The idea of the Arithmetica

Hajime Mashima

August 15, 2016

Abstract

About 375 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 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

最後に残ったフェルマー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、「フェルマーは本当に証明していたのだろうか?」という疑問が増してくる。しかし別の見方をすれば、証明可能な命題と分かった事によりフェルマーが証明していた可能性も示唆している。

この証明を試みる上で代数学的手法はもちろん、フェルマー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行っている。

1.1 Fermat's Last Theorem とは

Proposition 1 (Fermat's Last Theorem) 自然数 n の冪について, 以下の等式を満たす異なる x, y, z の自然数解は存在しない。

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

1.2 The Barlow-Abel Equations

Definition 2

- $x < y < z$
- x , y , z は互いに素とする。

Theorem 3 (The Barlow-Abel Equations)

p が奇素数であるとき以下の等式が成り立つ。$[1, p.45]$

$$x^p + y^p = (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 \cdots - xy^{p-2} + y^{p-1})$$
$$z^p - y^p = (z-y)(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 \cdots + zy^{p-2} + y^{p-1})$$
$$z^p - x^p = (z-x)(z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 \cdots + zx^{p-2} + x^{p-1})$$

Proposition 4

$$\begin{aligned} x + y &\not\equiv 0 \pmod{z} \\ z - y &\not\equiv 0 \pmod{x} \\ z - x &\not\equiv 0 \pmod{y} \end{aligned} \tag{1}$$

Proof 5 $z > x + y$ ならば、$\mathbf{N}$ を自然数として

$$z - (x+y) = \mathbf{N} > 0 \quad \text{とおける。}$$

$$z = x + y + \mathbf{N}$$
$$z^p = (x + y + \mathbf{N})^p$$

係数が 1 でない項の和は $p\mathbb{N}$ と表わせるので

$$z^p = x^p + y^p + \mathbf{N}^p + p\mathbb{N}$$
$$z^p = x^p + y^p \text{であるから}$$
$$0 = \mathbf{N}^p + p\mathbb{N}$$

しかし x , y , $\mathbf{N} > 0$ なので解が存在しないのは明らかである。

$$0 \neq \mathbf{N}^p + p\mathbb{N}$$

よって

$$x + y > z \tag{2}$$

$$2z = z + z > x + y > z \tag{3}$$

$x + y = kz$ ならば $k \geq 2$ となり、これは (3) に反する。よって

$$x + y \not\equiv 0 \pmod{z}$$

(2) より

$$\begin{aligned} x + y - z &> 0 \\ x - (z - y) &> 0 \\ y - (z - x) &> 0 \end{aligned}$$

$x > (z - y)$, $y > (z - x)$ であるから

$$\begin{aligned} z - y &\not\equiv 0 \pmod{x} \\ z - x &\not\equiv 0 \pmod{y} \end{aligned}$$

□

1.3 $(x + y - z)^p$ の考察

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

$$\begin{aligned} x^p =& ((x + y - z) + (z - y))^p = (z - y)^p + \frac{p!}{(p-1)!1!}(z - y)^{p-1}(x + y - z) \\ &+ \frac{p!}{(p-2)!2!}(z - y)^{p-2}(x + y - z)^2 \cdots + \frac{p!}{1!\,(p-1)!}(z - y)(x + y - z)^{p-1} + (x + y - z)^p \end{aligned} \tag{4}$$

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

Theorem 6　p は奇素数。

$$x^p + y^p = (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 \cdots - xy^{p-2} + y^{p-1}) \quad (5)$$
$$z^p - y^p = (z-y)(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 \cdots + zy^{p-2} + y^{p-1}) \quad (6)$$
$$z^p - x^p = (z-x)(z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 \cdots + zx^{p-2} + x^{p-1}) \quad (7)$$

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

$z^p = x^p + y^p$ が成り立つとして、(5) を代入する

$$(x+y-z)^p = -(x+y)\Big(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 \cdots - xy^{p-2} + y^{p-1}$$
$$- \frac{p!}{(p-1)!1!}z^{p-1} + \frac{p!}{(p-2)!2!}z^{p-2}(x+y) - \frac{p!}{(p-3)!3!}z^{p-3}(x+y)^2 \quad (8)$$
$$\cdots + \frac{p!}{1!(p-1)!}z(x+y)^{p-2} - (x+y)^{p-1}\Big)$$

