

The idea of the Arithmetica

Hajime Mashima

August 11, 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	1
1.1	Fermat's Last Theorem	2
1.2	Structure of the product	2
1.3	Case 1 ($p \perp xyz$)	5
1.3.1	$p = 3$	5
1.3.2	$p = 5$	6
1.3.3	$p \geq 7$	10
1.4	Case 2 ($p \mid xyz$)	13
1.4.1	$p = 3$	16
1.4.2	$p \geq 5$	17

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。この証明を試みる上で代数学的手法はもちろん、Fermat の人柄や当時の状況を想像したり、証明のための哲学およびヒューリスティック等の多角的アプローチを試みている。

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。

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

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

$$A^{p-1} \equiv 1 \pmod{p} \quad (1)$$

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

$$x^{p-1}x + y^{p-1}y - z^{p-1}z \equiv 0 \pmod{p}$$

$$(1) \text{ より } \quad x + y - z \equiv 0 \pmod{p}$$

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

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

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

以降用いる k は適当な整数とする。

Proposition 4 $p \perp xyz$ のとき

$$R \equiv 1 \pmod{p}$$

Proof 5 $p = 5$ を例とする。

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

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

$$z^5 - y^5 = (z - y)(5y^4 + 10y^3(z - y) + 10y^2(z - y)^2 + 5y(z - y)^3 + (z - y)^4) \quad (2)$$

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

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

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

他の素数についても同様なので一般的に

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

□

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

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

$z^p - x^p$ 、 $z^p - y^p$ 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)

$$q \equiv 1 \pmod{p} \quad (q \neq p)$$

Proof 9 $q \not\equiv 1 \pmod{p}$ ($q \neq p$) 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。

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

(3) より

$$g \not\equiv h \pmod{q} \tag{4}$$

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

$z^p - y^p = x^p$ だから

$$(q\mathbb{N}_1 + g)^p \equiv (q\mathbb{N}_2 + h)^p \pmod{q} \tag{5}$$

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

$$(q\mathbb{N}_1 + g)^{q-1} \equiv (q\mathbb{N}_2 + h)^{q-1} \pmod{q} \tag{6}$$

$q \not\equiv 1 \pmod p$ なので

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

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

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

(6) より

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

$(q - 1)k^{p-2} = pm + 1$ と置けるので

$$(q\mathbb{N}_1 + g)^{pm+1} \equiv (q\mathbb{N}_2 + h)^{pm+1} \pmod q \quad (7)$$

(5) より

$$(q\mathbb{N}_1 + g)^{pm} \equiv (q\mathbb{N}_2 + h)^{pm} \pmod q \quad (8)$$

(7) , (8) より

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

$$g \equiv h \pmod q$$

これは (4) に反する。

□

1.3 Case 1 ($p \perp xyz$)

1.3.1 $p = 3$

Proposition 10 $x^3 + y^3 = z^3 \Rightarrow 3 \mid xyz$

Proof 11

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

$x^3 + y^3 - z^3 = 0$ なのので

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

$3^3 \mid (x + y - z)^3$ なのので

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

$x + y - z \equiv 0 \pmod{3}$ であるから

$$x + y \equiv z \pmod{3}$$

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

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

よって

$$3 \mid xyz$$

□

1.3.2 $p = 5$

Proposition 12 $x^5 + y^5 \neq z^5$

Proof 13

$$\begin{aligned}(x + y - z)^5 &= 5x^4y - 5x^4z + 10x^3y^2 - 20x^3yz + 10x^3z^2 + 10x^2y^3 - 30x^2y^2z \\ &+ 30x^2yz^2 - 10x^2z^3 + 5xy^4 - 20xy^3z + 30xy^2z^2 - 20xyz^3 + 5xz^4 \\ &- 5y^4z + 10y^3z^2 - 10y^2z^3 + 5yz^4 + x^5 + y^5 - z^5\end{aligned}$$

