(x + y) + 10y^2(x + y)^2 - 5y(x + y)^3 + (x + y)^4)$$

他の素数についても同様なので一般的に

$$(z-y)^{p-1} \equiv (x+y)^{p-1} \equiv R \equiv 1 \mod p$$

□

Proposition 6 $p \perp xyz$ のとき

$$L \perp R \tag{3}$$

Proof 7 $x^p + y^p = L \cdot R$ において、$(x+y)$ の約数 c' を置くと

$$L \equiv 0 \mod c'$$
$$R \equiv py^{p-1} \mod c'$$

$c' \perp py$ なので

$$L \perp R \equiv py^{p-1} \mod c'$$

$z^p - x^p$、$z^p - y^p$ についても同様である。 □

Proposition 8 $q \mid R$ のとき (q は p でない素数)

$$q \equiv 1 \mod p \quad (q \neq p) \tag{4}$$

Proof 9 $q \not\equiv 1 \mod p \quad (q \neq p)$ と仮定する。

$q \mid x^p$ のとき、q を法とする y, z の余り $g, h(< q)$ を置く。

$$y \equiv g \mod q$$
$$z \equiv h \mod q$$
$$z - y \equiv h - g \mod q$$

(3) より

$$g \not\equiv h \mod q \tag{5}$$

$$y^p = (q\mathbb{N}_1 + g)^p$$
$$z^p = (q\mathbb{N}_2 + h)^p$$

$z^p - y^p = x^p$ だから

$$(q\mathbb{N}_1 + g)^p \equiv (q\mathbb{N}_2 + h)^p \mod q \tag{6}$$

$q \perp zy$ なので Fermat's little theorem より

$$(q\mathbb{N}_1 + g)^{q-1} \equiv (q\mathbb{N}_2 + h)^{q-1} \mod q \tag{7}$$

$q \not\equiv 1 \mod p$ なので

$$q - 1 = p\mathbb{N} + k \quad (0 < k < p)$$
$$(q-1)k^{p-2} = p\mathbb{N} \cdot k^{p-2} + k^{p-1}$$

$p \perp k$ であるから Fermat's little theorem より

$$(q-1)k^{p-2} \equiv 1 \mod p$$

(7) より

$$(q\mathbb{N}_1 + g)^{(q-1)k^{p-2}} \equiv (q\mathbb{N}_2 + h)^{(q-1)k^{p-2}} \mod q$$

$(q-1)k^{p-2} = pm + 1$ と置けるので

$$(q\mathbb{N}_1 + g)^{pm+1} \equiv (q\mathbb{N}_2 + h)^{pm+1} \mod q \tag{8}$$

(6) より

$$(q\mathbb{N}_1 + g)^{pm} \equiv (q\mathbb{N}_2 + h)^{pm} \mod q \tag{9}$$

(8) , (9) より

$$(q\mathbb{N}_1 + g) \equiv (q\mathbb{N}_2 + h) \mod q$$

$$g \equiv h \mod q$$

これは (5) に反する。

□

1.3 Case 1 $(p \perp xyz)$

Proposition 10 $x^p + y^p = z^p \quad \Rightarrow \quad p^2 \mid (x + y - z)$

Proof 11

(4) より

$$R = q_1^p \cdot q_2^p \cdot q_3^p \cdots$$

$$\begin{aligned} q_n^p &= (pk+1)^p \\ q_n^p &= (pk)^p + p^2(\ldots) + 1 \\ q_n^p &\equiv 1 \mod p^2 \end{aligned}$$

よって

$$\begin{aligned} R &\equiv 1 \mod p^2 \\ x^p + y^p - z^p &\equiv 0 \mod p^2 \end{aligned} \tag{10}$$

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

(10) より

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

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

□

1.3.1 $p = 3$

Proposition 12 $x^3 + y^3 = z^3 \Rightarrow 3 \mid xyz$

Proof 13

$$
\begin{aligned}
(x + (y - z))^3 &= x^3 + 3x^2(y - z) + 3x(y - z)^2 + (y - z)^3 \\
(x + y - z)^3 &= x^3 + 3x^2y - 3x^2z + 3x(y^2 - 2yz + z^2) + y^3 - 3y^2z + 3yz^2 - z^3 \\
&= x^3 + 3x^2y - 3x^2z + 3xy^2 - 6xyz + 3xz^2 + y^3 - 3y^2z + 3yz^2 - z^3 \\
&= x^3 + 3x^2y + 3xy^2 + 3xz^2 + y^3 + 3yz^2 - 3x^2z - 6xyz - 3y^2z - z^3
\end{aligned}
$$

