The idea of the Arithmetica

Hajime Mashima

October 23, 2015

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　フェルマーの小定理とは

Theorem 2 (多項定理) 3 項の n の冪 $(c+d+e)^n$ を展開したときの一般項は各文字を自然数として以下のように表わせる。また 4 項以上も同じ要領である。

$$\frac{n!}{f!g!h!}c^f d^g e^h \quad (f+g+h=n \ , \ 0 \leq f,g,h \leq n) \tag{1}$$

Lemma 3 (1) について n が素数 p であるときの係数 $\frac{p!}{f!g!h!} = 1$ でない項は、分母が p 未満の階乗の積となるので分子の p は残る。よって p で割り切れる。

$$\frac{p!}{f!g!h!} \equiv 0 \pmod{p} \quad (f+q+h=p \ , \ 0 \leq f,g,h < p) \tag{2}$$

Theorem 4 (フェルマーの小定理) a を自然数、p が素数で a と p が互いに素であるとき

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof 5 通し番号を付けた 1 の和で自然数 a を表わすと

$$\begin{aligned} 1 &= 1_1 \\ 2 &= 1_1 + 1_2 \\ 3 &= 1_1 + 1_2 + 1_3 \\ &\vdots \\ a &= 1_1 + 1_2 + 1_3 + \cdots + 1_a \end{aligned}$$

(2) より、係数が 1 でない数式を p と自然数 $\mathbb{N}$ の積で表わした a^p の展開式は

$$a^p = 1_1^p + 1_2^p + 1_3^p + \cdots + 1_a^p + p\mathbb{N} \tag{3}$$

両辺から a を引くと

$$\begin{aligned} a^p - a &= p\mathbb{N} \\ a^p - a &\equiv 0 \pmod{p} \\ a\left(a^{p-1} - 1\right) &\equiv 0 \pmod{p} \end{aligned}$$

ここで、a と p が互いに素であるならば

$$\begin{aligned} a^{p-1} - 1 &\equiv 0 \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

また、全ての自然数 a において

$$a^p \equiv a \pmod{p} \tag{4}$$

□

1.3 三項定理の考察

Corollary 6 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。

$$X+Y-Z \equiv 0 \pmod{p} \tag{5}$$

Proof 7 (3) より、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

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

□

Proof 8 (別証明) (4) より

$$(X^p-X)+(Y^p-Y)=Z^p-X-Y \equiv 0 \pmod{p} \tag{6}$$
$$(Z^p-Z)-(Y^p-Y)=X^p-Z+Y \equiv 0 \pmod{p} \tag{7}$$
$$(Z^p-Z)-(X^p-X)=Y^p-Z+X \equiv 0 \pmod{p} \tag{8}$$

$(7)+(8)-(6)$

$$2(X+Y-Z) \equiv 0 \pmod{p}$$

$p \geq 3$ について

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

□

この時 $X+Y>Z$ でなければならない。 (9)

Proof 9 (5) より $Z>X+Y$ ならば、$\mathbf{N}$ を自然数として

$Z-(X+Y) = p\mathbf{N}>0$ と仮定できる。

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

(3) より、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。

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

□

Proposition 10 フェルマーの命題が偽ならば、3 の冪について互いに素な x, y, z のいずれかは 3 で割り切れる。また $(x+y), (z-x), (z-y)$ のいずれかは 3^2 を約数に持ち、互いに素である。

Proof 11

$$
\begin{aligned}
(x+y-z)^3 &= x^3+y^3-z^3+3x^2y+3xy^2-3x^2z+3xz^2-3y^2z+3yz^2-6xyz \\
&\quad x^3+y^3-z^3=0 \text{ より} \\
&= 3\left(x^2y+xy^2-x^2z+xz^2-y^2z+yz^2-2xyz\right) \\
&= 3\left(xy\left(x+y\right)+xz^2+yz^2-x^2z-y^2z-2xyz\right) \\
&= 3\left(xy\left(x+y\right)+z^2\left(x+y\right)-z\left(x+y\right)^2\right) \\
&= 3(x+y)\left(xy+z^2-z\left(x+y\right)\right) \\
&= 3(x+y)(z-x)(z-y)
\end{aligned}
$$

$$
\begin{aligned}
x+y-z &\equiv 0 \pmod 3 \text{ であるから} \\
x+y &\equiv z \pmod 3 \\
z-x &\equiv y \pmod 3 \\
z-y &\equiv x \pmod 3
\end{aligned}
$$

x, y, z は互いに素であるから $(x+y), (z-x), (z-y)$ のいずれかは 3^2 を約数に持つ。

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

仮に公約数 $r(\neq 3)$ を持つとすると適当な自然数 l, m とおき

$$
\begin{aligned}
z-x &= rl && (10) \\
z-y &= rm && (11) \\
(10)+(11) & \\
2z-x-y &= r(l+m) \\
z-(x+y) &= r(l+m)-z \\
(x+y-z)^3 &= (z-r(l+m))^3 \\
(x+y-z)^3 &\equiv 0 \pmod{r^2} \\
(z-r(l+m))^3 &\equiv 0 \pmod{r^2} \\
z &\equiv 0 \pmod r
\end{aligned}
$$