$x^5 + y^5 - z^5 = 0$ なるので

$$\begin{aligned}(x + y - z)^5 &= \\ &5x^4y - 5x^4z + 10x^3y^2 - 20x^3yz + 10x^3z^2 + 10x^2y^3 - 30x^2y^2z \\ &+ 30x^2yz^2 - 10x^2z^3 + 5xy^4 - 20xy^3z + 30xy^2z^2 - 20xyz^3 + 5xz^4 \\ &- 5y^4z + 10y^3z^2 - 10y^2z^3 + 5yz^4 \\ &= 5(x^4y - x^4z + 2x^3y^2 - 4x^3yz + 2x^3z^2 + 2x^2y^3 - 6x^2y^2z \\ &+ 6x^2yz^2 - 2x^2z^3 + xy^4 - 4xy^3z + 6xy^2z^2 - 4xyz^3 + xz^4 \\ &- y^4z + 2y^3z^2 - 2y^2z^3 + yz^4) \\ &= 5(x^4y - x^4z + 2x^3z^2 + 2x^2y^3 - 4xy^3z + 6xy^2z^2 - 4xyz^3 + xz^4 \\ &+ 2x^3y^2 - 4x^3yz + 6x^2yz^2 + xy^4 - y^4z + 2y^3z^2 - 2y^2z^3 + yz^4 \\ &- 2x^2z^3 - 6x^2y^2z) \\ &= 5(x^4y - x^4z + 2x^3z^2 + x^2y^3 - xy^3z + 2xy^2z^2 - 2xyz^3 + xz^4 \\ &+ x^3y^2 - x^3yz + 2x^2yz^2 + xy^4 - y^4z + 2y^3z^2 - 2y^2z^3 + yz^4 \\ &+ x^2y^3 - 3xy^3z + 4xy^2z^2 - 2xyz^3 + x^3y^2 - 3x^3yz + 4x^2yz^2 \\ &- 2x^2z^3 - 6x^2y^2z) \\ &= 5(x(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4) \\ &+ y(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4) \\ &+ x^2y^3 + x^3y^2 - 3x^3yz + 4xy^2z^2 - 3xy^3z + 4x^2yz^2 - 2xyz^3 \\ &- 2x^2z^3 - 6x^2y^2z) \\ &= 5((x + y)(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4) \\ &+ x^2y^2(x + y) - 3x^3yz - 6x^2y^2z + 4x^2yz^2 - 3xy^3z + 4xy^2z^2 - 2xyz^3 \\ &- 2x^2z^3)\end{aligned}$$

$$\begin{aligned}
&= 5((x+y)(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4) \\
&\quad + x^2y^2(x+y) - 3x^2yz(x+y) - 3x^2y^2z + 4x^2yz^2 - 3xy^3z + 4xy^2z^2 \\
&\quad - 2xz^3(x+y)) \\
&= 5((x+y)(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4) \\
&\quad + x^2y^2(x+y) - 3x^2yz(x+y) - 3xy^2z(x+y) + 4x^2yz^2 + 4xy^2z^2 \\
&\quad - 2xz^3(x+y)) \\
&= 5((x+y)(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4) \\
&\quad + x^2y^2(x+y) - 3x^2yz(x+y) - 3xy^2z(x+y) + 4xyz^2(x+y) \\
&\quad - 2xz^3(x+y)) \\
&= 5(x+y)(x^3y - x^3z + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - 2yz^3 + z^4 \\
&\quad + x^2y^2 - 3x^2yz - 3xy^2z + 4xyz^2 - 2xz^3) \\
&= 5(x+y)(-x^3(z-y) + 2x^2z^2 + xy^3 - y^3z + 2y^2z^2 - yz^3 + z^3(z-y) \\
&\quad + x^2y^2 - 3x^2yz - 3xy^2z + 4xyz^2 - 2xz^3) \\
&= 5(x+y)((z^3 - x^3)(z-y) + 2x^2z^2 + xy^3 - y^3z + y^2z^2 + y^2z^2 - yz^3 \\
&\quad + x^2y^2 - x^2yz - 2x^2yz - 3xy^2z + 4xyz^2 - 2xz^3) \\
&= 5(x+y)((z^3 - x^3)(z-y) + xy^3 - y^3z + y^2z^2 + y^2z^2 - yz^3 \\
&\quad + x^2y^2 - x^2yz + 2x^2z(z-y) - 3xyz(y-z) + xyz^2 - 2xz^3) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz)(z-y) + xy^3 - y^2z(y-z) \\
&\quad + y^2z^2 - yz^3 + x^2y^2 - x^2yz + xyz^2 - 2xz^3) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z)(z-y) + xy^3 \\
&\quad + yz^2(y-z) + x^2y(y-z) + xyz^2 - 2xz^3) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y)(z-y) \\
&\quad + xy^3 + xyz^2 - 2xz^3) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y)(z-y) \\
&\quad + xy^3 + xyz^2 - xz^3 - xz^3)
\end{aligned}$$