$x^3 + y^3 - z^3 = 0$ なので

$$
\begin{aligned}
&= 3x^2y + 3xy^2 + 3xz^2 + 3yz^2 - 3x^2z - 6xyz - 3y^2z \\
&= 3\left(x^2y + xy^2 + xz^2 + yz^2 - x^2z - 2xyz - y^2z\right) \\
&= 3\left(xy\left(x + y\right) + z^2\left(x + y\right) - z\left(x^2 + 2xy + y^2\right)\right) \\
&= 3\left(xy\left(x + y\right) + z^2\left(x + y\right) - z\left(x + y\right)^2\right) \\
&= 3(x + y)\left(xy + z^2 - z\left(x + y\right)\right) \\
(x + y - z)^3 &= 3(x + y)(z - x)(z - y)
\end{aligned}
$$

$3^3 \mid (x + y - z)^3$ なので

$$3^2 \mid (x + y)(z - x)(z - y)$$

$$x + y - z \equiv 0 \mod 3 \text{ であるから}$$

$$
\begin{aligned}
x + y &\equiv z \mod 3 \\
z - x &\equiv y \mod 3 \\
z - y &\equiv x \mod 3
\end{aligned}
$$

よって

$$3 \mid xyz$$

□

1.3.2 $p \geqq 5$

Proposition 14 $x^p + y^p \neq z^p$

Proof 15

Definition 16

- $\theta \mid x + y - z$
- $\theta \perp xyz$
- $\theta \perp 2$

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

$$x^p + sz^{p-1} \equiv ty^{p-1} \mod \theta$$

ここで s , t を変数とするとき満たすべき解を考察する。

$$\begin{aligned}
x^p + sz^{p-1} &\equiv ty^{p-1} \mod \theta \\
z^p - y^p + sz^{p-1} &\equiv ty^{p-1} \mod \theta \\
z^p + sz^{p-1} &\equiv y^p + ty^{p-1} \mod \theta \\
z^{p-1}(z+s) &\equiv y^{p-1}(y+t) \mod \theta \\
z^{p-1}(zy+sy) &\equiv yy^{p-1}(y+t) \mod \theta
\end{aligned}$$

$yz \equiv st \mod \theta$ より

$$\begin{aligned}
z^{p-1}(st+sy) &\equiv y^p(y+t) \mod \theta \\
sz^{p-1}(y+t) &\equiv y^p(y+t) \mod \theta
\end{aligned}$$

同様に

$$\begin{aligned}
z^p(z+s) &\equiv y^{p-1}(zy+zt) \mod \theta \\
z^p(z+s) &\equiv y^{p-1}(st+zt) \mod \theta \\
z^p(z+s) &\equiv ty^{p-1}(z+s) \mod \theta
\end{aligned}$$

よって $yz \equiv st \mod \theta$ ならば、定義域において以下の合同式を満たす。

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

ただし $\theta \perp x$ より $y^p \not\equiv z^p \mod \theta$

$$s \not\equiv z \mod \theta \quad , \quad t \not\equiv y \mod \theta$$

ここで以下の仮定をする。

$$yz \equiv 1 \cdot k_1 \cdot k_2 \mod \theta \quad , (1 < k_1 \leqq k_2 < \theta) \tag{11}$$

ところで

Proposition 17 s , t を満たす解 s_1 , t_1 と s_2 , t_2 が存在するとき、
$sz^{p-1} \equiv y^p \mod \theta$, $z^p \equiv ty^{p-1} \mod \theta$ ならば、それらは合同である。

$$s_1 \equiv s_2 \mod \theta \quad , t_1 \equiv t_2 \mod \theta$$

仮定を当てはめると

$$\begin{cases} s_1 \equiv 1 \mod \theta \\ t_1 \equiv k_1 \cdot k_2 \mod \theta \end{cases}$$

$$\begin{cases} s_2 \equiv k_1 \mod \theta \\ t_2 \equiv k_2 \mod \theta \end{cases}$$

しかし (11) より $s_1 \not\equiv s_2 \mod \theta$

よって $yz \equiv 1 \cdot k \mod \theta$ でなければならないので

$$\begin{cases} s \equiv 1 \mod \theta \\ t \equiv yz \mod \theta \end{cases}$$

$\wedge$

$$\begin{cases} s \equiv -yz \mod \theta \\ t \equiv -1 \mod \theta \end{cases}$$

$$yz \equiv -1 \mod \theta \tag{12}$$

また同様に

$$xz \equiv -1 \mod \theta \tag{13}$$

Remark 18 θ が奇数ならば $(s \not\equiv 1 \wedge -1 \mod \theta)$ なので $(s \equiv 1 \vee -1 \mod \theta)$
, $(t \equiv -1 \vee 1 \mod \theta)$ として考える。