(10), (11) より x, y, z が公約数 r を持つので、互いに素である前提に反する。これは $x+y$ の組についても同様である。 □

1.4　フェルマーの着想

ここまでの流れは、フェルマーの命題の証明に直接関わらないと考えられるが、小定理の証明に関してフェルマーが多項定理あるいはそれに近いものを取り扱っていたという可能性を示唆したものである。

$$\frac{n!}{f!g!h!}c^f d^g e^h \quad (f+g+h=n\ ,\ 0\leq f,g,h\leq n)$$

当時、フェルマーはディオファントスの「算術」第 2 巻：第 8 問の平方数を 2 つの平方数の和に表す問題について読んでいた。つまりピタゴラス方程式である。

$$x^2+y^2=z^2$$

そして冪が 3 や 4 の場合について等式が成り立つ x,y,z の組はあるのか代入してみた。この時はまだ 1 つや 2 つの解はあるだろうと思っていたが、解は直ぐに見つけられなかったので関心を持ち調べる事にしたと考えられる。

$$x^n+y^n=z^n$$

ところで後世の数学者がこの命題に執着してきたのは、フェルマーが「証明した。」と示したにも関わらず 100 年また 100 年と時を経ても証明が見つからない等それ相応の理由がある。しかし、出題者のフェルマーにそれは該当しない。そもそも解があるのかどうかも分からないので、長らく解が得られないのであれば普通は放棄するものである。よって大半を占める奇素数の証明に関しては割と短い期間で証明を得ていたと考えられる。また各冪について異なる証明であっては無限個まで続く冪の帰納法は得られないため、一貫性のある証明法と推測できる。

フェルマーが唯一、4 の冪について証明を与えた事は無視できないものがある。この証明にはフェルマーが考案した無限降下法が用いられているが、これが一般解の証明のヒントであるのか、または奇素数でないため個別に証明を必要としたのか等、想像を掻き立てられる。

$$\left(x^2\right)^2+\left(y^2\right)^2=Z^2$$

先に書いたようにフェルマーが多項定理を扱っていたと推測するが、特にフェルマーの命題に関しては互いに素な $x,y,-z$ の 3 項を用いる。

$$(x+y-z)^n$$

簡単のため上式 n が 3 の条件を例にすると、$x^3+y^3=z^3$ が成り立つときの展開式は係数 1 となる項 $x^3,y^3,-z^3$ が消えるので以下の式となる。

$$\frac{3!}{2!1!0!}x^2y^1+\frac{3!}{1!2!0!}x^1y^2-\frac{3!}{2!0!1!}x^2z^1+\frac{3!}{1!0!2!}x^1z^2-\frac{3!}{0!2!1!}y^2z^1+\frac{3!}{0!1!2!}y^1z^2+\frac{3!}{1!1!1!}x^1y^1z^1$$

この式を眺めていると気が付く事がある。おそらくフェルマーは 3 以上の冪を調べるための着想として「このような 1 の係数項を欠いた展開式が $\mathbb{N}^n$ であるならば $x+y-z$ を組み替えて 1 の係数項を持つ別の展開式で再構築できる。それが可能であろうか?」というアプローチを行っていたと考えられる。あえて命題らしく表現するならば「$x^n+y^n=z^n$ であるような $\mathbb{N}^n$ は成り立つか?」と言う事である。

1.5 互いに素による証明

Proposition 12 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 $(x < y < z)$。

$$\begin{aligned} y &= x + s & z &= x + s + t \\ y^p &= (x+s)^p & z^p &= (x+s+t)^p \end{aligned} \tag{12}$$

1.5.1 $t > 1$ のとき

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

$0 = -x^p + z^p - y^p$ より

$$\begin{aligned} 0 &= -x^p + \frac{p!}{(p-1)!1!}(x+s)^{p-1}t + \frac{p!}{(p-2)!2!}(x+s)^{p-2}t^2 \cdots + \frac{p!}{1!\,(p-1)!}(x+s)\,t^{p-1} + t^p \\ 0 &= -x^p + \frac{p!}{(p-1)!1!}x^{p-1}t + \frac{p!}{(p-1)!1!}s^{p-1}t + \frac{p!}{(p-1)!1!}((x+s)^{p-1} - x^{p-1} - s^{p-1})t \\ &\quad + \frac{p!}{(p-2)!2!}x^{p-2}t^2 + \frac{p!}{(p-2)!2!}s^{p-2}t^2 + \frac{p!}{(p-2)!2!}((x+s)^{p-2} - x^{p-2} - s^{p-2})t^2 \\ &\quad \cdots + \frac{p!}{1!\,(p-1)!}xt^{p-1} + \frac{p!}{1!\,(p-1)!}st^{p-1} + t^p \end{aligned} \tag{13}$$