$$\begin{aligned}
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y)(z-y) \\
&\quad + xy^3 + xz^2(y-z) - xz^3) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y)(z-y) \\
&\quad + xy^3 - xz^3 + xz^2(y-z)) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y)(z-y) \\
&\quad + x(y^3 - z^3) + xz^2(y-z)) \\
&= 5(x+y)((z^3 - x^3 + 2x^2z + 3xyz + y^2z - yz^2 - x^2y - xz^2)(z-y) \\
&\quad - x(z-y)(y^2 + yz + z^2)) \\
&= 5(x+y)(z-y)((z-x)(x^2 + xz + z^2) \\
&\quad + 2x^2z + 3xyz + y^2z - yz^2 - x^2y - xz^2 - x(y^2 + yz + z^2)) \\
&= 5(x+y)(z-y)((z-x)(x^2 + xz + z^2) \\
&\quad + 2x^2z + 3xyz + y^2z - yz^2 - x^2y - xz^2 - xy^2 - xyz - xz^2) \\
&= 5(x+y)(z-y)((z-x)(x^2 + xz + z^2) \\
&\quad + 2x^2z - 2xz^2 + 2xyz + y^2z - yz^2 - x^2y - xy^2) \\
&= 5(x+y)(z-y)((z-x)(x^2 + xz + z^2) \\
&\quad + 2xz(x-z) + 2xyz + y^2(z-x) - yz^2 - x^2y) \\
&= 5(x+y)(z-y)((z-x)(x^2 - xz + z^2 + y^2) \\
&\quad + xyz + xyz - yz^2 - x^2y) \\
&= 5(x+y)(z-y)((z-x)(x^2 - xz + z^2 + y^2) \\
&\quad + xyz + yz(x-z) - x^2y) \\
&= 5(x+y)(z-y)((z-x)(x^2 - xz + z^2 + y^2 - yz) \\
&\quad + xyz - x^2y) \\
&= 5(x+y)(z-y)((z-x)(x^2 + y^2 + z^2 - xz - yz) + xy(z-x))
\end{aligned}$$

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

ここで

$$\begin{aligned} (x + y - z)^2 &= x^2 + y^2 + z^2 + 2xy - 2xz - 2yz \\ (x + y - z)^2 - (xy - xz - yz) &= x^2 + y^2 + z^2 + (xy - xz - yz) \end{aligned} \quad (9)$$

よって

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

$x + y - z \equiv 0 \pmod{5}$ であるから

$$\begin{aligned} x + y &\equiv z \pmod{5} \\ z - x &\equiv y \pmod{5} \\ z - y &\equiv x \pmod{5} \end{aligned}$$

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

$$\begin{aligned} 5^4 &\mid \left((x + y - z)^2 - (xy - xz - yz) \right) \\ 5^2 &\mid (xy - xz - yz) \end{aligned}$$

(9) より

$$x^2 + y^2 + z^2 \equiv 0 \pmod{5} \quad (10)$$

$5 \nmid xyz$ なので、 $\theta = \{x, y, z\}$ のとき

$$\begin{aligned} \theta^4 &\equiv 1 \pmod{5} \\ \theta^2 &\equiv \pm 1 \pmod{5} \end{aligned}$$