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

$$\begin{cases} s \equiv y \mod \theta \\ t \equiv z \mod \theta \end{cases}$$

$$\begin{cases} y \equiv 1 \mod \theta \\ z \equiv -1 \mod \theta \end{cases}$$

よって $yz \equiv 1 \cdot k \mod \theta$ を満たしている。

$$x^p y^{-(p-1)} \equiv -t \mod \theta \quad , \quad y^p x^{-(p-1)} \equiv s \mod \theta$$

$$-ty^{p-1} + sx^{p-1} \equiv z^p \mod \theta$$

ここで s , t を変数とするとき満たすべき解を考察する。

$$\begin{aligned}
-ty^{p-1} + sx^{p-1} &\equiv z^p \mod \theta \\
-ty^{p-1} + sx^{p-1} &\equiv x^p + y^p \mod \theta \\
-x^p + sx^{p-1} &\equiv y^p + ty^{p-1} \mod \theta \\
-x^{p-1}(x-s) &\equiv y^{p-1}(y+t) \mod \theta \\
-x^{p-1}(xy - sy) &\equiv yy^{p-1}(y+t) \mod \theta
\end{aligned}$$

$xy \equiv -st \mod \theta$ より

$$\begin{aligned}
-x^{p-1}(-st - sy) &\equiv y^p(y+t) \mod \theta \\
sx^{p-1}(y+t) &\equiv y^p(y+t) \mod \theta
\end{aligned}$$

同様に

$$\begin{aligned}
-x^p(x-s) &\equiv y^{p-1}(xy + xt) \mod \theta \\
-x^p(x-s) &\equiv y^{p-1}(-st + xt) \mod \theta \\
-x^p(x-s) &\equiv ty^{p-1}(x-s) \mod \theta
\end{aligned}$$

よって $xy \equiv -st \mod \theta$ であるならば、定義域の範囲で以下の合同式を満たす。

$$\begin{aligned}
sx^{p-1} &\equiv y^p \mod \theta \\
-x^p &\equiv ty^{p-1} \mod \theta
\end{aligned}$$

ただし $\theta \perp z$ より $-x^p \not\equiv y^p \mod \theta$

$$s \not\equiv -x \mod \theta \quad , \quad t \not\equiv y \mod \theta$$

Remark 19

$sx^{p-1} \cdot 0 \equiv y^p \cdot 0 \mod \theta$ および $-x^p \cdot 0 \equiv ty^{p-1} \cdot 0 \mod \theta$ となる条件でも
$xy \equiv -st \mod \theta$ であり、p.10 が成り立つ。

ここで以下の仮定をする。

$$xy \equiv 1 \cdot k_1 \cdot k_2 \mod \theta \quad , (1 < k_1 \leqq k_2 < \theta) \tag{14}$$

ところで

Proposition 20 s , t を満たす解 s_1 , t_1 と s_2 , t_2 が存在するとき、
$sx^{p-1} \equiv y^p \mod \theta$, $-x^p \equiv ty^{p-1} \mod \theta$ ならば、それらは合同である。

$$s_1 \equiv s_2 \mod \theta \quad , t_1 \equiv t_2 \mod \theta$$

仮定を当てはめると

$$\begin{cases} s_1 \equiv 1 \mod \theta \\ t_1 \equiv k_1 \cdot k_2 \mod \theta \end{cases}$$

$$\begin{cases} s_2 \equiv k_1 \mod \theta \\ t_2 \equiv k_2 \mod \theta \end{cases}$$

しかし (14) より $s_1 \not\equiv s_2 \mod \theta$

よって $xy \equiv 1 \cdot k \mod \theta$ でなければならないので

$$\begin{cases} s \equiv 1 \mod \theta \\ t \equiv -xy \mod \theta \end{cases}$$

$\wedge$

$$\begin{cases} s \equiv xy \mod \theta \\ t \equiv -1 \mod \theta \end{cases}$$

$$xy \equiv 1 \mod \theta \tag{15}$$

Remark 21 θ が奇数ならば $(s \not\equiv 1 \wedge -1 \mod \theta)$ なので $(s \equiv 1 \vee -1 \mod \theta)$
, $(t \equiv -1 \vee 1 \mod \theta)$ として考える。

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

$$\begin{cases} s \equiv y \mod \theta \\ t \equiv -x \mod \theta \end{cases}$$

$$\begin{cases} y \equiv 1 \mod \theta \\ x \equiv 1 \mod \theta \end{cases}$$

よって $xy \equiv 1 \cdot k \mod \theta$ を満たしている。

(12)(13) より

$$\begin{aligned} yz &\equiv xz \mod \theta \\ y &\equiv x \mod \theta \\ x - y &\equiv 0 \mod \theta \end{aligned}$$

