Fermat's Last Theorem

Hajime Mashima

November 19, 2018

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 $p = 5$

Proposition 14 $x^5 + y^5 \neq z^5$

Proof 15

$$(x+y-z)^5 = 5x^4y - 5x^4z + 10x^3y^2 - 20x^3yz + 10x^3z^2 + 10x^2y^3 - 30x^2y^2z$$
$$+ 30x^2yz^2 - 10x^2z^3 + 5xy^4 - 20xy^3z + 30xy^2z^2 - 20xyz^3 + 5xz^4$$
$$- 5y^4z + 10y^3z^2 - 10y^2z^3 + 5yz^4 + x^5 + y^5 - z^5$$

$x^5 + y^5 - z^5 = 0$ なので

$$(x+y-z)^5 =$$
$$5x^4y - 5x^4z + 10x^3y^2 - 20x^3yz + 10x^3z^2 + 10x^2y^3 - 30x^2y^2z$$
$$+ 30x^2yz^2 - 10x^2z^3 + 5xy^4 - 20xy^3z + 30xy^2z^2 - 20xyz^3 + 5xz^4$$
$$- 5y^4z + 10y^3z^2 - 10y^2z^3 + 5yz^4$$

$$= 5\left(x^4y - x^4z + 2x^3y^2 - 4x^3yz + 2x^3z^2 + 2x^2y^3 - 6x^2y^2z\right.$$
$$+6x^2yz^2 - 2x^2z^3 + xy^4 - 4xy^3z + 6xy^2z^2 - 4xyz^3 + xz^4$$
$$\left.-y^4z + 2y^3z^2 - 2y^2z^3 + yz^4\right)$$

$$= 5\left(x^4y - x^4z + 2x^3z^2 + 2x^2y^3 - 4xy^3z + 6xy^2z^2 - 4xyz^3 + xz^4\right.$$
$$+2x^3y^2 - 4x^3yz + 6x^2yz^2 + xy^4 - y^4z + 2y^3z^2 - 2y^2z^3 + yz^4$$
$$\left.-2x^2z^3 - 6x^2y^2z\right)$$

$$= 5\left(x^4y - x^4z + 2x^3z^2 + x^2y^3 - xy^3z + 2xy^2z^2 - 2xyz^3 + xz^4\right.$$
$$+x^3y^2 - x^3yz + 2x^2yz^2 + xy^4 - y^4z + 2y^3z^2 - 2y^2z^3 + yz^4$$
$$+x^2y^3 - 3xy^3z + 4xy^2z^2 - 2xyz^3 + x^3y^2 - 3x^3yz + 4x^2yz^2$$
$$\left.-2x^2z^3 - 6x^2y^2z\right)$$

$$= 5\left(x\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right)\right.$$
$$+y\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right)$$
$$+x^2y^3 + x^3y^2 - 3x^3yz + 4xy^2z^2 - 3xy^3z + 4x^2yz^2 - 2xyz^3$$
$$\left.-2x^2z^3 - 6x^2y^2z\right)$$

$$= 5\left((x+y)\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right)\right.$$
$$+x^2y^2(x+y) - 3x^3yz - 6x^2y^2z + 4x^2yz^2 - 3xy^3z + 4xy^2z^2 - 2xyz^3$$
$$\left.-2x^2z^3\right)$$

$$= 5\left((x+y)\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right)\right.$$
$$+x^2y^2(x+y) - 3x^2yz(x+y) - 3x^2y^2z + 4x^2yz^2 - 3xy^3z + 4xy^2z^2$$
$$\left.-2xz^3(x+y)\right)$$

$$= 5\left((x+y)\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right)\right.$$
$$+x^2y^2(x+y) - 3x^2yz(x+y) - 3xy^2z(x+y) + 4x^2yz^2 + 4xy^2z^2$$
$$\left.-2xz^3(x+y)\right)$$