よって得られる解は

$$x^2 + y^2 + z^2 \equiv \pm 1 \pmod{5}$$

または

$$x^2 + y^2 + z^2 \equiv \pm 3 \pmod{5}$$

これは (10) と反する。

□

1.3.3 $p \geq 7$

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

Definition 15 $L \perp R$ なので

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

Proof 16

a を法とする場合

$$x^p = (z - y) \left(\frac{p!}{(p-1)!1!} y^{p-1} + \frac{p!}{(p-2)!2!} y^{p-2} (z - y) + \cdots + \frac{p!}{1!(p-1)!} y (z - y)^{p-2} + (z - y)^{p-1} \right)$$
$$x \cdot x^{p-1} \equiv (z - y) (py^{p-1} + 0 + \cdots + 0) \pmod{a}$$
$$x \cdot x^{p-1} \equiv (z - y) py^{p-1} \pmod{a}$$

ここで $a \nmid x$, $a^p \mid (z - y)$ なので剰余において

$$\frac{(z - y)}{x} \not\equiv 1 \pmod{a}$$

$a \perp py$ であるから

$$x^{p-1} \not\equiv py^{p-1} \pmod{a}$$

p を法とする場合

$$x^p = (z - y) \left(\frac{p!}{(p-1)!1!} y^{p-1} + \frac{p!}{(p-2)!2!} y^{p-2} (z - y) + \cdots + \frac{p!}{1!(p-1)!} y (z - y)^{p-2} + (z - y)^{p-1} \right)$$
$$x \cdot x^{p-1} \equiv (z - y) (0 + \cdots + 0 + (z - y)^{p-1}) \pmod{p}$$
$$x \cdot x^{p-1} \equiv (z - y)(z - y)^{p-1} \pmod{p}$$

ここで $p \nmid x$, $p \mid (z - y)$ なので剰余において

$$\frac{(z - y)}{x} \equiv 1 \pmod{p}$$

よって

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

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

p を法とするとき剰余において以下の式が成り立つ。

$$\begin{aligned}\frac{(z - y)}{x} &\equiv 1 \pmod{p} \\ \frac{(z - x)}{y} &\equiv 1 \pmod{p} \\ \frac{(x + y)}{z} &\equiv 1 \pmod{p}\end{aligned}$$

また $p' = (x + y - z)$ と省略する。

$$\begin{aligned}p'^5 &\equiv 5z y x (p'^2 - (xy - xz - yz)) + x^5 + y^5 - z^5 \\ p'^5 &\equiv 5x y z p'^2 - 5x y z (xy - xz - yz) + x^5 + y^5 - z^5 \\ p'^5 - 5x y z p'^2 &\equiv -5x y z (xy - xz - yz) + x^5 + y^5 - z^5 \\ p'^5 - 5x y z p'^2 &\equiv -5x y z (x(y - z) - yz) + x^5 + y^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv -5x y z (-x^2 - yz) + x^5 + y^5 - z^5\end{aligned}$$

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

上式を代入する。

$$\begin{aligned}p'^2(p'^3 - 5x y z) &\equiv 5x y z (x^2 + yz) + z(5y^4 - 10y^3z + 10y^2z^2 - 5yz^3) + (x + y)^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv z(5x y (x^2 + yz) + 5y^4 - 10y^3z + 10y^2z^2 - 5yz^3) + (x + y)^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv 5z(x y (x^2 + yz) + y^4 - 2y^3z + 2y^2z^2 - yz^3) + (x + y)^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv 5y z (x(x^2 + yz) + y^3 - 2y^2z + 2yz^2 - z^3) + (x + y)^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv 5y z (x^3 + x y z + y^3 + 2y z (z - y) - z^3) + (x + y)^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv 5y z (x y z + 2x y z + x^3 + y^3 - z^3) + (x + y)^5 - z^5 \\ p'^2(p'^3 - 5x y z) &\equiv 5y z (3x y z + x^3 + y^3 - z^3) + (x + y)^5 - z^5\end{aligned}$$

$$\begin{aligned}(x + y - z)^3 &= 3(x + y)(z - x)(z - y) + x^3 + y^3 - z^3 \\ (x + y - z)^3 &\equiv 3z y x + x^3 + y^3 - z^3\end{aligned}$$