(12)(15) より

$$\begin{aligned} yz &\equiv -xy \mod \theta \\ z &\equiv -x \mod \theta \\ z + x &\equiv 0 \mod \theta \end{aligned}$$

(13)(15) より

$$\begin{aligned} xz &\equiv -xy \mod \theta \\ z &\equiv -y \mod \theta \\ z + y &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} (x + y - z) + (x - y) + (z + x) &\equiv 0 \mod \theta \\ (x + y - z) + (2x - y + z) &\equiv 0 \mod \theta \\ 3x &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} (x + y - z) + (y - x) + (z + y) &\equiv 0 \mod \theta \\ (x + y - z) + (-x + 2y + z) &\equiv 0 \mod \theta \\ 3y &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} -(x + y - z) + (z + x) + (z + y) &\equiv 0 \mod \theta \\ -(x + y - z) + (x + y + 2z) &\equiv 0 \mod \theta \\ 3z &\equiv 0 \mod \theta \end{aligned}$$

よって

$$\theta = p \ (\geqq 5) \ \Rightarrow \ p \mid xyz$$

これは $p \perp xyz$ の前提に反する。 □

1.4 Case 2 $(p \mid xyz)$

Proposition 22

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

Proof 23

$p \mid x \quad , \quad p \mid (z-y)$ と仮定する。(2) から、一般的に

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

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

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

$$p^1 \mid R$$

よって p を除き、x^p の L と R は互いに素なので $p \perp abc$ と置くと

Definition 24

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

$$p \mid (x + y - z)$$

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

$p \mid L \Leftrightarrow p \mid R$ なので、$b^p - c^p$ は少なくとも p^2 の積を有する。

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

$$p^2 \mid x \tag{16}$$

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

$x^p = (z-y)p\alpha^p$ と置き、上式に代入する。

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

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \qquad (17)$$

(16) より $x = ap^2\alpha$ と置けるので

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

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

(17) ， $p \perp \alpha^p$ 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

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

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

1.4.1 $p \mid x(or\ y)$

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

Proposition 25 $x + z - y = p^n aS \quad , \ \delta \mid S \ \Rightarrow \ \delta \perp xyz$

Proof 26

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

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

$\delta \mid S \quad , \delta \mid a$ ならば $\delta \mid \alpha$ でなければならず矛盾する。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 $\delta \perp \gamma$ □

Proposition 27 $2p \mid x$ ， $2p \perp yz$ のとき $x^p + y^p \neq z^p$

Proof 28

Definition 29

- $\delta \mid x + z - y$
- $\delta \perp xyz$

$y^p z^{-(p-1)} \equiv s \mod \delta$ ， $z^p y^{-(p-1)} \equiv t \mod \delta$

$$x^p + sz^{p-1} \equiv ty^{p-1} \mod \delta$$

ここで s ， t を変数とするとき満たすべき解を考察する。

$$\begin{aligned}
x^p + sz^{p-1} &\equiv ty^{p-1} \mod \delta \\
z^p - y^p + sz^{p-1} &\equiv ty^{p-1} \mod \delta \\
z^p + sz^{p-1} &\equiv y^p + ty^{p-1} \mod \delta \\
z^{p-1}(z+s) &\equiv y^{p-1}(y+t) \mod \delta \\
z^{p-1}(zy+sy) &\equiv yy^{p-1}(y+t) \mod \delta
\end{aligned}$$

$yz \equiv st \mod \delta$ より

$$\begin{aligned}
z^{p-1}(st+sy) &\equiv y^p(y+t) \mod \delta \\
sz^{p-1}(y+t) &\equiv y^p(y+t) \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
z^p(z+s) &\equiv y^{p-1}(zy+zt) \mod \delta \\
z^p(z+s) &\equiv y^{p-1}(st+zt) \mod \delta \\
z^p(z+s) &\equiv ty^{p-1}(z+s) \mod \delta
\end{aligned}$$

よって $yz \equiv st \mod \delta$ ならば、定義域において以下の合同式を満たす。

$$\begin{aligned}
sz^{p-1} &\equiv y^p \mod \delta \\
z^p &\equiv ty^{p-1} \mod \delta
\end{aligned}$$

ただし $\delta \perp x$ より $y^p \not\equiv z^p \mod \delta$

$$s \not\equiv z \mod \delta \quad , \ t \not\equiv y \mod \delta$$

ここで以下の仮定をする。

$$yz \equiv 1 \cdot k_1 \cdot k_2 \mod \delta \quad , (1 < k_1 \leqq k_2 < \delta) \tag{18}$$