$$= 5\left((x+y)\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right)\right.$$
$$+x^2y^2(x+y) - 3x^2yz(x+y) - 3xy^2z(x+y) + 4xyz^2(x+y)$$
$$\left.-2xz^3(x+y)\right)$$

$$= 5(x+y)\left(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4\right.$$
$$\left.+x^2y^2 - 3x^2yz - 3xy^2z + 4xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(-x^3(z-y) + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - yz^3 + z^3(z-y)\right.$$
$$\left.+x^2y^2 - 3x^2yz - 3xy^2z + 4xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(\left(z^3 - x^3\right)(z-y) + 2x^2z^2 + xy^3 - y^3z + y^2z^2 + y^2z^2 - yz^3\right.$$
$$\left.+x^2y^2 - x^2yz - 2x^2yz - 3xy^2z + 4xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(\left(z^3 - x^3\right)(z-y) + xy^3 - y^3z + y^2z^2 + y^2z^2 - yz^3\right.$$
$$\left.+x^2y^2 - x^2yz + 2x^2z(z-y) - 3xyz(y-z) + xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(\left(z^3 - x^3 + 2x^2z + 3xyz\right)(z-y) + xy^3 - y^2z(y-z)\right.$$
$$\left.+y^2z^2 - yz^3 + x^2y^2 - x^2yz + xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(\left(z^3 - x^3 + 2x^2z + 3xyz + y^2z\right)(z-y) + xy^3\right.$$
$$\left.+yz^2(y-z) + x^2y(y-z) + xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(\left(z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y\right)(z-y)\right.$$
$$\left.+xy^3 + xyz^2 - 2xz^3\right)$$

$$= 5(x+y)\left(\left(z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y\right)(z-y)\right.$$
$$\left.+xy^3 + xyz^2 - xz^3 - xz^3\right)$$

$$= 5\,(x+y)\,\big(\big(z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y\big)\,(z-y)$$
$$+xy^3 + xz^2(y-z) - xz^3\big)$$

$$= 5\,(x+y)\,\big(\big(z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y\big)\,(z-y)$$
$$+xy^3 - xz^3 + xz^2(y-z)\big)$$

$$= 5\,(x+y)\,\big(\big(z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y\big)\,(z-y)$$
$$+x(y^3 - z^3) + xz^2(y-z)\big)$$

$$= 5\,(x+y)\,\big(\big(z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y - xz^2\big)\,(z-y)$$
$$-x(z-y)(y^2 + yz + z^2)\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 + xz + z^2)$$
$$+2x^2z + 3xyz + y^2z - yz^2 - x^2y - xz^2 - x(y^2 + yz + z^2)\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 + xz + z^2)$$
$$+2x^2z + 3xyz + y^2z - yz^2 - x^2y - xz^2 - xy^2 - xyz - xz^2\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 + xz + z^2)$$
$$+2x^2z - 2xz^2 + 2xyz + y^2z - yz^2 - x^2y - xy^2\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 + xz + z^2)$$
$$+2xz(x-z) + 2xyz + y^2(z-x) - yz^2 - x^2y\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 - xz + z^2 + y^2)$$
$$+xyz + xyz - yz^2 - x^2y\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 - xz + z^2 + y^2)$$
$$+xyz + yz(x-z) - x^2y\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 - xz + z^2 + y^2 - yz)$$
$$+xyz - x^2y\big)$$