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

$x^p = z^p - y^p$ が成り立つとして、(6) を代入する

$$(x+y-z)^p = (z-y)\Big(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \cdots + zy^{p-2} + y^{p-1}$$
$$- \frac{p!}{(p-1)!1!}x^{p-1} + \frac{p!}{(p-2)!2!}x^{p-2}(z-y) - \frac{p!}{(p-3)!3!}x^{p-3}(z-y)^2 \quad (9)$$
$$\cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1}\Big)$$

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

$y^p = z^p - x^p$ が成り立つとして、(7) を代入する

$$(x+y-z)^p = (z-x)\Big(z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \cdots + zx^{p-2} + x^{p-1}$$
$$- \frac{p!}{(p-1)!1!}y^{p-1} + \frac{p!}{(p-2)!2!}y^{p-2}(z-x) - \frac{p!}{(p-3)!3!}y^{p-3}(z-x)^2 \quad (10)$$
$$\cdots + \frac{p!}{1!(p-1)!}y(z-x)^{p-2} - (z-x)^{p-1}\Big)$$

Definition 7

$$\begin{aligned} c \mid z \\ a \mid x \\ b \mid y \end{aligned} \tag{11}$$

x , y , z が互いに素ならば

$$\begin{aligned} z &\not\equiv 0 \pmod{a\ ,\ b} \\ x &\not\equiv 0 \pmod{b\ ,\ c} \\ y &\not\equiv 0 \pmod{c\ ,\ a} \end{aligned}$$

Proposition 8 (4)〜(11) より

$$\begin{aligned} c^p \mid x+y \\ a^p \mid z-y \\ b^p \mid z-x \\ abc \mid x+y-z \end{aligned} \tag{12}$$

(8)〜(10) より
$(x+y)$, $(z-y)$, $(z-x) \mid (x+y-z)^p$

(4) より $(x+y)$, $(z-y)$, $(z-x)$ は互いに素であるから

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

Theorem 9　p は奇素数。

$$
\begin{aligned}
x^p + y^p &= (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 \cdots - xy^{p-2} + y^{p-1}) \\
z^p - y^p &= (z-y)(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 \cdots + zy^{p-2} + y^{p-1}) \\
z^p - x^p &= (z-x)(z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 \cdots + zx^{p-2} + x^{p-1})
\end{aligned}
$$

Definition 10

$$
\begin{aligned}
l &= (x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 \cdots - xy^{p-2} + y^{p-1}) \\
m &= (z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 \cdots + zy^{p-2} + y^{p-1}) \\
n &= (z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 \cdots + zx^{p-2} + x^{p-1})
\end{aligned}
\tag{13}
$$

$$
\begin{aligned}
x^p + y^p &= z^p = (x+y)l \\
z^p - y^p &= x^p = (z-y)m \\
z^p - x^p &= y^p = (z-x)n
\end{aligned}
$$

$$
\begin{aligned}
z^p &= ((x+y)-z)l + zl \\
x^p &= (x+(z-y))m - xm \\
y^p &= (y+(z-x))n - yn
\end{aligned}
\tag{14}
$$

(1) より

$$
\begin{aligned}
(x+y) - z &\not\equiv 0 \pmod{z} \\
x + (z-y) &\not\equiv 0 \pmod{x} \\
y + (z-x) &\not\equiv 0 \pmod{y}
\end{aligned}
\tag{15}
$$

(14)、(15) より

$$
\begin{aligned}
l &\equiv 0 \pmod{z} \\
m &\equiv 0 \pmod{x} \\
n &\equiv 0 \pmod{y}
\end{aligned}
$$

また、(11) より

$$
\begin{aligned}
l &\equiv 0 \pmod{c} \\
m &\equiv 0 \pmod{a} \\
n &\equiv 0 \pmod{b}
\end{aligned}
\tag{16}
$$

1.4 互いに素に関して

1.4.1 公約数 a ($z-y>1$ のとき)