ところで

Proposition 30 s , t を満たす解 s_1 , t_1 と s_2 , t_2 が存在するとき、
$sz^{p-1} \equiv y^p \mod \delta$, $z^p \equiv ty^{p-1} \mod \delta$ ならば、それらは合同である。

$$s_1 \equiv s_2 \mod \delta \quad , t_1 \equiv t_2 \mod \delta$$

仮定を当てはめると

$$\begin{cases} s_1 \equiv 1 \mod \delta \\ t_1 \equiv k_1 \cdot k_2 \mod \delta \end{cases}$$

$$\begin{cases} s_2 \equiv k_1 \mod \delta \\ t_2 \equiv k_2 \mod \delta \end{cases}$$

しかし (18) より $s_1 \not\equiv s_2 \mod \delta$

よって $yz \equiv 1 \cdot k \mod \delta$ でなければならないので

$$\begin{cases} s \equiv 1 \mod \delta \\ t \equiv yz \mod \delta \end{cases}$$

$\wedge$

$$\begin{cases} s \equiv -yz \mod \delta \\ t \equiv -1 \mod \delta \end{cases}$$

Remark 31 δ は奇数だから $(s \not\equiv 1 \wedge -1 \mod \delta)$ なので $(s \equiv 1 \vee -1 \mod \delta)$
, $(t \equiv -1 \vee 1 \mod \delta)$ として考える。

$$yz \equiv -1 \mod \delta \tag{19}$$

また同様に

$$xz \equiv -1 \mod \delta \tag{20}$$

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

$$\begin{cases} s \equiv y \mod \delta \\ t \equiv z \mod \delta \end{cases}$$

$$\begin{cases} y \equiv 1 \mod \delta \\ z \equiv -1 \mod \delta \end{cases}$$

よって $yz \equiv 1 \cdot k \mod \delta$ を満たしている。

$$x^p y^{-(p-1)} \equiv -t \mod \delta \quad , \quad y^p x^{-(p-1)} \equiv s \mod \delta$$

$$-ty^{p-1} + sx^{p-1} \equiv z^p \mod \delta$$

ここで s , t を変数とするとき満たすべき解を考察する。

$$\begin{aligned}
-ty^{p-1} + sx^{p-1} &\equiv z^p \mod \delta \\
-ty^{p-1} + sx^{p-1} &\equiv x^p + y^p \mod \delta \\
-x^p + sx^{p-1} &\equiv y^p + ty^{p-1} \mod \delta \\
-x^{p-1}(x-s) &\equiv y^{p-1}(y+t) \mod \delta \\
-x^{p-1}(xy - sy) &\equiv yy^{p-1}(y+t) \mod \delta
\end{aligned}$$

$xy \equiv -st \mod \delta$ より

$$\begin{aligned}
-x^{p-1}(-st - sy) &\equiv y^p(y+t) \mod \delta \\
sx^{p-1}(y+t) &\equiv y^p(y+t) \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
-x^p(x-s) &\equiv y^{p-1}(xy + xt) \mod \delta \\
-x^p(x-s) &\equiv y^{p-1}(-st + xt) \mod \delta \\
-x^p(x-s) &\equiv ty^{p-1}(x-s) \mod \delta
\end{aligned}$$

よって $xy \equiv -st \mod \delta$ であるならば、定義域の範囲で以下の合同式を満たす。

$$\begin{aligned}
sx^{p-1} &\equiv y^p \mod \delta \\
-x^p &\equiv ty^{p-1} \mod \delta
\end{aligned}$$

ただし $\delta \perp z$ より $-x^p \not\equiv y^p \mod \delta$

$$s \not\equiv -x \mod \delta \quad , \quad t \not\equiv y \mod \delta$$

ここで以下の仮定をする。

$$xy \equiv 1 \cdot k_1 \cdot k_2 \mod \delta \quad , (1 < k_1 \leqq k_2 < \delta) \tag{21}$$

ところで

Proposition 32 s , t を満たす解 s_1 , t_1 と s_2 , t_2 が存在するとき、
$sx^{p-1} \equiv y^p \mod \delta$, $-x^p \equiv ty^{p-1} \mod \delta$ ならば、それらは合同である。

$$s_1 \equiv s_2 \mod \delta \quad , t_1 \equiv t_2 \mod \delta$$

仮定を当てはめると

$$\begin{cases} s_1 \equiv 1 \mod \delta \\ t_1 \equiv k_1 \cdot k_2 \mod \delta \end{cases}$$

$$\begin{cases} s_2 \equiv k_1 \mod \delta \\ t_2 \equiv k_2 \mod \delta \end{cases}$$

