Fermat's Last Theorem

Hajime Mashima

October 23, 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。

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

1.2 Case 1 $(p \perp xyz)$

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

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

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

Proposition 3 $R \equiv 1 \mod p$

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

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

Proof 4 $p = 5$ を例とする。

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

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

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

$$\begin{aligned} x^5 + y^5 &= (x + y)(5y^4 - 10y^3(x + y) + 10y^2(x + y)^2 - 5y(x + y)^3 + (x + y)^4) \\ R &= py^4 - 2py^3(x + y) + 2py^2(x + y)^2 - py(x + y)^3 + (x + y)^{p-1} \end{aligned}$$

他の素数についても同様なので一般的に

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

$\square$

Proposition 5

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

Proof 6 $x^p + y^p = L \cdot R$ において、$c' \mid (x+y)$ と置くと

$$\begin{aligned} L &\equiv 0 \mod c' \\ R &\equiv py^{p-1} \mod c' \\ c' \perp py \text{ なので} \\ L \perp R &\equiv py^{p-1} \mod c' \end{aligned}$$

$z^p - x^p$、$z^p - y^p$ についても同様である。 □

Proposition 7 $q \mid R$ のとき (q は p でない素数)

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

Proof 8 $q \not\equiv 1 \mod p \quad (q \neq p)$ 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。

$$\begin{aligned} y &\equiv g \mod q \\ z &\equiv h \mod q \\ z - y &\equiv h - g \mod q \end{aligned}$$

(3) より

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

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

$z^p - y^p = x^p$ 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。

□

※以降 k は適当な整数とする。

Proposition 9 $x^p + y^p = z^p \quad \Rightarrow \quad p^2 \mid (x+y-z)$

Proof 10

(3) より

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

(4) より

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

よって

$$R \equiv 1 \mod p^2 \tag{10}$$

$$x^p + y^p - z^p \equiv 0 \mod p^2$$

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

(10) より

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

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

□

1.2.1 $p=3$

Proposition 11 $x^3+y^3=z^3 \Rightarrow 3 \mid xyz$

Proof 12

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

$x^3+y^3-z^3=0$ なので

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

$3^{3n} \mid (x+y-z)^3$ なので

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

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

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

よって

$$3 \mid xyz$$

□

1.2.2 $p \geqq 5$

Proposition 13 $x^p + y^p \neq z^p$

Proof 14

Definition 15

- $\theta \perp xyz$
- $\theta \perp 2$

$$x^p + sz^{p-1} \equiv ty^{p-1} \mod \theta \tag{11}$$

ここで s ，t について満たすべき解を考察する。

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

以下の仮定をおく。

$$zy \equiv st \mod \theta \tag{12}$$

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

同様に

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

よって

$$\begin{aligned}
sz^{p-1} \equiv y^p \mod \theta \\
z^p \equiv ty^{p-1} \mod \theta
\end{aligned} \tag{13}$$

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

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

$x^p - z^p = -y^p$ より
$s = -z \quad , \ t = -y$ のとき (11), (12) を満たすが

$$sz^{p-1} \cdot 0 \equiv y^p \cdot 0 \mod \theta$$
$$z^p \cdot 0 \equiv ty^{p-1} \cdot 0 \mod \theta$$

となり (13) を満たすか不明である。

ここで別の観点から s , t について満たすべき解を考察する。

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

$$\begin{aligned} -ty^p + stz^{p-1} &\equiv t(-z^p + ty^{p-1}) \mod \theta \\ -ty^p + yz^p &\equiv t(ty^{p-1} - z^p) \mod \theta \\ -y(ty^{p-1} - z^p) &\equiv t(ty^{p-1} - z^p) \mod \theta \end{aligned}$$

同様に

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

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

よって

$$\begin{aligned} -y &\equiv t \mod \theta \\ s &\equiv -z \mod \theta \end{aligned} \tag{14}$$

$\theta = p$ のとき Fermat's little theorem より

$$z^{p-1} \equiv 1 \mod p \quad , \ y^{p-1} \equiv 1 \mod p$$

(13) より

$$\begin{aligned} s &\equiv y \mod p \\ t &\equiv z \mod p \end{aligned}$$

(14) より

$$-z \equiv y \mod p$$
$$z + y \equiv 0 \mod p \tag{15}$$

x のときも同様なので

$$z + x \equiv 0 \mod p \tag{16}$$

再び s , t について満たすべき解を考察する。

$$-ty^{p-1}+sx^{p-1}\equiv z^p \mod \theta \tag{17}$$

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

以下の仮定をおく。

$$xy\equiv -st \mod \theta \tag{18}$$

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

同様に

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

よって

$$\begin{aligned}
sx^{p-1}\equiv y^p \mod \theta\\
-x^p\equiv ty^{p-1} \mod \theta
\end{aligned} \tag{19}$$