上式を代入する。

$$p'^2(p'^3 - 5x y z) \equiv 5y z (x + y - z)^3 + (x + y)^5 - z^5$$

$5y z (x + y - z)^3 = 5y z (x + y - z)_1^3$ と置く。

$$p'^2(p'^3 - 5xyz) \equiv 5yz(x+y-z)_1^3 + (x+y)^5 - z^5$$

ところで $(x+y-z)$ は $p \mid (x+y-z)$ の関係における合同式の最少要素である。
よって係数 k_1 を用いて上式を表すと

$$(x+y-z)^2((x+y-z)^3 - 5xyz) \equiv 5yzk_1(x+y-z)^3 + (x+y)^5 - z^5 \quad (11)$$

$$\begin{aligned} (x+y)^5 - z^5 &= ((x+y-z) + z)^5 - z^5 \\ &= (x+y-z)^2(\dots) + 5(x+y-z)z^4 \equiv (x+y-z)^2 \\ &5z^4 \not\equiv 0 \pmod{p} \quad (p \geq 7) \end{aligned}$$

以下同様に

$$\begin{aligned} p'^5 - 5xyzp'^2 &\equiv -5xyz(xy - xz - yz) + x^5 + y^5 - z^5 \\ p'^5 - 5xyzp'^2 &\equiv -5xyz(xy - (x+y)z) + x^5 + y^5 - z^5 \\ p'^2(p'^3 - 5xyz) &\equiv -5xyz(xy - z^2) + x^5 + y^5 - z^5 \end{aligned}$$

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

上式を代入する。

$$\begin{aligned} p'^2(p'^3 - 5xyz) &\equiv -5xyz(xy - z^2) - x(5y^4 + 10y^3x + 10y^2x^2 + 5yx^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5xyz) &\equiv -5xyz(xy - z^2) - 5x(y^4 + 2y^3x + 2y^2x^2 + yx^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5xyz) &\equiv -5x(yz(xy - z^2) + y^4 + 2y^3x + 2y^2x^2 + yx^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5xyz) &\equiv -5xy(z(xy - z^2) + y^3 + 2y^2x + 2yx^2 + x^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5xyz) &\equiv -5xy(xyz - z^3 + y^3 + 2xy(x+y) + x^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5xyz) &\equiv -5xy(3xyz - z^3 + y^3 + x^3) + x^5 - (z-y)^5 \end{aligned}$$

$$\begin{aligned} (x+y-z)^2((x+y-z)^3 - 5xyz) &\equiv -5xy(x+y-z)_2^3 + x^5 - (z-y)^5 \\ (x+y-z)^2((x+y-z)^3 - 5xyz) &\equiv -5xyk_2(x+y-z)^3 + x^5 - (z-y)^5 \end{aligned}$$

$$\begin{aligned} x^5 - (z-y)^5 &= x^5 + (y-z)^5 \\ &= x^5 + ((x+y-z) - x)^5 \\ &= (x+y-z)^2(\dots) + 5(x+y-z)x^4 \equiv (x+y-z)^2 \\ &5x^4 \not\equiv 0 \pmod{p} \quad (p \geq 7) \end{aligned}$$

□

1.4 Case 2 ($p \mid xyz$)

Proposition 17

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

Proof 18

$p \mid x$, $p \mid (z - y)$ 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 19

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

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

$$(z - x) - (x + y) = b^p - c^p$$

$$-(x + y - z) - x = b^p - c^p \equiv 0 \pmod{p}$$

$$(z - y) - 2x = b^p - c^p \equiv 0 \pmod{p}$$

$p \mid L \Leftrightarrow p \mid R$ 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。