$$= 5\,(x+y)\,(z-y)\,\big((z-x)(x^2 + y^2 + z^2 - xz - yz) + xy(z-x)\big)$$

$$(x+y-z)^5 = 5(x+y)(z-y)(z-x)(x^2+y^2+z^2+xy-xz-yz)$$

ここで

$$(x+y-z)^2 = x^2+y^2+z^2+2xy-2xz-2yz$$

$$(x+y-z)^2-(xy-xz-yz) = x^2+y^2+z^2+(xy-xz-yz) \qquad (11)$$

よって

$$(x+y-z)^5 = 5(x+y)(z-y)(z-x)\left((x+y-z)^2-(xy-xz-yz)\right)$$

$x+y-z \equiv 0 \mod 5$ であるから

$$x+y \equiv z \mod 5$$
$$z-x \equiv y \mod 5$$
$$z-y \equiv x \mod 5$$

$5^5 \mid (x+y-z)^5$, $5 \perp (x+y)(z-y)(z-x)$ より

$$5^4 \mid \left((x+y-z)^2-(xy-xz-yz)\right)$$
$$5^2 \mid (xy-xz-yz)$$

(11) より

$$x^2+y^2+z^2 \equiv 0 \mod 5 \qquad (12)$$

$5 \perp xyz$ なので、$k=\{x,y,z\}$ のとき

$$k^4 \equiv 1 \mod 5$$
$$k^2 \equiv \pm 1 \mod 5$$

よって得られる解は

$$x^2+y^2+z^2 \equiv \pm 1 \mod 5$$

または

$$x^2+y^2+z^2 \equiv \pm 3 \mod 5$$

これは (12) と反する。 □

1.3.3 $p \geqq 7$

Proposition 16 $x^p + y^p \neq z^p$

Definition 17

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

Proof 18

$$\begin{aligned} x^p + y^p - z^p &= 0 \\ x^p + y^p &\equiv z^p \mod \theta \\ x^p + yy^{p-1} &\equiv zz^{p-1} \mod \theta \end{aligned} \tag{13}$$

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

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

$\theta \perp yz$ なので θ を法とする y^{p-1} ， z^{p-1} の逆元 k' が存在する。

$k = k'x^{p-1}$ として

$$\begin{aligned} ky^{p-1} &\equiv x^{p-1} \mod \theta \\ kz^{p-1} &\equiv x^{p-1} \mod \theta \end{aligned}$$

と置ける。
(13) より

$$\begin{aligned} kx^p + yky^{p-1} &\equiv zkz^{p-1} \mod \theta \\ kx^p + yx^{p-1} &\equiv zx^{p-1} \mod \theta \end{aligned}$$

$k \equiv 1 \mod \theta$ なので

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

・$y^{p-1} \equiv z^{p-1} \mod \theta$ ，$y^{p-1} \not\equiv z^{p-1} \mod \theta$ の一般的条件

$\theta \perp yz$ なので θ を法とする $y^{p-1}z^{p-1}$ の逆元 k' が存在する。$k = k'x^{p-1}$ として

$$ky^{p-1}z^{p-1} \equiv x^{p-1} \mod \theta \tag{14}$$

と置ける。

$$\begin{aligned} x^p + yx^{p-1} &\equiv zx^{p-1} \mod \theta \\ x^p + yky^{p-1}z^{p-1} &\equiv zky^{p-1}z^{p-1} \mod \theta \\ x^p + y^pkz^{p-1} &\equiv z^pky^{p-1} \mod \theta \\ z^p - y^p + y^pkz^{p-1} &\equiv z^pky^{p-1} \mod \theta \end{aligned} \tag{15}$$

$$\begin{aligned} y^pkz^{p-1} - y^p &\equiv z^pky^{p-1} - z^p \mod \theta \\ y^p(kz^{p-1} - 1) &\equiv z^p(ky^{p-1} - 1) \mod \theta \\ yy^{p-1}(kz^{p-1} - 1) &\equiv zz^{p-1}(ky^{p-1} - 1) \mod \theta \\ yky^{p-1}(kz^{p-1} - 1) &\equiv zkz^{p-1}(ky^{p-1} - 1) \mod \theta \end{aligned} \tag{16}$$

$$0 < (ky^{p-1})' < \theta$$
$$0 < (kz^{p-1})' < \theta$$

と置くと、$ky^{p-1} \not\equiv 1 \mod \theta$ ，$kz^{p-1} \not\equiv 1 \mod \theta$ ならば

$$(ky^{p-1})' \perp (ky^{p-1})' - 1$$
$$(kz^{p-1})' \perp (kz^{p-1})' - 1$$

であるから

$$ky^p \equiv skz^{p-1} \mod \theta \tag{17}$$
$$kz^p \equiv tky^{p-1} \mod \theta \tag{18}$$
$$y^p \equiv sz^{p-1} \mod \theta \tag{19}$$
$$z^p \equiv ty^{p-1} \mod \theta \tag{20}$$

