

# Fermat's Last Theorem

Hajime Mashima

## 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.

## 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。

**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。

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

これは以下と同値である。

$$x^p + y^p \neq z^p \quad (p \geq 3, \quad x, y, z \text{ は一つが偶数で互いに素})$$

**Definition 2**

$$\theta \perp 6xyz$$

**Proposition 3**  $x^p + y^p \not\equiv z^p \pmod{\theta}$ 

$\theta \perp xyz$  ならば、その逆元が存在するので以下のように表すことができる。

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \pmod{\theta}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} &\equiv x^p y^p \pmod{\theta} \\ stz^{p-1} &\equiv xy^p \pmod{\theta} \end{aligned} \tag{1}$$

$$\begin{aligned} tx^{p-1} \cdot uy^{p-1} &\equiv y^p z^p \pmod{\theta} \\ tux^{p-1} &\equiv yz^p \pmod{\theta} \end{aligned} \tag{2}$$

$$\begin{aligned} sz^{p-1} \cdot uy^{p-1} &\equiv x^p z^p \pmod{\theta} \\ suy^{p-1} &\equiv x^p z \pmod{\theta} \end{aligned} \tag{3}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} \cdot uy^{p-1} &\equiv x^p y^p z^p \pmod{\theta} \\ stu &\equiv xyz \pmod{\theta} \end{aligned} \tag{4}$$

$$\begin{aligned}sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\tu \cdot sz^{p-1} + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta}\end{aligned}$$

(4) より

$$\begin{aligned}xyz^p + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta} \\xy(x^p + y^p) + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta} \\x^{p+1}y + xy^{p+1} + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta} \\x^{p+1}y + t^2ux^{p-1} &\equiv tu^2y^{p-1} - xy^{p+1} \pmod{\theta} \\x^{p+1}y + t^2ux^{p-1} &\equiv y^{p-1}(tu^2 - xy^2) \pmod{\theta} \\tx^{p-1}(x^{p+1}y + t \cdot tux^{p-1}) &\equiv y^{p-1}(t^2u^2x^{p-1} - xy^2 \cdot tx^{p-1}) \pmod{\theta}\end{aligned}$$

(2) より

$$\begin{aligned}tx^{p-1}(x^{p+1}y + tyz^p) &\equiv y^{p-1}(tu \cdot yz^p - tx^p y^2) \pmod{\theta} \\tx^{p-1}(x^{p+1}y + tyz^p) &\equiv y^p(tuz^p - tx^p y) \pmod{\theta}\end{aligned}$$

$$\begin{aligned}x^{p+1}y + tyz^p &\equiv tuz^p - tx^p y \pmod{\theta} \\x^{p+1}y + tx^p y &\equiv tuz^p - tyz^p \pmod{\theta} \\x^p(xy + ty) &\equiv z^{p-1}(tuz - tyz) \pmod{\theta} \\x^p(sxy + sty) &\equiv sz^{p-1}(tuz - tyz) \pmod{\theta}\end{aligned}$$

$$sy(x + t) \equiv tz(u - y) \pmod{\theta} \tag{5}$$

$$\begin{aligned}sy(x^p + tx^{p-1}) &\equiv tx^{p-1}z(u - y) \pmod{\theta} \\sy(x^p + y^p) &\equiv y^p z(u - y) \pmod{\theta} \\syx^p &\equiv y^p z(u - y) \pmod{\theta} \\sz^{p-1} &\equiv y^{p-1}(u - y) \pmod{\theta}\end{aligned}$$

$$x^p \equiv y^{p-1}(u - y) \pmod{\theta} \tag{6}$$

同様に

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\ s^2tz^{p-1} + st^2x^{p-1} &\equiv st \cdot uy^{p-1} \pmod{\theta} \end{aligned}$$

(4) より

$$\begin{aligned} s^2tz^{p-1} + st^2x^{p-1} &\equiv xzy^p \pmod{\theta} \\ s^2tz^{p-1} + st^2x^{p-1} &\equiv xz(z^p - x^p) \pmod{\theta} \\ s^2tz^{p-1} + st^2x^{p-1} &\equiv xz^{p+1} - x^{p+1}z \pmod{\theta} \\ x^{p+1}z + st^2x^{p-1} &\equiv xz^{p+1} - s^2tz^{p-1} \pmod{\theta} \\ x^{p-1}(x^2z + st^2) &\equiv xz^{p+1} - s^2tz^{p-1} \pmod{\theta} \\ x^{p-1}(sx^2z^p + s^2t^2z^{p-1}) &\equiv sz^{p-1}(xz^{p+1} - s \cdot stz^{p-1}) \pmod{\theta} \end{aligned}$$

(1) より

$$\begin{aligned} x^{p-1}(sx^2z^p + st \cdot xy^p) &\equiv sz^{p-1}(xz^{p+1} - sxy^p) \pmod{\theta} \\ x^p(sxz^p + sty^p) &\equiv sz^{p-1}(xz^{p+1} - sxy^p) \pmod{\theta} \end{aligned}$$

$$\begin{aligned} sxz^p + sty^p &\equiv xz^{p+1} - sxy^p \pmod{\theta} \\ sty^p + sxy^p &\equiv xz^{p+1} - sxz^p \pmod{\theta} \\ y^{p-1}(sty + sxy) &\equiv z^p(xz - sx) \pmod{\theta} \\ uy^{p-1}(sty + sxy) &\equiv z^p(uxz - sux) \pmod{\theta} \end{aligned}$$

$$sy(t+x) \equiv ux(z-s) \pmod{\theta} \quad (7)$$

$$\begin{aligned} sz^{p-1}y(t+x) &\equiv ux(z^p - sz^{p-1}) \pmod{\theta} \\ x^py(t+x) &\equiv ux(z^p - x^p) \pmod{\theta} \\ x^{p-1}y(t+x) &\equiv uy^p \pmod{\theta} \\ x^{p-1}(t+x) &\equiv uy^{p-1} \pmod{\theta} \end{aligned}$$

$$x^{p-1}(t+x) \equiv z^p \pmod{\theta} \quad (8)$$

同様に

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + su \cdot tx^{p-1} &\equiv su^2y^{p-1} \pmod{\theta} \end{aligned}$$