Proposition 11 フェルマーの命題が偽ならば, 互いに素な x,y,z の組は必ず存在する。そのような組が存在しないならばフェルマーの命題は真である。

x を基準として y,z を自然数の加算値 s,t で表現する ($x<y<z$)。

$$\begin{aligned} z&=x+s+t & y&=x+s \\ s&=y-x & t&=z-y \end{aligned} \tag{17}$$

$$((x+s)+t)^p=(x+s)^p+\frac{p!}{(p-1)!1!}(x+s)^{p-1}t\cdots+\frac{p!}{1!\,(p-1)!}(x+s)\,t^{p-1}+t^p$$

$$z^p=y^p+\frac{p!}{(p-1)!1!}(x+s)^{p-1}t\cdots+\frac{p!}{1!\,(p-1)!}(x+s)\,t^{p-1}+t^p$$

$x^p=z^p-y^p$, $t=z-y$ より

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

(13) より $x^p=(z-y)m$ なので

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

(12) , (16) より

$$\begin{aligned} \frac{p!}{(p-1)!1!}(x+s)^{p-1}&\equiv 0 \pmod a \\ p\,(x+s)^{p-1}&\equiv 0 \pmod a \end{aligned}$$

p は m の展開式 2 項以降も存在するので $p=a$, $p\neq a$ によらず

$$\begin{aligned} (x+s)^{p-1}&\equiv 0 \pmod a & & \\ x^{p-1}+xs(\cdots)+s^{p-1}&\equiv 0 \pmod a & & (11)\text{ より} \\ s^{p-1}&\equiv 0 \pmod a & & t>1\text{ より }s\neq 1 \end{aligned}$$

よって s と a は公約数を持つ。

(17) より $t>1$ のとき x,y,z は公約数を持つ。 (18)

1.4.2　公約数 b

x を基準として y, z を自然数の加算値 s, t で表現する $(x < y < z)$。

$$\begin{aligned} z &= x + s + t & y &= x + s \\ 2x + s &= x + y & s + t &= z - x \end{aligned} \tag{19}$$

$$(x + (s+t))^p = x^p + \frac{p!}{(p-1)!1!}x^{p-1}(s+t) \cdots + \frac{p!}{1!\,(p-1)!}x\,(s+t)^{p-1} + (s+t)^p$$

$y^p = z^p - x^p$, $s + t = z - x$ より

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

(13) より $y^p = (z-x)n$ なので

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

(12) , (16) より

$$\begin{aligned} \frac{p!}{(p-1)!1!}x^{p-1} &\equiv 0 \pmod{b} \\ px^{p-1} &\equiv 0 \pmod{b} \end{aligned}$$

p は n の展開式 2 項以降も存在するので $p = b$, $p \neq b$ によらず

$$x^{p-1} \equiv 0 \pmod{b}$$

x と b は公約数を持つ。

また、$y \neq x$ より $s \neq 0$
$t = 1$ ならば $s + t = z - x \neq 1$
よって

$$(11) \text{ より } x, y, z \text{ は公約数を持つ。} \tag{20}$$

1.4.3　公約数 c

$$(-x+(2x+s))^p = -x^p + \frac{p!}{(p-1)!1!}x^{p-1}(2x+s)\cdots - \frac{p!}{1!\,(p-1)!}x\,(2x+s)^{p-1} + (2x+s)^p$$

$y^p + x^p = z^p$, $2x+s = x+y$ より

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

(13) より $z^p = (x+y)l$ なので

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

(12) , (16) より

$$\begin{aligned} \frac{p!}{(p-1)!1!}x^{p-1} &\equiv 0 \pmod{c} \\ px^{p-1} &\equiv 0 \pmod{c} \end{aligned}$$

p は l の展開式 2 項以降も存在するので $p = c$, $p \neq c$ によらず

$$x^{p-1} \equiv 0 \pmod{c}$$

x と c は公約数を持つ。

また、$x+y \neq 1$
よって

$$(11) \text{ より } x, y, z \text{ は公約数を持つ。} \tag{21}$$

(18) , (20) , (21) より $x^p + y^p = z^p$ ならば x, y, z は必ず公約数を持つ。
これは互いに素な x, y, z の組が存在することに反する。よって

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

References

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