$x^p + y^p \equiv z^p \mod \theta$ より、以下の合同式を満たす。

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

(19)·(20) より

$$yz \equiv st \mod \theta \tag{21}$$

よって (15) より

$$\begin{aligned} y^pk \cdot z^pk &\equiv st \mod \theta \\ k^2y^pz^p &\equiv yz \mod \theta \\ k^2y^{p-1}z^{p-1} &\equiv 1 \mod \theta \end{aligned}$$

(14) より

$$kx^{p-1} \equiv 1 \mod \theta \tag{22}$$

$$yky^{p-1}(kz^{p-1}-1) \equiv zkz^{p-1}(ky^{p-1}-1) \mod \theta$$
$$ky^p(kz^{p-1}-1) \equiv z(k^2y^{p-1}z^{p-1}-kz^{p-1}) \mod \theta$$
$$ky^p(kz^{p-1}-1) \equiv z(kx^{p-1}-kz^{p-1}) \mod \theta$$

(22) より

$$ky^p(kz^{p-1}-1) \equiv -z(kz^{p-1}-1) \mod \theta$$

同様に

$$-y(ky^{p-1}-1) \equiv kz^p(ky^{p-1}-1) \mod \theta$$

$ky^{p-1} \not\equiv 1 \mod \theta$, $kz^{p-1} \not\equiv 1 \mod \theta$ ならば

$$ky^p \equiv -z \mod \theta$$
$$kz^p \equiv -y \mod \theta$$

このとき、(15) より以下のように置ける。

$$s \equiv -z \mod \theta$$
$$t \equiv -y \mod \theta$$

$$x^p + yx^{p-1} \equiv zx^{p-1} \mod \theta$$
$$x^p + yy^{p-1} \equiv zz^{p-1} \mod \theta$$

$$yy^{p-1} - yx^{p-1} \equiv zz^{p-1} - zx^{p-1} \mod \theta$$
$$y(y^{p-1} - x^{p-1}) \equiv z(z^{p-1} - x^{p-1}) \mod \theta$$

(22) より

$$y(ky^{p-1}-1) \equiv z(kz^{p-1}-1) \mod \theta \tag{23}$$

(16) から

$$z^p(ky^{p-1}-1) \equiv y^p(kz^{p-1}-1) \mod \theta$$
$$z^p(y(ky^{p-1}-1)) \equiv y^{p+1}(kz^{p-1}-1) \mod \theta$$

(23) より

$$z^p(z(kz^{p-1}-1))) \equiv y^{p+1}(kz^{p-1}-1) \mod \theta$$
$$z^{p+1}(kz^{p-1}-1) \equiv y^{p+1}(kz^{p-1}-1) \mod \theta$$
$$(z^{p+1}-y^{p+1})(kz^{p-1}-1) \equiv 0 \mod \theta$$

同様に $(z^{p+1}-y^{p+1})(ky^{p-1}-1) \equiv 0 \mod \theta$

$ky^{p-1} \not\equiv 1 \mod \theta$, $kz^{p-1} \not\equiv 1 \mod \theta$ ならば

$$z^{p+1} \equiv y^{p+1} \mod \theta \tag{24}$$

$s \equiv -z \mod \theta$, $t \equiv -y \mod \theta$ を (19)(20) へ代入する。

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

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

(24) より

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

よって

$$s \equiv y \mod \theta \quad , \quad t \equiv z \mod \theta$$

(17) より

$$ky^{p-1} \equiv kz^{p-1} \mod \theta$$

$$x^p + y^p \equiv z^p \mod \theta$$
$$x^p ky^{p-1} + y^p ky^{p-1} \equiv z^p ky^{p-1} \mod \theta$$
$$x^p ky^{p-1} + y^p kz^{p-1} \equiv z^p ky^{p-1} \mod \theta$$