$x + y - z = x - t$ (9) より $(x > t)$, p が奇素数について

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

上式と (13) の和は

$$\begin{aligned} (x-t)^p &= \frac{p!}{(p-2)!2!}2x^{p-2}t^2 + \frac{p!}{(p-4)!4!}2x^{p-4}t^4 + \frac{p!}{(p-6)!6!}2x^{p-6}t^6 + \cdots + \frac{p!}{1!\,(p-1)!}2xt^{p-1} \\ &\quad + \frac{p!}{(p-1)!1!}s^{p-1}t + \frac{p!}{(p-2)!2!}s^{p-2}t^2 + \frac{p!}{(p-3)!3!}s^{p-3}t^3 \cdots + \frac{p!}{1!\,(p-1)!}st^{p-1} \\ &\quad + \frac{p!}{(p-1)!1!}((x+s)^{p-1} - x^{p-1} - s^{p-1})t + \frac{p!}{(p-2)!2!}((x+s)^{p-2} - x^{p-2} - s^{p-2})t^2 \\ &\quad + \frac{p!}{(p-3)!3!}((x+s)^{p-3} - x^{p-3} - s^{p-3})t^3 \cdots + \frac{p!}{1!\,(p-1)!}((x+s) - x - s)t^{p-1} \end{aligned}$$

$$\begin{aligned} (x-t)^p &= pt^2\left(\frac{(p-1)!}{(p-2)!2!}2x^{p-2} + \frac{(p-1)!}{(p-4)!4!}2x^{p-4}t^2 + \frac{(p-1)!}{(p-6)!6!}2x^{p-6}t^4 + \cdots + \frac{(p-1)!}{1!\,(p-1)!}2xt^{p-3}\right) \\ &\quad + pts^{p-1} + pt^2\left(\frac{(p-1)!}{(p-2)!2!}s^{p-2} + \frac{(p-1)!}{(p-3)!3!}s^{p-3}t \cdots + \frac{(p-1)!}{1!\,(p-1)!}st^{p-3}\right) \\ &\quad + pt\left((x+s)^{p-1} - x^{p-1} - s^{p-1}\right) + pt^2(\cdots 略 \cdots) \end{aligned}$$

$$(x-t)^p \equiv 0 \pmod{t} \qquad \text{なので } x = kt \text{ とおける。} \tag{14}$$
$$\text{よって} \quad (x+s)^{p-1} - x^{p-1} - s^{p-1} \equiv 0 \pmod{t} \tag{15}$$

2 の冪について

$$0 = -x^2 + ((x+s)+t)^2 - (x+s)^2 = -x^2 + 2t(x+s) + t^2$$
$$(x-t)^2 = x^2 - 2tx + t^2 = 2st + 2t^2 = 2t(s+t) \text{ よって} \quad x = kt \text{ とおける。}$$
$$t^2(k-1)^2 = 2t(s+t) \quad (k \neq 1) \quad \text{仮に } t = 2 \text{ ならば}$$
$$y = 2k + s \qquad\qquad z = 2k + s + 2$$

特に矛盾点は見つからない。

奇素数の冪について

$$\begin{aligned}
(kt-t)^p &= t^p(k-1)^p \quad (k \neq 1) \qquad \text{仮に } t = p \text{ ならば} \\
\text{左辺} &= p^p(k-1)^p \qquad\qquad (15) \text{ より} \\
\text{右辺} &= pts^{p-1} + p^3(\cdots\text{略}\cdots)
\end{aligned}$$

仮に $t = p$ であっても右辺の項 pts^{p-1} の s は少なくとも t を約数にもつ。
(12), (14) より x, y, z は公約数 t を持つので互いに素である前提に反する。