(4) より

$$\begin{aligned} s^2uz^{p-1} + yzx^p &\equiv su^2y^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + yz(z^p - y^p) &\equiv su^2y^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + yz^{p+1} - y^{p+1}z &\equiv su^2y^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + yz^{p+1} &\equiv su^2y^{p-1} + y^{p+1}z \pmod{\theta} \\ z^{p-1}(s^2u + yz^2) &\equiv su^2y^{p-1} + y^{p+1}z \pmod{\theta} \\ z^{p-1}(s^2u^2y^{p-1} + uy^pz^2) &\equiv uy^{p-1}(u \cdot suy^{p-1} + y^{p+1}z) \pmod{\theta} \end{aligned}$$

(3) より

$$\begin{aligned} z^{p-1}(sux^pz + uy^pz^2) &\equiv uy^{p-1}(ux^pz + y^{p+1}z) \pmod{\theta} \\ z^p(sux^p + uy^pz) &\equiv uy^{p-1}(ux^pz + y^{p+1}z) \pmod{\theta} \end{aligned}$$

$$\begin{aligned} sux^p + uy^pz &\equiv ux^pz + y^{p+1}z \pmod{\theta} \\ sux^p - ux^pz &\equiv y^{p+1}z - uy^pz \pmod{\theta} \\ x^{p-1}(sux - uxz) &\equiv y^p(yz - uz) \pmod{\theta} \\ tx^{p-1}(sux - uxz) &\equiv y^p(tyz - tuz) \pmod{\theta} \\ ux(s - z) &\equiv tz(y - u) \pmod{\theta} \end{aligned} \tag{9}$$

$$\begin{aligned} uy^{p-1}x(s - z) &\equiv tz(y^p - uy^{p-1}) \pmod{\theta} \\ z^px(s - z) &\equiv tz(y^p - z^p) \pmod{\theta} \\ z^{p-1}x(s - z) &\equiv -tx^p \pmod{\theta} \\ z^{p-1}(s - z) &\equiv -tx^{p-1} \pmod{\theta} \end{aligned}$$

$$z^{p-1}(z - s) \equiv y^p \pmod{\theta} \tag{10}$$

項  $x^p, y^p, z^p$  について位相変換する  $k_1, k_2, k_3$  を仮定する。つまり

$$\begin{aligned} y^p - z^p &\equiv -x^p \pmod{\theta} \\ k_1 y^p - k_2 z^p &\equiv -k_3 x^p \pmod{\theta} \\ x^p + y^p &\equiv z^p \pmod{\theta} \end{aligned}$$

(6)(8)(10) より

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\ (u-y)y^{p-1} + (z-s)z^{p-1} &\equiv (t+x)x^{p-1} \pmod{\theta} \end{aligned}$$

$$\begin{aligned} u - y &\equiv k_1 y \pmod{\theta} \\ u &\equiv (k_1 + 1)y \pmod{\theta} \\ z - s &\equiv -k_2 z \pmod{\theta} \\ s &\equiv (k_2 + 1)z \pmod{\theta} \\ t + x &\equiv -k_3 x \pmod{\theta} \\ t &\equiv -(k_3 + 1)x \pmod{\theta} \end{aligned}$$

以下、3 式の各項は合同である。

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{\theta} \\ (k_2 + 1)z^p - (k_3 + 1)x^p &\equiv (k_1 + 1)y^p \pmod{\theta} \\ k_1 y^p - k_2 z^p &\equiv -k_3 x^p \pmod{\theta} \end{aligned}$$

$$\begin{aligned} x^p &\equiv k_1 y^p \pmod{\theta} \\ -k_3 x^p &\equiv -k_3 k_1 y^p \pmod{\theta} \\ (k_1 + 1)y^p &\equiv -k_3 k_1 y^p \pmod{\theta} \\ (k_1 + 1 + k_1 k_3)y^p &\equiv 0 \pmod{\theta} \\ (k_1(k_3 + 1) + 1)y^p &\equiv 0 \pmod{\theta} \end{aligned}$$

$$\begin{aligned} y^p &\equiv -k_2 z^p \pmod{\theta} \\ k_1 y^p &\equiv -k_1 k_2 z^p \pmod{\theta} \\ (k_2 + 1)z^p &\equiv -k_1 k_2 z^p \pmod{\theta} \\ (k_2 + 1 + k_1 k_2)z^p &\equiv 0 \pmod{\theta} \\ (k_2(k_1 + 1) + 1)z^p &\equiv 0 \pmod{\theta} \end{aligned}$$

$$\begin{aligned} z^p &\equiv -k_3 x^p \pmod{\theta} \\ -k_2 z^p &\equiv k_2 k_3 x^p \pmod{\theta} \\ -(k_3 + 1)x^p &\equiv k_2 k_3 x^p \pmod{\theta} \\ (k_3 + 1 + k_2 k_3)x^p &\equiv 0 \pmod{\theta} \\ (k_3(k_2 + 1) + 1)x^p &\equiv 0 \pmod{\theta} \end{aligned}$$