(15) より

$$ky^{p-1} \equiv 1 \mod \theta \qquad kz^{p-1} \equiv 1 \mod \theta$$

また

$$z + y \equiv 0 \mod \theta \qquad z + x \equiv 0 \mod \theta \tag{25}$$

・$x^{p-1} \equiv y^{p-1} \mod \theta$ ，$x^{p-1} \not\equiv y^{p-1} \mod \theta$ の一般的条件

$\theta \perp xy$ なので θ を法とする $x^{p-1}y^{p-1}$ の逆元 k' が存在する。$k = k'z^{p-1}$ として

$$kx^{p-1}y^{p-1} \equiv z^{p-1} \mod \theta \tag{26}$$

と置ける。

$$\begin{aligned} xz^{p-1} + yz^{p-1} &\equiv z^p \mod \theta \\ xkx^{p-1}y^{p-1} + ykx^{p-1}y^{p-1} &\equiv z^p \mod \theta \\ x^pky^{p-1} + y^pkx^{p-1} &\equiv z^p \mod \theta \\ x^pky^{p-1} + y^pkx^{p-1} &\equiv x^p + y^p \mod \theta \end{aligned} \tag{27}$$

$$\begin{aligned} y^pkx^{p-1} - y^p &\equiv x^p - x^pky^{p-1} \mod \theta \\ y^p(kx^{p-1} - 1) &\equiv -x^p(ky^{p-1} - 1) \mod \theta \\ yy^{p-1}(kx^{p-1} - 1) &\equiv -xx^{p-1}(ky^{p-1} - 1) \mod \theta \\ yky^{p-1}(kx^{p-1} - 1) &\equiv -xkx^{p-1}(ky^{p-1} - 1) \mod \theta \end{aligned} \tag{28}$$

$$0 < (ky^{p-1})' < \theta$$
$$0 < (kx^{p-1})' < \theta$$

と置くと、$kx^{p-1} \not\equiv 1 \mod \theta$ ，$ky^{p-1} \not\equiv 1 \mod \theta$ ならば

$$(ky^{p-1})' \perp (ky^{p-1})' - 1$$
$$(kx^{p-1})' \perp (kx^{p-1})' - 1$$

であるから

$$ky^p \equiv skx^{p-1} \mod \theta \tag{29}$$
$$-kx^p \equiv tky^{p-1} \mod \theta \tag{30}$$
$$y^p \equiv sx^{p-1} \mod \theta \tag{31}$$
$$x^p \equiv -ty^{p-1} \mod \theta \tag{32}$$

$x^p + y^p \equiv z^p \mod \theta$ より、以下の合同式を満たす。

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

(31)·(32) より

$$xy \equiv -st \mod \theta \tag{33}$$

よって (27) より

$$x^pk \cdot y^pk \equiv -st \mod \theta$$
$$k^2x^py^p \equiv xy \mod \theta$$
$$k^2x^{p-1}y^{p-1} \equiv 1 \mod \theta$$

(26) より

$$kz^{p-1} \equiv 1 \mod \theta \tag{34}$$

$$yky^{p-1}(kx^{p-1}-1) \equiv -xkx^{p-1}(ky^{p-1}-1) \mod \theta$$
$$ky^p(kx^{p-1}-1) \equiv -x(k^2x^{p-1}y^{p-1}-kx^{p-1}) \mod \theta$$
$$ky^p(kx^{p-1}-1) \equiv -x(kz^{p-1}-kx^{p-1}) \mod \theta$$