よって互いに素な組の $t > 1$ については解が存在しない。

4 の冪について

$$\begin{aligned}
(x+s)^4 &= s^4 + 4s^3x + 6s^2x^2 + 4sx^3 + x^4 \\
(x+s+t)^4 &= s^4 + 4s^3x + 6s^2x^2 + 4sx^3 + x^4 + 4s^3t + 6s^2t^2 + 12s^2tx + 4st^3 \\
&\quad +12st^2x + 12stx^2 + t^4 + 4t^3x + 6t^2x^2 + 4tx^3 \\
0 &= -x^4 + z^4 - y^4 \text{だから} \\
0 &= -x^4 + 4s^3t + 6s^2t^2 + 12s^2tx + 4st^3 \\
&\quad +12st^2x + 12stx^2 + t^4 + 4t^3x + 6t^2x^2 + 4tx^3 \qquad (16)
\end{aligned}$$

$$\begin{aligned}
x + y - z &= x - t \text{ より} \\
(x-t)^4 &= t^4 - 4t^3x + 6t^2x^2 - 4tx^3 + x^4 \\
&\quad \text{上式と } (16) \text{ の和は} \\
(x-t)^4 &= 4s^3t + 6s^2t^2 + 12s^2tx + 4st^3 + 12st^2x + 12stx^2 + 2t^4 + 12t^2x^2 \\
&= 2t\left(2s^3 + 3s^2t + 6s^2x + 2st^2 + 6stx + 6sx^2 + t^3 + 6tx^2\right)
\end{aligned}$$

$$\begin{aligned}
(x-t)^4 &\equiv 0 \pmod{t} \qquad \text{なので } x = kt \text{ とおけるので} \\
t^4(k-1)^4 &= 2t\left(2s^3 + 3s^2t + 6s^2kt + 2st^2 + 6skt^2 + 6s(kt)^2 + t^3 + 6t(kt)^2\right)
\end{aligned}$$

$t = 2$ のとき x は偶数、s は奇数となるので $\quad 2s^3 + 3s^2t \equiv 0 \pmod{2^2}$

よって互いに素な組の $t > 2$ については解が存在しない。 (17)

1.6 偶奇性による証明

ここからフェルマーが行ったと考えられる証明を示す。

Theorem 13 p が奇素数であるとき以下の等式が成り立つ。[*1, p.45*]

$$x^p + y^p = (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1}) \quad (18)$$
$$z^p - y^p = (z-y)(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + \cdots + zy^{p-2} + y^{p-1}) \quad (19)$$
$$z^p - x^p = (z-x)(z^{p-1} + z^{p-2}x + z^{p-3}x^2 + \cdots + zx^{p-2} + x^{p-1}) \quad (20)$$

$x-t$ は偶数なので $t=1$ のとき、下表に示した x が奇数の組み合わせとなる。
y が奇数、z が偶数のとき (18)、y が偶数、z が奇数のとき (20) の式を参照する。

x	y	z	参照
奇数	奇数	偶数	(18)
偶数	奇数	奇数	(19)
奇数	偶数	奇数	(20)

奇素数の冪について

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

$y^p = z^p - x^p$ が成り立つとして、(20) を代入すると

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

$$(y-(z-x))^p \equiv 0 \pmod{z-x}$$ なので $y = k'(z-x)$ とおける。よって
$$(k'(z-x)-(z-x))^p \equiv 0 \pmod{z-x}$$
$$(z-x)^p\,(k'-1)^p \equiv 0 \pmod{z-x} \qquad (k' \neq 1)$$

$$(z-x)^{p-1}(k'-1)^p = z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \cdots + zx^{p-2} + x^{p-1} \\ - \frac{p!}{(p-1)!1!}y^{p-1} + \frac{p!}{(p-2)!2!}y^{p-2}(z-x) - \frac{p!}{(p-3)!3!}y^{p-3}(z-x)^2 \\ \cdots + \frac{p!}{1!(p-1)!}y(z-x)^{p-2} - (z-x)^{p-1}$$

$z-x$ は偶数なので

$$\text{左辺} = (z-x)^{p-1}(k'-1)^p = \text{偶数} \quad (21)$$

右辺 zx 項は奇数で $p-2$ (奇数) 個ある。また $z^{p-1}+x^{p-1}$ が偶数なので

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

後に続く数式の $y,(z-x)$ は偶数なので

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

よって右辺は奇数となり、これは左辺が偶数となる (21) に反する。別の条件でも偶奇性は変わらないため、フェルマーの命題について奇素数の冪は成り立たない。

4 の冪について

$$(y-(z-x))^4=y^4-4(z-x)y^3+6(z-x)^2y^2-4(z-x)^3y+(z-x)^4$$

$$\begin{aligned}z^4-y^4 &= (z-y)(y^3+y^2z+yz^2+z^3) \\ z^4-x^4 &= (z-x)(x^3+x^2z+xz^2+z^3)\end{aligned}$$

奇素数の場合と同じ操作をすると「偶数 = 偶数」となる。
(17) および偶奇性による 4 の冪について不明なためフェルマーの証明を適用する。

References

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