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。

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

これは以下と同値である。

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

Definition 2

$$\theta \perp 6xyz$$

Proposition 3 $x^p + y^p \not\equiv z^p \mod \theta$

$\theta \perp xyz$ 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。

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

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

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

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

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

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta$$
$$tu \cdot sz^{p-1} + t^2 ux^{p-1} \equiv tu^2 y^{p-1} \mod \theta$$

(4) より

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

(2) より

$$tx^{p-1}(x^{p+1}y + tyz^p) \equiv y^{p-1}(tu \cdot yz^p - tx^p y^2) \mod \theta$$
$$tx^{p-1}(x^{p+1}y + tyz^p) \equiv y^p(tuz^p - tx^p y) \mod \theta$$

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

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

$$sy(x^p + tx^{p-1}) \equiv tx^{p-1}z(u - y) \mod \theta$$
$$sy(x^p + y^p) \equiv y^p z(u - y) \mod \theta$$
$$syz^p \equiv y^p z(u - y) \mod \theta$$
$$sz^{p-1} \equiv y^{p-1}(u - y) \mod \theta$$

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

同様に

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta$$
$$s^2tz^{p-1} + st^2x^{p-1} \equiv st \cdot uy^{p-1} \mod \theta$$

(4) より

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

(1) より

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

$$sxz^p + sty^p \equiv xz^{p+1} - sxy^p \mod \theta$$
$$sty^p + sxy^p \equiv xz^{p+1} - sxz^p \mod \theta$$
$$y^{p-1}(sty + sxy) \equiv z^p(xz - sx) \mod \theta$$
$$uy^{p-1}(sty + sxy) \equiv z^p(uxz - sux) \mod \theta$$

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

$$sz^{p-1}y(t + x) \equiv ux(z^p - sz^{p-1}) \mod \theta$$
$$x^py(t + x) \equiv ux(z^p - x^p) \mod \theta$$
$$x^{p-1}y(t + x) \equiv uy^p \mod \theta$$
$$x^{p-1}(t + x) \equiv uy^{p-1} \mod \theta$$

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

同様に

$$sz^{p-1} + tx^{p-1} \equiv uy^{p-1} \mod \theta$$
$$s^2uz^{p-1} + su \cdot tx^{p-1} \equiv su^2y^{p-1} \mod \theta$$

(4) より

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

(3) より

$$z^{p-1}(sux^pz + uy^pz^2) \equiv uy^{p-1}(ux^pz + y^{p+1}z) \mod \theta$$
$$z^p(sux^p + uy^pz) \equiv uy^{p-1}(ux^pz + y^{p+1}z) \mod \theta$$

$$sux^p + uy^pz \equiv ux^pz + y^{p+1}z \mod \theta$$
$$sux^p - ux^pz \equiv y^{p+1}z - uy^pz \mod \theta$$
$$x^{p-1}(sux - uxz) \equiv y^p(yz - uz) \mod \theta$$
$$tx^{p-1}(sux - uxz) \equiv y^p(tyz - tuz) \mod \theta$$

$$ux(s - z) \equiv tz(y - u) \mod \theta \tag{9}$$

$$uy^{p-1}x(s - z) \equiv tz(y^p - uy^{p-1}) \mod \theta$$
$$z^px(s - z) \equiv tz(y^p - z^p) \mod \theta$$
$$z^{p-1}x(s - z) \equiv -tx^p \mod \theta$$
$$z^{p-1}(s - z) \equiv -tx^{p-1} \mod \theta$$

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

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

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

(6)(8)(10) より

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

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

$$\begin{aligned} k_1 sz^{p-1} + k_2 tx^{p-1} &\equiv k_3 uy^{p-1} \mod \theta \\ (k_3 u - y)y^{p-1} + (z - k_1 s)z^{p-1} &\equiv (k_2 t + x)x^{p-1} \mod \theta \end{aligned}$$

$$\begin{aligned} k_1 sz^{p-1} &\equiv y^p \mod \theta \\ \Rightarrow k_3 u &\equiv 2y \mod \theta \\ k_2 tx^{p-1} &\equiv -z^p \mod \theta \\ \Rightarrow k_1 s &\equiv 2z \mod \theta \\ k_3 uy^{p-1} &\equiv -x^p \mod \theta \\ \Rightarrow k_2 t &\equiv -2x \mod \theta \end{aligned}$$

$$\begin{aligned} 2z^p &\equiv y^p \mod \theta \\ -2x^p &\equiv -z^p \mod \theta \\ 2y^p &\equiv -x^p \mod \theta \end{aligned}$$

$$\begin{aligned} 2z^p - y^p &\equiv 0 \mod \theta \\ 2x^p - z^p &\equiv 0 \mod \theta \\ 2y^p + x^p &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} z^p + x^p &\equiv 0 \mod \theta \\ x^p - y^p &\equiv 0 \mod \theta \\ z^p + y^p &\equiv 0 \mod \theta \end{aligned} \tag{11}$$

(5)(7)(9) について
θ を法として $x+t\equiv 0 \quad , s-z\equiv 0 \quad , \ y-u\equiv 0$ のとき

$$\begin{aligned} t &\equiv -x \mod \theta \\ u &\equiv y \mod \theta \\ s &\equiv z \mod \theta \end{aligned} \tag{12}$$

(2)(12) より

$$\begin{aligned} -yx^p &\equiv yz^p \mod \theta \\ -x^p &\equiv z^p \mod \theta \\ z^p + x^p &\equiv 0 \mod \theta \end{aligned}$$

(1)(12) より

$$\begin{aligned} -xz^p &\equiv xy^p \mod \theta \\ -z^p &\equiv y^p \mod \theta \\ z^p + y^p &\equiv 0 \mod \theta \end{aligned}$$

(3)(12) より

$$\begin{aligned} zy^p &\equiv x^p z \mod \theta \\ y^p &\equiv x^p \mod \theta \\ x^p - y^p &\equiv 0 \mod \theta \end{aligned}$$

よって

$$\begin{aligned} (x^p + y^p - z^p) + (x^p - y^p) + (z^p + x^p) &\equiv 0 \mod \theta \\ (x^p + y^p - z^p) + (2x^p - y^p + z^p) &\equiv 0 \mod \theta \\ 3x^p &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} (x^p + y^p - z^p) + (y^p - x^p) + (z^p + y^p) &\equiv 0 \mod \theta \\ (x^p + y^p - z^p) + (-x^p + 2y^p + z^p) &\equiv 0 \mod \theta \\ 3y^p &\equiv 0 \mod \theta \end{aligned}$$

$$\begin{aligned} -(x^p + y^p - z^p) + (z^p + x^p) + (z^p + y^p) &\equiv 0 \mod \theta \\ -(x^p + y^p - z^p) + (x^p + y^p + 2z^p) &\equiv 0 \mod \theta \\ 3z^p &\equiv 0 \mod \theta \end{aligned}$$

また (11) も同様である事から、$\theta \perp 6xyz$ の前提に反する。