The idea of the Arithmetica

Hajime Mashima

July 7, 2016

Abstract

Ago 360 years, 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 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は逆の可能性も示唆していると言える。この証明を試みる上で必要なのは当時の数学的手法はもちろん、フェルマーの人柄や当時の行い、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が主体となっている。

1.1　フェルマーの最終定理とは

Proposition 1 (フェルマーの最終定理) 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。(以降、フェルマーの命題とする。)

$$X^n + Y^n = Z^n \quad (XYZ \neq 0 \ , \ n \geq 3)$$

1.2　三項の考察

Corollary 2 フェルマーの命題が偽であるならば、3 以上の素数 p において以下の合同式を満たす。

$$X + Y - Z \equiv 0 \pmod{p}$$

Proof 3　係数が 1 でない数式は $p\mathbb{N}(p$ は奇素数) と表わせるので

$$(X+Y-Z)^p = X^p + Y^p - Z^p + p\mathbb{N}$$

$X^p + Y^p - Z^p = 0$ であるから

$$(X+Y-Z)^p = p\mathbb{N}$$

$X + Y - Z$ は p を約数に持つので

$$X + Y - Z \equiv 0 \pmod{p}$$

□

この時 $X + Y > Z$ でなければならない。

Proof 4　$Z > X + Y$ ならば、$\mathbf{N}$ を自然数として

$$Z - (X+Y) = p\mathbf{N} > 0 \quad \text{と仮定できる。}$$

$$Z = X + Y + p\mathbf{N}$$
$$Z^p = (X + Y + p\mathbf{N})^p$$

展開した式の係数が 1 でない数式は $p\mathbb{N}$ と表わせるので

$$Z^p = X^p + Y^p + (p\mathbf{N})^p + p\mathbb{N}$$
$$Z^p = X^p + Y^p \text{であるから}$$
$$0 = (p\mathbf{N})^p + p\mathbb{N}$$

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

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

□

1.3 $t > 1$, $s \neq 1$ のとき

Proposition 5 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 $(x < y < z)$。

$$\begin{array}{ll} y = x + s & z = x + s + t \\ y^p = (x + s)^p & z^p = (x + s + t)^p \end{array} \tag{1}$$

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

$x^p = z^p - y^p$ より

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

right より $x = k_1 t$ とおける。 (2)

$$k_1^p t^p = p\,(k_1 t + s)^{p-1} t + \frac{p!}{(p-2)!2!}(k_1 t + s)^{p-2} t^2 \cdots + \frac{p!}{1!\,(p-1)!}(k_1 t + s)\, t^{p-1} + t^p$$

$p \neq t$, $p = t$ に関わらず

$(k_1 t + s)^{p-1} \equiv 0 \pmod{t}$
$k_1^{p-1} t^{p-1} + k_1 ts(\cdots) + s^{p-1} \equiv 0 \pmod{t}$
よって
$s^{p-1} \equiv 0 \pmod{t}$ $t > 1$ より $s \neq 1$

ここで s_d を s の約数とおくと、以下の条件が考えられる。

$$t = s_d k_2 \quad , \ s = t \quad , \ s = tk_3 \qquad (s_d | s) \tag{3}$$

(1), (2), (3) より x, y, z は公約数を持つので互いに素である前提に反する。

1.4 $t=1$, $s=1$ のとき

$$y=x+1 \qquad\qquad z=x+1+1$$

Theorem 6 p が奇素数であるとき以下の等式が成り立つ。[*1, p.45*]

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

t , $s=1$ であるから、(6) を参照する。

x	y	z	参照
odd	odd	even	(4)
even	odd	odd	(5)
odd	even	odd	(6)

奇素数の冪について

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

$y^p=z^p-x^p$ が成り立つと仮定して、(6) を代入すると

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

$z-x=2$ なので

$$(y-2)^p \equiv 0 \pmod 2$$

$y=$even なので $y=2k_4$とおける。よって

$$\begin{aligned}(2k_4-2)^p &\equiv 0 \pmod{z-x}\\ 2^p\,(k_4-1)^p &\equiv 0 \pmod{z-x} \qquad (k_4\neq 1)\end{aligned}$$

$$\begin{aligned}2^{p-1}(k_4-1)^p = z^{p-1}&+z^{p-2}x+z^{p-3}x^2+z^{p-4}x^3+\cdots+zx^{p-2}+x^{p-1}\\ &-\frac{p!}{(p-1)!1!}y^{p-1}+\frac{p!}{(p-2)!2!}y^{p-2}(z-x)-\frac{p!}{(p-3)!3!}y^{p-3}(z-x)^2\\ &\cdots+\frac{p!}{1!(p-1)!}y(z-x)^{p-2}-(z-x)^{p-1}\end{aligned}$$

$$\text{left}=(z-x)^{p-1}(k_4-1)^p=\text{even} \qquad (7)$$

right zx 項は odd で $p-2$ (odd) 個ある。また $z^{p-1}+x^{p-1}$ が even なので

$$\text{odd} \quad = \quad z^{p-1}+z^{p-2}x+z^{p-3}x^2+z^{p-4}x^3+\cdots+zx^{p-2}+x^{p-1}$$

後に続く数式の $y,(z-x)$ は even なので

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

よって right は odd となり、これは left が even となる (7) に反する。

1.5 $t = 1$, $s > 1$ のとき

$$y = x + s \qquad\qquad z = x + s + 1$$

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

$x^p = z^p - y^p$ より

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

上式より

$$\begin{aligned} x^p - 1 &\equiv 0 \pmod p \\ x^p - x &\equiv 0 \pmod p \text{ より} \\ x - 1 &\equiv 0 \pmod p \end{aligned} \tag{8}$$

よって x と p が互いに素であるからフェルマーの小定理が成り立つはず

$$x^{p-1} - 1 \equiv 0 \pmod p \tag{9}$$

(8) より

$$x^p - 1 \equiv 0 \pmod p$$

(9) より

$$\begin{aligned} xpm_1 + x^{p-1} - 1 &\equiv 0 \pmod p \\ x(pm_1 + x^{p-2}) - 1 &\equiv 0 \pmod p \\ pm_1 + x^{p-2} &= x^{p-1} \end{aligned}$$

x と p が互いに素ならば p の積は残るので

$$\begin{aligned} x^{p-2}\left(\frac{m_1}{x^{p-2}}p + 1\right) &= x^{p-2} \cdot x \\ x &\equiv 1 \pmod p \\ x^p &\equiv x^{p-1} \pmod p \end{aligned}$$

よって x は p と互いに素である事と矛盾する。

References

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