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

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

$y^p+x^p=z^p$ より
$s=x$, $t=-y$ は (17), (18) を満たすが

$$\begin{aligned}
sx^{p-1}\cdot 0\equiv y^p\cdot 0 \mod \theta\\
-x^p\cdot 0\equiv ty^{p-1}\cdot 0 \mod \theta
\end{aligned}$$

となり (19) を満たすか不明である。

ここで別の観点から s , t について満たすべき解を考察する。

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

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

同様に

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

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

よって

$$
\begin{aligned}
-y \equiv t \mod \theta \\
s \equiv x \mod \theta
\end{aligned} \tag{20}
$$

$\theta = p$ のとき Fermat's little theorem より

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

(19) より

$$
\begin{aligned}
s \equiv y \mod p \\
t \equiv -x \mod p
\end{aligned}
$$

(20) より

$$
\begin{aligned}
x &\equiv y \mod p \\
x - y &\equiv 0 \mod p
\end{aligned} \tag{21}
$$

(15)(16)(21) より

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

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

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

これは $p \perp xyz$ $(p \geqq 5)$ の前提に反する。 □

1.3 Case 2 $(p \mid xyz)$

Proposition 16

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

Proof 17

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

$$p^1 \mid R$$

※ p を除き、

$$L \perp R$$

Definition 18 $p \perp abc$

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

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

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

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

$$p^2 \mid x \tag{22}$$

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

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

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

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \tag{23}$$

(22) より $x = ap^2\alpha$ と置けるので

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

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

(23)　, $p \perp \alpha^p$ より

$$p^1 \mid K \text{ でなければならない。}$$

よって

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

一般的に

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

□

また

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

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

1.3.1 $p \mid x$

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

Proposition 19 $x + z - y = p^n aS \quad , \; \delta \mid S \;\Rightarrow\; \delta \perp xyz$

Proof 20

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

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

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

Proposition 21 $2p \mid x$, $2p \perp yz$ のとき $x^p + y^p \neq z^p$

Proof 22

$\delta \perp xyz$ なので

$$y^p \not\equiv z^p \mod \delta, (x^p \not\equiv z^p \mod \delta) \quad , \quad x^p \not\equiv -y^p \mod \delta$$

(13)(14), (19)(20) より、$\theta = \delta$ ならば

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

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

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

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

これは $\delta \perp xyz$ の前提に反する。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。 □

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

Proposition 23 $z - x + y = bU \quad , \ \delta'' \mid U \ \Rightarrow \ \delta'' \perp xyz$

Proof 24

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

$$\beta \perp b$$

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

$$\delta'' \perp y$$

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

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

$$\delta'' \perp ac$$

$\delta'' \mid \alpha$ ならば $\delta'' \mid z + y$

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

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

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

よって $\delta'' \perp \alpha$

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

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

よって $\delta'' \perp \gamma$ □

Proposition 25 $p \mid x$, $p \perp yz$, $2 \mid y$, $2 \perp xz$ のとき $x^p + y^p \neq z^p$

$\delta'' \perp xyz$ なので

$$y^p \not\equiv z^p \mod \delta'', (x^p \not\equiv z^p \mod \delta'') \quad , \quad x^p \not\equiv -y^p \mod \delta''$$

(13)(14), (19)(20) より、$\theta = \delta''$ ならば

$$\begin{aligned} -z^p &\equiv y^p \mod \delta'' \quad , \quad (-z^p \equiv x^p \mod \delta'') \\ x^p &\equiv y^p \mod \delta'' \end{aligned}$$

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

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

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

これは $\delta'' \perp xyz$ の前提に反する。よって $U = 2^k$

$$z - x + y = b2^k$$

・$2 \mid y$, $2 \perp xz$ のとき

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

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

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

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

しかし、$b^{p-1} + \beta > 1$ なので矛盾する。 $\square$

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

Proposition 26 $x + y + z = cT$, $\epsilon \mid T \ \Rightarrow \ \epsilon \perp xyz$

Proof 27

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

$$\gamma \perp c$$

$\epsilon \mid T$, $\epsilon \mid c$ ならば矛盾する。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 $\epsilon \perp \beta$

$\epsilon \mid \alpha$, $\epsilon \mid y + z$ 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 28 $p \mid x$, $p \perp yz$, $2 \mid z$, $2 \perp xy$ のとき $x^p + y^p \neq z^p$

