The idea of the Arithmetica

Hajime Mashima

July 23, 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 **1**
1.1 Fermat's Last Theorem とは 2
1.2 三項の考察 2

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 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。(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。 (1)

Proof 4 $z > x + y$ ならば、$\mathbf{N}$ を自然数として

$$z - (x+y) = \mathbf{N} > 0 \quad \text{と仮定できる。}$$

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

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

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

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。

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

□

Theorem 5　p が奇素数であるとき以下の等式が成り立つ。[*1, p.45*]

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

$z > y > x$ とおく。

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

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

$-((x+y)-z)^p$ を (3) へ代入する。

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

(2) を代入して

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

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

(2) より $x^p+y^p=z^p$ ならば

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

(1) より満たすべき条件は

$$
\begin{aligned}
x+y-z&=z\\
x+y&=2z\\
x&=2z-y
\end{aligned}
\tag{4}
$$

$x>z$ となるため再定義する。

Definition 6

$$x=z_1 \quad y=-y_1 \quad z=x_1$$

$$z_1^p-y_1^p=x_1^p \qquad (z_1>(y_1\ ,\ x_1)>1)$$

(4) より

$$z_1-y_1=2x_1$$

よって

$$x_1+y_1-z_1<0$$

(1) より $x_1^p+y_1^p\neq z_1^p$

References

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