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

$$p^2 \mid x \tag{12}$$

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

$x^p = (z - y)p\alpha^p$ と置き、上式に代入する。

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

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \quad (13)$$

(12) より $x = ap^2\alpha$

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

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

(13) , $p \perp \alpha^p$ より

$$p^1 \mid K \text{ でなければならぬ。}$$

よって

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

一般的に

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

□

また

$$\begin{aligned} x + y - z &= x - (z-y) \\ x + y - z &= p^n a \alpha - p^{pn-1} a^p \\ x + y - z &= p^n (a \alpha - p^{n(p-1)-1} a^p) \\ p^n &\mid x + y - z \end{aligned} \quad (14)$$

Proposition 20

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

Proof 21

$x + y - z = p^n abcT$ と素数 t を仮定する。

$$\begin{array}{ll} t \mid T & t \mid x + y - z \\ t \perp xyz & t \perp (x + y)(z - x)(z - y) \end{array}$$

(14) より $t \neq p$ と置く。

t は Case 1 における p と同値である。(11) より

$$5z^4 \equiv 0 \pmod{t} \quad (t \neq 5 \text{ のとき}) \quad 5z^4 \equiv 0 \pmod{t^2} \quad (t = 5 \text{ のとき})$$

よって x, y, z の何れか t の積を有する。

$$t \mid xyz \quad , \quad t \mid z \Rightarrow t \mid x + y$$

$$\begin{aligned} ((x + y) - z)^p &= -z^p + \frac{p!}{(p-1)!1!} z^{p-1}(x + y) - \frac{p!}{(p-2)!2!} z^{p-2}(x + y)^2 + \frac{p!}{(p-3)!3!} z^{p-3}(x + y)^3 \\ &\quad \cdots - \frac{p!}{1!(p-1)!} z(x + y)^{p-1} + (x + y)^p \end{aligned} \quad (15)$$

$$x^p + y^p = (x + y) \left(py^{p-1} - \frac{p!}{(p-2)!2!} y^{p-2}(x + y) + \cdots - \frac{p!}{1!(p-1)!} y(x + y)^{p-2} + (x + y)^{p-1} \right) \quad (16)$$

$z^p = x^p + y^p$ が成り立つとして、(16) を (15) へ代入する。

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

よって

$$t \mid py^{p-1}$$

これは $z \perp y$ に矛盾する。 □

1.4.1 $p = 3$

Proposition 22 $x^3 + y^3 \neq z^3$

Proof 23 $p \perp yz$ のとき剰余において以下の式が成り立つ。

$$\frac{(z-x)}{y} \equiv 1 \pmod{p}, \quad \frac{(x+y)}{z} \equiv 1 \pmod{p}$$

また $p' = (x+y-z)$, $x' = (z-y)$ と省略する。

$$\begin{aligned} (x+y-z)^5 &= 5(x+y)(z-y)(z-x) \left((x+y-z)^2 - (xy-xz-yz) \right) + x^5 + y^5 - z^5 \\ p'^5 &\equiv 5z(z-y)y(p'^2 - (xy-xz-yz)) + x^5 + y^5 - z^5 \\ p'^5 &\equiv 5yz(z-y)p'^2 - 5yzx'(xy-xz-yz) + x^5 + y^5 - z^5 \\ p'^5 - 5yz(z-y)p'^2 &\equiv -5yzx'(xy-xz-yz) + x^5 + y^5 - z^5 \\ p'^5 - 5yz(z-y)p'^2 &\equiv -5yzx'(xy - (x+y)z) + x^5 + y^5 - z^5 \\ p'^2(p'^3 - 5yz(z-y)) &\equiv 5yzx'((x+y)z - xy) + x^5 - (z^5 - y^5) \\ z^5 - y^5 &= (z-y)(5y^4 + 10y^3(z-y) + 10y^2(z-y)^2 + 5y(z-y)^3) + (z-y)^5 \\ z^5 - y^5 &= x'(5y^4 + 10y^3x' + 10y^2x'^2 + 5yx'^3) + (z-y)^5 \end{aligned}$$