$\epsilon \perp xyz$ なので

$$y^p \not\equiv z^p \mod \epsilon, (x^p \not\equiv z^p \mod \epsilon) \quad , \quad x^p \not\equiv -y^p \mod \epsilon$$

(13)(14), (19)(20) より、$\theta = \epsilon$ ならば

$$\begin{aligned} -z^p &\equiv y^p \mod \epsilon \quad , \quad (-z^p \equiv x^p \mod \epsilon) \\ x^p &\equiv y^p \mod \epsilon \end{aligned}$$

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

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

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

これは $\epsilon \perp xyz$ の前提に反する。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。 $\square$

1.3.2 $p \mid z$

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

Proposition 29 $z + x + y = p^n cS$ ， $\delta' \mid S \;\Rightarrow\; \delta' \perp xyz$

Proof 30

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

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

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

$$\delta' \perp z$$

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

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

$$\delta' \perp ab$$

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

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

$z^p - x^p = y^p \equiv 0 \mod \delta'$ 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 $$\delta' \perp \beta$$

$\delta' \mid \alpha$ ， $\delta' \mid z + y$ 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 31 $2p \mid z$, $2p \perp xy$ のとき $x^p + y^p \neq z^p$

Proof 32

$\delta' \perp xyz$ なので

$$y^p \not\equiv z^p \mod \delta', (x^p \not\equiv z^p \mod \delta') \quad , \quad x^p \not\equiv -y^p \mod \delta'$$

(13)(14), (19)(20) より、$\theta = \delta'$ ならば

$$\begin{aligned} -z^p &\equiv y^p \mod \delta' \quad , \quad (-z^p \equiv x^p \mod \delta') \\ x^p &\equiv y^p \mod \delta' \end{aligned}$$

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

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

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

これは $\delta' \perp xyz$ の前提に反する。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。 $\square$

$$
\begin{array}{ll}
x = a\alpha & z - y = a^p \\
y = b\beta & z - x = b^p \\
z = p^n c\gamma & x + y = p^{pn-1} c^p \\
p \perp xyc\gamma T & 2 \perp \epsilon'
\end{array}
$$

Proposition 33 $z - y + x = aT \quad , \ \epsilon' \mid T \ \Rightarrow \ \epsilon' \perp xyz$

Proof 34

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

$$\alpha \perp a$$

$\epsilon' \mid T \quad , \ \epsilon' \mid a$ 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 35 $p \mid z$, $p \perp xy$, $2 \mid x$, $2 \perp yz$ のとき $x^p + y^p \neq z^p$

Proof 36

$\epsilon' \perp xyz$ なので

$$y^p \not\equiv z^p \mod \epsilon', (x^p \not\equiv z^p \mod \epsilon') \quad , \quad x^p \not\equiv -y^p \mod \epsilon'$$

(13)(14), (19)(20) より、$\theta = \epsilon'$ ならば

$$\begin{aligned} -z^p &\equiv y^p \mod \epsilon' \quad , \quad (-z^p \equiv x^p \mod \epsilon') \\ x^p &\equiv y^p \mod \epsilon' \end{aligned}$$

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

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

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

これは $\epsilon' \perp xyz$ の前提に反する。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。 □

1.3.3 Supplement

Proposition 37

$$\begin{aligned} \delta &\neq p \\ \delta'' &\neq p \\ \delta &\neq 3 \\ \delta'' &\neq 3 \end{aligned}$$

p.13

$$\begin{aligned} &S = \alpha + p^{(p-1)n-1}a^{p-1} \\ &\delta \neq p \end{aligned}$$

p.15

$$\begin{aligned} &p \mid x \\ &p \mid z - y \\ &p = \delta'' \\ \Rightarrow\ &p \mid z + y \\ \Rightarrow\ &p \mid zy \end{aligned}$$

p.13

$$\begin{aligned} 3 \mid \delta \quad &, \ 3 \perp xyz \\ x \equiv \pm 1 &\mod 3 \\ y \equiv \pm 2 &\mod 3 \\ z \equiv \pm 1 &\mod 3 \\ x - y \not\equiv 0 &\mod 3 \\ x^p - y^p \equiv 0 &\mod 3 \end{aligned}$$

p.15

$$\begin{aligned} 3 \mid \delta'' \quad &, \ 3 \perp xyz \\ x \equiv \pm 1 &\mod 3 \\ y \equiv \pm 2 &\mod 3 \\ z \equiv \pm 2 &\mod 3 \\ x - y \not\equiv 0 &\mod 3 \\ x^p - y^p \equiv 0 &\mod 3 \end{aligned}$$

□