しかし (21) より $s_1 \not\equiv s_2 \mod \delta$

よって $xy \equiv 1 \cdot k \mod \delta$ でなければならないので

$$\begin{cases} s \equiv 1 \mod \delta \\ t \equiv -xy \mod \delta \end{cases}$$

$\wedge$

$$\begin{cases} s \equiv xy \mod \delta \\ t \equiv -1 \mod \delta \end{cases}$$

Remark 33 δ は奇数だから $(s \not\equiv 1 \wedge -1 \mod \delta)$ なので $(s \equiv 1 \vee -1 \mod \delta)$
, $(t \equiv -1 \vee 1 \mod \delta)$ として考える。

$$xy \equiv 1 \mod \delta \tag{22}$$

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

$$\begin{cases} s \equiv y \mod \delta \\ t \equiv -x \mod \delta \end{cases}$$

$$\begin{cases} y \equiv 1 \mod \delta \\ x \equiv 1 \mod \delta \end{cases}$$

よって $xy \equiv 1 \cdot k \mod \delta$ を満たしている。

(19)(22) より

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

これは $\delta \perp y$ に反する。

よって $S = 2^k$

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

・$2 \mid x$ ， $2 \perp yz$ のとき

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

$$\begin{aligned} &2 \mid L = p^{pn-1} a^p \\ &2 \mid a \end{aligned}$$

$$\begin{aligned} &2 \perp R = p\alpha^p \\ &2 \perp \alpha \end{aligned}$$

$$\begin{aligned} x + z - y &= p^n a(\alpha + p^{(p-1)n-1} a^{p-1}) \\ 2^k &= \alpha + p^{(p-1)n-1} a^{p-1} \\ 2^k &= 1 \end{aligned}$$

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

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

Proposition 34 $x + y + z = cT \quad , \ \epsilon \mid T \ \Rightarrow \ \epsilon \perp xyz$

Proof 35

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

$$\gamma \perp c$$

$\epsilon \mid T \quad , \ \epsilon \mid c$ ならば $\epsilon \mid \gamma$ でなければならず矛盾する。よって

$$\epsilon \perp z$$

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

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

$$\epsilon \perp ab$$

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

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

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

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

よって $\epsilon \perp \beta$

$\epsilon \mid \alpha \quad , \ \epsilon \mid y + z$ ならば同様に

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

よって $\epsilon \perp \alpha$ □

Proposition 36 $p \mid x$ ， $p \perp yz$ ， $2 \mid z$ ， $2 \perp xy$ のとき $x^p + y^p \neq z^p$

Proof 37

p.15〜p.18 と同様。

(20)(22) より

$$\begin{aligned} xz &\equiv -xy \mod \epsilon \\ z &\equiv -y \mod \epsilon \\ z + y &\equiv 0 \mod \epsilon \end{aligned}$$

これは $\epsilon \perp x$ に反する。

よって $T = 2^k$

$$x + y + z = c2^k$$

・$2 \mid z$ ， $2 \perp xy$ のとき

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

$$\begin{aligned} &2 \mid L = c^p \\ &2 \mid c \end{aligned}$$

$$\begin{aligned} &2 \perp R = \gamma^p \\ &2 \perp \gamma \end{aligned}$$

$$\begin{aligned} x + y + z &= c(c^{p-1} + \gamma) \\ 2^k &= c^{p-1} + \gamma \\ 2^k &= 1 \end{aligned}$$

しかし、$c^{p-1} + \gamma > 1$ なので矛盾する。 □

1.4.2 $p \mid z$

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

Proposition 38 $z + x + y = p^n cS \quad , \quad \delta \mid S \;\Rightarrow\; \delta \perp xyz$

Proof 39

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

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

$\delta \mid S \quad , \quad \delta \mid c$ ならば $\delta \mid \gamma$ でなければならず矛盾する。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 $\delta \mid z + x$

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

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

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

よって $\delta \perp \beta$

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

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

よって $\delta \perp \alpha$ □

Proposition 40 $2p \mid z$ ， $2p \perp xy$ のとき $x^p + y^p \neq z^p$

Proof 41

Definition 42

- $\delta \mid z + x + y$
- $\delta \perp xyz$

$y^p z^{-(p-1)} \equiv s \mod \delta$ ， $z^p y^{-(p-1)} \equiv t \mod \delta$

$$x^p + sz^{p-1} \equiv ty^{p-1} \mod \delta$$

ここで s ， t を変数とするとき満たすべき解を考察する。

$$\begin{aligned}
x^p + sz^{p-1} &\equiv ty^{p-1} \mod \delta \\
z^p - y^p + sz^{p-1} &\equiv ty^{p-1} \mod \delta \\
z^p + sz^{p-1} &\equiv y^p + ty^{p-1} \mod \delta \\
z^{p-1}(z+s) &\equiv y^{p-1}(y+t) \mod \delta \\
z^{p-1}(zy+sy) &\equiv yy^{p-1}(y+t) \mod \delta
\end{aligned}$$