上式を代入する。

$$\begin{aligned} p'^2(p'^3 - 5yz(z-y)) &\equiv 5x'yz((x+y)z - xy) - x'(5y^4 + 10y^3x' + 10y^2x'^2 + 5yx'^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5yz(z-y)) &\equiv 5x'yz(z^2 - xy) - 5x'y(y^3 + 2y^2x' + 2yx'^2 + x'^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5yz(z-y)) &\equiv 5x'yz^3 - 5x'xy^2z - 5x'y^4 - 5x'y(2y^2x' + 2yx'^2 + x'^3) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5yz(z-y)) &\equiv 5x'yz^3 - 5x'y^4 - 5x'xy^2z - 5x'^2y(2y^2 + 2yx' + x'^2) + x^5 - (z-y)^5 \\ p'^2(p'^3 - 5yz(z-y)) &\equiv 5x'y(z^3 - y^3) - 5x'xy^2z - 5x'^2y(2y^2 + 2yx' + x'^2) + x^5 - (z-y)^5 \\ z^3 - y^3 &= (z-y)(y^2 + yz + z^2) \\ &= (z-y)((z-y)^2 + 3yz) \end{aligned}$$

$$p'^2(p'^3 - 5yz(z-y)) \equiv 5y(z-y)^2((z-y)^2 + pyz) - 5x'xy^2z - 5x'^2y(\dots) + x^5 - (z-y)^5$$

$p^n \mid p' = (x+y-z)$, $p^{3n-1} \mid x' = (z-y)$ なるので

$$\begin{aligned} p'^2(p'^{3n} - 5yza^3p^{3n-1}) &\equiv 5ya^6p^{6n-2}(p) - 5a^3p^{3n-1}ap^n\alpha y^2z - 5a^6p^{6n-2}y(\dots) + x^5 - (z-y)^5 \\ p^{5n-1}(abc)^2(p(abc)^3 - 5yza^3) &\equiv 5ya^6p^{6n-1} - 5a^4\alpha y^2zp^{4n-1} - 5a^6y(\dots)p^{6n-2} + p^{5n}(a\alpha)^5 - (a^3p^{3n-1})^5 \end{aligned}$$

$p \neq 5$, $n \geq 2$ であるから p の指数のみ注目すると

$$\begin{aligned} p^{5n-1} &\equiv p^{6n-1} - p^{4n-1} - p^{6n-2} + p^{5n} - p^{15n-5} \\ p^{5n-1} &\not\equiv p^{5n-1}(p^n - p^{n-1} + p - p^{10n-4}) - p^{4n-1} \end{aligned}$$

□

1.4.2 $p \geq 5$

Proposition 24 $x^p + y^p \neq z^p$

Proof 25

$z - (x + y) = k > 0$ と置く。

$$\begin{aligned} z &= x + y + k \\ z^p &= x^p + y^p + k^p + p(\dots) \end{aligned}$$

$z^p = x^p + y^p$ より

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

$p(\dots) > 0$ だから

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

よって

$$p^n abc = x + y - z > 0 \tag{17}$$

$$(x + y - z)^3 = 3(x + y)(z - x)(z - y) + x^3 + y^3 - z^3$$

$$(p^n abc)^3 = 3(x + y)(z - x)(z - y) + x^3 + y^3 - z^3$$

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

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

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

(17) より $abc > 0$

$p \geq 5$ より

$$p^{3n}(abc)^3(1 - 3p^{n(p-3)-1}(abc)^{p-3}) < 0 \tag{18}$$

$A < B < C$, $A^n + B^n = C^n$ のとき

$$A^n B^m + B^{n+m} < C^{n+m}$$

$$A^{n+m} + B^{n+m} < A^n B^m + B^{n+m} < C^{n+m}$$

$$A^{n+m} + B^{n+m} < C^{n+m}$$

$$x^p + y^p = z^p \ (p \geq 5) \Rightarrow x^3 + y^3 - z^3 > 0 \tag{19}$$

(18) と (19) は矛盾する。 □

References

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