(34) より

$$ky^p(kx^{p-1}-1) \equiv x(kx^{p-1}-1) \mod \theta$$

同様に

$$-y(ky^{p-1}-1) \equiv -kx^p(ky^{p-1}-1) \mod \theta$$

$kx^{p-1} \not\equiv 1 \mod \theta$, $ky^{p-1} \not\equiv 1 \mod \theta$ ならば

$$ky^p \equiv x \mod \theta$$
$$kx^p \equiv y \mod \theta$$

このとき、(27) より以下のように置ける。

$$s \equiv x \mod \theta$$
$$-t \equiv y \mod \theta$$

$$xz^{p-1}+yz^{p-1} \equiv z^p \mod \theta$$
$$xx^{p-1}+yy^{p-1} \equiv z^p \mod \theta$$

$$xz^{p-1}-xx^{p-1} \equiv -yz^{p-1}+yy^{p-1} \mod \theta$$
$$-x(x^{p-1}-z^{p-1}) \equiv y(y^{p-1}-z^{p-1}) \mod \theta$$

(34) より

$$-x(kx^{p-1}-1) \equiv y(ky^{p-1}-1) \mod \theta \tag{35}$$

(28) から

$$y^p(kx^{p-1}-1) \equiv -x^p(ky^{p-1}-1) \mod \theta$$
$$y^p(-x(kx^{p-1}-1)) \equiv x^{p+1}(ky^{p-1}-1) \mod \theta$$

(35) より

$$y^p(y(ky^{p-1}-1)) \equiv x^{p+1}(ky^{p-1}-1) \mod \theta$$
$$y^{p+1}(ky^{p-1}-1) \equiv x^{p+1}(ky^{p-1}-1) \mod \theta$$
$$(y^{p+1}-x^{p+1})(ky^{p-1}-1) \equiv 0 \mod \theta$$

同様に $(x^{p+1}-y^{p+1})(kx^{p-1}-1) \equiv 0 \mod \theta$

$kx^{p-1} \not\equiv 1 \mod \theta$, $ky^{p-1} \not\equiv 1 \mod \theta$ ならば

$$x^{p+1} \equiv y^{p+1} \mod \theta \tag{36}$$

$s \equiv x \mod \theta$, $-t \equiv y \mod \theta$ を (31)(32) へ代入する。

$$y^p \equiv x^p \mod \theta \qquad x^p \equiv y^p \mod \theta$$

$$x^{p+1} \equiv xy^p \mod \theta$$

(36) より

$$y^{p+1} \equiv xy^p \mod \theta$$
$$y \equiv x \mod \theta$$

よって

$$s \equiv y \mod \theta \quad , \quad -t \equiv x \mod \theta$$

(29) より

$$ky^{p-1} \equiv kx^{p-1} \mod \theta$$

(27) より

$$kx^{p-1} \equiv 1 \mod \theta \qquad ky^{p-1} \equiv 1 \mod \theta$$

また

$$x - y \equiv 0 \mod \theta \tag{37}$$

(25)(37) より

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

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

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

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 19

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

Proof 20

$p \mid x \quad , \quad p \mid (z-y)$ 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

$$p^1 \mid R \tag{38}$$

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 21

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

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

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

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

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

$$p^2 \mid x \tag{39}$$

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

$x^p = (z-y)p\alpha^p$ と置き、上式に代入する。

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

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \qquad (40)$$

(39) より $x = ap^2\alpha$

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

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

(40) ， $p \perp \alpha^p$ 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

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

$$p^n \mid x+y-z \qquad (41)$$

1.4.1 Comon($p \geqq 3$)

Proposition 22

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

Proof 23

・$3 \mid x$ ， $3 \perp yz$ のとき

$$x^p + y^p - z^p \equiv 0 \mod 3$$

Fermat's little theorem より

$$k^{2n} \equiv 1 \mod 3 \quad (k \perp 3) \tag{42}$$

よって

$$\begin{aligned} y^p - z^p &\equiv 0 \mod 3 \\ yy^{p-1} - zz^{p-1} &\equiv 0 \mod 3 \\ yy^{2n} - zz^{2n} &\equiv 0 \mod 3 \\ y - z &\equiv 0 \mod 3 \\ x + y - z &\equiv 0 \mod 3 \end{aligned}$$