$yz \equiv st \mod \delta$ より

$$\begin{aligned}
z^{p-1}(st+sy) &\equiv y^p(y+t) \mod \delta \\
sz^{p-1}(y+t) &\equiv y^p(y+t) \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
z^p(z+s) &\equiv y^{p-1}(zy+zt) \mod \delta \\
z^p(z+s) &\equiv y^{p-1}(st+zt) \mod \delta \\
z^p(z+s) &\equiv ty^{p-1}(z+s) \mod \delta
\end{aligned}$$

よって $yz \equiv st \mod \delta$ ならば、定義域において以下の合同式を満たす。

$$\begin{aligned}
sz^{p-1} &\equiv y^p \mod \delta \\
z^p &\equiv ty^{p-1} \mod \delta
\end{aligned}$$

ただし $\delta \perp x$ より $y^p \not\equiv z^p \mod \delta$

$$s \not\equiv z \mod \delta \quad , \quad t \not\equiv y \mod \delta$$

ここで以下の仮定をする。

$$yz \equiv 1 \cdot k_1 \cdot k_2 \mod \delta \quad , (1 < k_1 \leqq k_2 < \delta) \tag{23}$$

ところで

Proposition 43 s , t を満たす解 s_1 , t_1 と s_2 , t_2 が存在するとき、
$sz^{p-1} \equiv y^p \mod \delta$, $z^p \equiv ty^{p-1} \mod \delta$ ならば、それらは合同である。

$$s_1 \equiv s_2 \mod \delta \quad , t_1 \equiv t_2 \mod \delta$$

仮定を当てはめると

$$\begin{cases} s_1 \equiv 1 \mod \delta \\ t_1 \equiv k_1 \cdot k_2 \mod \delta \end{cases}$$

$$\begin{cases} s_2 \equiv k_1 \mod \delta \\ t_2 \equiv k_2 \mod \delta \end{cases}$$

しかし (23) より $s_1 \not\equiv s_2 \mod \delta$

よって $yz \equiv 1 \cdot k \mod \delta$ でなければならないので

$$\begin{cases} s \equiv 1 \mod \delta \\ t \equiv yz \mod \delta \end{cases}$$

$\wedge$

$$\begin{cases} s \equiv -yz \mod \delta \\ t \equiv -1 \mod \delta \end{cases}$$

Remark 44 δ は奇数だから $(s \not\equiv 1 \wedge -1 \mod \delta)$ なので $(s \equiv 1 \vee -1 \mod \delta)$, $(t \equiv -1 \vee 1 \mod \delta)$ として考える。

$$yz \equiv -1 \mod \delta \tag{24}$$

また同様に

$$xz \equiv -1 \mod \delta \tag{25}$$

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

$$\begin{cases} s \equiv y \mod \delta \\ t \equiv z \mod \delta \end{cases}$$

$$\begin{cases} y \equiv 1 \mod \delta \\ z \equiv -1 \mod \delta \end{cases}$$

よって $yz \equiv 1 \cdot k \mod \delta$ を満たしている。

$$x^p y^{-(p-1)} \equiv -t \mod \delta \quad , \quad y^p x^{-(p-1)} \equiv s \mod \delta$$

$$-ty^{p-1} + sx^{p-1} \equiv z^p \mod \delta$$

ここで s , t を変数とするとき満たすべき解を考察する。

$$\begin{aligned}
-ty^{p-1} + sx^{p-1} &\equiv z^p \mod \delta \\
-ty^{p-1} + sx^{p-1} &\equiv x^p + y^p \mod \delta \\
-x^p + sx^{p-1} &\equiv y^p + ty^{p-1} \mod \delta \\
-x^{p-1}(x-s) &\equiv y^{p-1}(y+t) \mod \delta \\
-x^{p-1}(xy - sy) &\equiv yy^{p-1}(y+t) \mod \delta
\end{aligned}$$

$xy \equiv -st \mod \delta$ より

$$\begin{aligned}
-x^{p-1}(-st - sy) &\equiv y^p(y+t) \mod \delta \\
sx^{p-1}(y+t) &\equiv y^p(y+t) \mod \delta
\end{aligned}$$

同様に

$$\begin{aligned}
-x^p(x-s) &\equiv y^{p-1}(xy + xt) \mod \delta \\
-x^p(x-s) &\equiv y^{p-1}(-st + xt) \mod \delta \\
-x^p(x-s) &\equiv ty^{p-1}(x-s) \mod \delta
\end{aligned}$$

