The idea of the Arithmetica

Hajime Mashima

August 3, 2016

Abstract

Ago 379 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 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 Commutative

Theorem 2 p が奇素数であるとき以下の等式が成り立つ。[*1*, *p.45*]

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

Example 3

$$x^p + y^p = z^p$$

$$z \leftrightarrow x \ , \ y \to -y$$

$$z^p - y^p = x^p$$

Example 4 (1) より

$$\begin{gathered} x^p + y^p = (x+y)(x^{p-1} - x^{p-2}y + \cdots) \\ x \to (z-y) \ , \ y \to (z-x) \\ (z-y)^p + (z-x)^p = ((z-y)+(z-x))((z-y)^{p-1} - (z-y)^{p-2}(z-x) + \cdots) \\ z \to (x+y) \\ ((x+y)-y)^p + ((x+y)-x)^p = (((x+y)-y)+((x+y)-x))(((x+y)-y)^{p-1} - \cdots) \\ x^p + y^p = (x+y)(x^{p-1} - x^{p-2}y + \cdots) \end{gathered} \quad (4)$$

Lemma 5

$$\begin{gathered} x^p + y^p = z^p \\ \text{(4) より} \\ x \to (z-y) \ , \ y \to (z-x) \\ (z-y)^p + (z-x)^p = z^p \\ z \to (x+y) \\ x^p + y^p = (x+y)^p \end{gathered}$$

$x^p + y^p = z^p$ ならば $x + y \neq z$

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

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

$x^p + y^p = z^p$ より

$$\begin{aligned} z^p =&(z-x)^p - \frac{p!}{(p-1)!1!}(z-x)^{p-1}z + \frac{p!}{(p-2)!2!}(z-x)^{p-2}z^2 \\ &\cdots - \frac{p!}{2!\,(p-2)!}(z-x)^2 z^{p-2} + \frac{p!}{1!\,(p-1)!}(z-x)z^{p-1} \end{aligned} \tag{5}$$

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

(4) より
$x \to (z-y)\ ,\ y \to (z-x)$

$$z^p \neq y^p - \frac{p!}{(p-1)!1!}y^{p-1}z + \frac{p!}{(p-2)!2!}y^{p-2}z^2$$
$$\cdots - \frac{p!}{2!\,(p-2)!}y^2 z^{p-2} + \frac{p!}{1!\,(p-1)!}yz^{p-1}$$

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

$z \to (x+y)$

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

Proof 6 Replace the right-hand side only

$$
\begin{aligned}
& z^p = x^p + y^p \\
x \to (z-y)\ ,\ y \to (z-x) & \\
& z^p = (z-y)^p + (z-x)^p
\end{aligned}
\tag{6}
$$

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

(5) より

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

(6) より

$x \to (z-y)\ ,\ y \to (z-x)$

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

$z \to (x+y)$

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

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

$x^p + y^p = z^p$ より

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

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

$$\begin{aligned} 0 =& (y-(x+y))^p - y^p + (x+y)^p \\ & + (x-(x+y))^p - x^p + (x+y)^p \end{aligned}$$

$$\begin{aligned} 0 =& - x^p - y^p + (x+y)^p \\ & - y^p - x^p + (x+y)^p \end{aligned}$$

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

References

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