$3 \mid z$ ， $3 \perp xy$ についても同様である。

・$3 \perp xyz$ のとき

$$x^p + y^p - z^p \equiv 0 \mod 3$$

(42) より

$$\begin{aligned} x^p + y^p - z^p &\equiv 0 \mod 3 \\ xx^{p-1} + yy^{p-1} - zz^{p-1} &\equiv 0 \mod 3 \\ x + y - z &\equiv 0 \mod 3 \end{aligned}$$

□

Proposition 24

$$x^p + y^p = z^p \ \ (p \geqq 3) \quad \Rightarrow x + y - z = 3^m p^n abc$$

Proof 25

$x + y - z = p^n abcT$ と θ を仮定する。また (41) より　$p \perp T$ と置く。

$$\theta \mid T \qquad \theta \mid x + y - z \qquad \theta \neq p \qquad \theta \neq 3$$

$\theta \neq 3$ の条件は、Case 1 と同値なので $\theta \perp xyz$ は成り立たない。よって

$$\theta \mid xyz$$

$\theta \mid z$ ，$\theta \mid x + y$ の例

$$\begin{aligned}((x+y)-z)^p = -z^p + \frac{p!}{(p-1)!1!}z^{p-1}(x+y) - \frac{p!}{(p-2)!2!}z^{p-2}(x+y)^2 + \frac{p!}{(p-3)!3!}z^{p-3}(x+y)^3 \\ \cdots - \frac{p!}{1!(p-1)!}z(x+y)^{p-1} + (x+y)^p\end{aligned} \tag{43}$$

$$x^p + y^p = (x+y)\left(py^{p-1} - \frac{p!}{(p-2)!2!}y^{p-2}(x+y) + \cdots - \frac{p!}{1!(p-1)!}y(x+y)^{p-2} + (x+y)^{p-1}\right) \tag{44}$$

$z^p = x^p + y^p$ が成り立つとして、(44) を (43) へ代入する。

$$\begin{aligned}(x+y-z)^p = -(x+y)\Bigg(&py^{p-1} - \frac{p!}{(p-2)!2!}y^{p-2}(x+y) + \cdots - \frac{p!}{1!(p-1)!}y(x+y)^{p-2} + (x+y)^{p-1} \\ &- \frac{p!}{(p-1)!1!}z^{p-1} + \frac{p!}{(p-2)!2!}z^{p-2}(x+y) - \frac{p!}{(p-3)!3!}z^{p-3}(x+y)^2 \\ &\cdots + \frac{p!}{1!(p-1)!}z(x+y)^{p-2} - (x+y)^{p-1}\Bigg)\end{aligned}$$

$$\begin{aligned}(p^n abT)^p = -\Bigg(&py^{p-1} - \frac{p!}{(p-2)!2!}y^{p-2}(x+y) + \cdots - \frac{p!}{1!(p-1)!}y(x+y)^{p-2} + (x+y)^{p-1} \\ &- \frac{p!}{(p-1)!1!}z^{p-1} + \frac{p!}{(p-2)!2!}z^{p-2}(x+y) - \frac{p!}{(p-3)!3!}z^{p-3}(x+y)^2 \\ &\cdots + \frac{p!}{1!(p-1)!}z(x+y)^{p-2} - (x+y)^{p-1}\Bigg)\end{aligned}$$

よって

$$\theta \mid py^{p-1}$$
$$\theta \mid y$$

これは $z \perp y$ に矛盾する。　□

1.4.2　$p = 3$

Leonhard Euler の証明を適用する。

1.4.3 $p \geqq 5$

Proposition 26 $3 \mid xyz \quad , \quad x+y-z = 3^m p^n abc \;\Rightarrow\; x^p + y^p \neq z^p$