よって $xy \equiv -st \mod \delta$ であるならば、定義域の範囲で以下の合同式を満たす。

$$\begin{aligned}
sx^{p-1} &\equiv y^p \mod \delta \\
-x^p &\equiv ty^{p-1} \mod \delta
\end{aligned}$$

ただし $\delta \perp z$ より $-x^p \not\equiv y^p \mod \delta$

$$s \not\equiv -x \mod \delta \quad , \quad t \not\equiv y \mod \delta$$

ここで以下の仮定をする。

$$xy \equiv 1 \cdot k_1 \cdot k_2 \mod \delta \quad , (1 < k_1 \leqq k_2 < \delta) \tag{26}$$

ところで

Proposition 45 s , t を満たす解 s_1 , t_1 と s_2 , t_2 が存在するとき、
$sx^{p-1} \equiv y^p \mod \delta$, $-x^p \equiv ty^{p-1} \mod \delta$ ならば、それらは合同である。

$$s_1 \equiv s_2 \mod \delta \quad , t_1 \equiv t_2 \mod \delta$$

仮定を当てはめると

$$\begin{cases} s_1 \equiv 1 \mod \delta \\ t_1 \equiv k_1 \cdot k_2 \mod \delta \end{cases}$$

$$\begin{cases} s_2 \equiv k_1 \mod \delta \\ t_2 \equiv k_2 \mod \delta \end{cases}$$

しかし (26) より $s_1 \not\equiv s_2 \mod \delta$

よって $xy \equiv 1 \cdot k \mod \delta$ でなければならないので

$$\begin{cases} s \equiv 1 \mod \delta \\ t \equiv -xy \mod \delta \end{cases}$$

$\wedge$

$$\begin{cases} s \equiv xy \mod \delta \\ t \equiv -1 \mod \delta \end{cases}$$

Remark 46 δ は奇数だから $(s \not\equiv 1 \wedge -1 \mod \delta)$ なので $(s \equiv 1 \vee -1 \mod \delta)$
, $(t \equiv -1 \vee 1 \mod \delta)$ として考える。

$$xy \equiv 1 \mod \delta \tag{27}$$

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

$$\begin{cases} s \equiv y \mod \delta \\ t \equiv -x \mod \delta \end{cases}$$

$$\begin{cases} y \equiv 1 \mod \delta \\ x \equiv 1 \mod \delta \end{cases}$$

よって $xy \equiv 1 \cdot k \mod \delta$ を満たしている。

(24)(27) より

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

これは $\delta \perp y$ に反する。

よって $S = 2^k$

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

・$2 \mid z$ ，$2 \perp xy$ のとき

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

$$\begin{aligned} &2 \mid L = p^{pn-1} c^p \\ &2 \mid c \end{aligned}$$

$$\begin{aligned} &2 \perp R = p\gamma^p \\ &2 \perp \gamma \end{aligned}$$

$$\begin{aligned} z + x + y &= p^n c(\gamma + p^{(p-1)n-1} c^{p-1}) \\ 2^k &= \gamma + p^{(p-1)n-1} c^{p-1} \\ 2^k &= 1 \end{aligned}$$

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

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

Proposition 47 $z - y + x = aT \quad , \ \epsilon \mid T \ \Rightarrow \ \epsilon \perp xyz$

Proof 48

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

$$\alpha \perp a$$

$\epsilon \mid T \quad , \ \epsilon \mid a$ ならば $\epsilon \mid \alpha$ でなければならず矛盾する。よって

$$\epsilon \perp x$$

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

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

$$\epsilon \perp bc$$

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

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

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

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

よって $\epsilon \perp \beta$

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

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

よって $\epsilon \perp \gamma$ □

Proposition 49 $p \mid z$ ， $p \perp xy$ ， $2 \mid x$ ， $2 \perp yz$ のとき $x^p + y^p \neq z^p$

Proof 50

p.23〜p.26 と同様。

(24)(25) より

$$\begin{aligned} xz &\equiv yz \mod \epsilon \\ x &\equiv y \mod \epsilon \\ x - y &\equiv 0 \mod \epsilon \end{aligned}$$

これは $\epsilon \perp z$ に反する。

よって $T = 2^k$

$$z - y + x = a2^k$$

・$2 \mid x$ ， $2 \perp yz$ のとき

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

$$\begin{aligned} &2 \mid L = a^p \\ &2 \mid a \end{aligned}$$

$$\begin{aligned} &2 \perp R = \alpha^p \\ &2 \perp \alpha \end{aligned}$$

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

しかし、$a^{p-1} + \alpha > 1$ なので矛盾する。 □

References

[1] Laubenbacher R, Pengelley D (2007).“Voici ce que j’ai trouvé:” Sophie Germain’s grand plan to prove Fermat’s Last Theorem