・$m > 1$ のとき、$3 \mid z \quad , \quad 3 \perp xy$ の例

$$3 \mid z \qquad 3^p \mid (x+y)$$

Proof 27

$$\begin{aligned}(x+y-z)^p = -(x+y)\Bigg(&py^{p-1} - \frac{p!}{(p-2)!2!}y^{p-2}(x+y) + \cdots - \frac{p!}{1!(p-1)!}y(x+y)^{p-2} + (x+y)^{p-1} \\ &- \frac{p!}{(p-1)!1!}z^{p-1} + \frac{p!}{(p-2)!2!}z^{p-2}(x+y) - \frac{p!}{(p-3)!3!}z^{p-3}(x+y)^2 \\ &\cdots + \frac{p!}{1!(p-1)!}z(x+y)^{p-2} - (x+y)^{p-1}\Bigg)\end{aligned}$$

$$\begin{aligned}(3^m p^n abc)^p &= -c^p\left(py^{p-1} - \ldots\right) \\ (3^m p^n ab)^p &= -\left(py^{p-1} - \ldots\right) \\ 3^{pm}\,(p^n ab)^p &= -\left(py^{p-1} - \ldots\right)\end{aligned}$$

よって $p \geqq 5$ であるから

$$\begin{aligned}&3 \mid py^{p-1} \\ &3 \mid y^{p-1} \\ &3 \mid y\end{aligned}$$

これは $3 \perp y$ に矛盾する。

$$m = 0 \;\Rightarrow\; x+y-z = p^n abc \tag{45}$$

Proposition 28 $\quad 3 \perp xyz \;\Rightarrow\; x+y-z = 3p^n abc$

$3^2 \mid x+y-z$ ならば、Case.1 より

$$\begin{aligned}3x &\equiv 0 \mod \theta \\ 3x &\equiv 0 \mod 3^2 \\ 3 &\mid x\end{aligned}$$

これは $3 \perp xyz$ に反する。よって

$$3 \perp xyz \;\Rightarrow\; x+y-z = 3p^n abc \tag{46}$$

$z-(x+y)=k>0$ と置く。

$$z=x+y+k$$
$$z^p=x^p+y^p+k^p+p(\ldots)$$

$z^p=x^p+y^p$ より

$$0=k^p+p(\ldots)$$

$p(\ldots)>0$ だから

$$0\neq k^p+p(\ldots)$$

よって

$$Kp^nabc=x+y-z>0 \tag{47}$$

$$(x+y-z)^3=3(x+y)(z-x)(z-y)+x^3+y^3-z^3$$
$$(Kp^nabc)^3=3(x+y)(z-x)(z-y)+x^3+y^3-z^3$$
$$K^3p^{3n}(abc)^3=3p^{pn-1}(abc)^p+x^3+y^3-z^3$$
$$K^3p^{3n}(abc)^3-3p^{pn-1}(abc)^p=x^3+y^3-z^3$$

$$p^{3n}(abc)^3(K^3-3p^{n(p-3)-1}(abc)^{p-3})=x^3+y^3-z^3$$

(47) より $abc>0$

$p\geqq 5$, (45) のとき $K^3=1$ だから

$$p^{3n}(abc)^3(1-3p^{n(p-3)-1}(abc)^{p-3})<0 \tag{48}$$

$p\geqq 5$, (46) のとき $K^3=3^3$ だから

$$3p^{3n}(abc)^3(3^2-p^{n(p-3)-1}(abc)^{p-3})<0 \tag{49}$$

$X<Y<Z$, $X^n+Y^n=Z^{\,n}$ のとき

$$X^nY^m+Y^{n+m}<Z^{\,n+m}$$
$$X^{n+m}+Y^{n+m}<X^nY^m+Y^{n+m}<Z^{\,n+m}$$
$$X^{n+m}+Y^{n+m}<Z^{\,n+m}$$

$$x^p+y^p=z^p\ \ (p\geqq 5)\Rightarrow x^3+y^3-z^3>0 \tag{50}$$

(48)(49) は (50) に矛盾する。 □

References

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