# フェルマーの最終定理の初等的証明

壊れた扉（完成者)
愛犬ベルのために (基案者)

最新 2021 年 11 月 13 日第 4 版

## 更新履歴

初版 2021 年 10 月 28 日
第 2 版 2021 年 10 月 28 日「a：奇数，b：奇数，c：偶数 の場合」の「左辺が奇数になった場合」の 2 の指数修正
第 3 版 2021 年 11 月 12 日「a：奇数，b：奇数，c：偶数 の場合」の「左辺が奇数になった場合」の 2 の指数修正
第 4 版 2021 年 11 月 13 日「a：奇数，b：奇数，c：偶数 の場合」の「左辺が奇数になった場合」の 2 の指数修正

## はじめに

[*1]フェルマーの最終定理は $n = 3, 4$ の場合などが初等的に証明されていて、例えば、$n = 15$ の場合などは、$(a^5)^3 + (b^5)^3 = (c^5)^3$ などとすれば成り立たない事は自明なので、あとは $n$ が奇素数の場合のみ考えれば良い。

そこで、$a^n + b^n = c^n \quad (n$ は奇素数) となる自然数 $a, b, c$ が存在すると仮定すると、

i. a：偶数，b：偶数，c：偶数
ii. a：偶数，b：奇数，c：奇数
iii. a：奇数，b：奇数，c：偶数

の 3 通りの場合があり、i. の場合は両辺を 2 で割り続ければ ii. か iii. の場合に帰着する. よって、ii.、iii. の場合を示せば良い。

[*1] フェルマーの最終定理を初等的証明で解いて見ました。基本案は愛犬ベルのためにですが、大幅に改定して下さったのが壊れた扉さんです。

# 1　a：偶数，b：奇数，c：奇数の場合

$a = 2^u p, b = 2q+1, c = 2r+1$　　$(p, q, r, u$ は自然数で $p$ は奇数とする$)$ と置いて $a^n + b^n = c^n$ に代入すると、

$$(2^u p)^n + (2q+1)^n = (2r+1)^n$$

$$(2^u p)^n = (2r+1)^n - (2q+1)^n$$

これを二項定理で展開すると、

$$2^{un}p^n = (2r)^n +_n C_1(2r)^{n-1} +_n C_2(2r)^{n-2} + \cdots +_n C_{n-2}(2r)^2 +_n C_1(2r) + 1$$
$$-\{(2q)^n +_n C_1(2q)^{n-1} +_n C_2(2q)^{n-2} + \cdots +_n C_{n-2}(2q)^2 +_n C_1(2q) + 1\}$$

$$= 2^n(r^n - q^n) +_n C_1 2^{n-1}\{r^{n-1} - q^{n-1}\} +_n C_2 2^{n-2}\{r^{n-2} - q^{n-2}\} + \cdots$$
$$+_n C_{n-2}2^2(r^2 - q^2) +_n C_{n-1}2(r-q)$$

公式

$$a^n - b^n = (a-b)\{a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\} \text{ 式 } 1$$

を考えれば、この右辺は $2(r-q)$ で割り切れるので、左辺も $2(r-q)$ で割り切れ、左辺は偶数である。

ところが、$n$ は奇素数 ${}_nC_{n-1} = n$ より右辺は 偶数 + 奇数 となり奇数である。よって、矛盾が生じる。

### 1.0.1　左辺が奇数になった場合

この右辺は $2(r-q)$ で割り切れるので、左辺も $2(r-q)$ で割り切れ、左辺は奇数になったとする。

$$2^{un}p^n = 2^n(r^n - q^n) +_n C_1 2^{n-1}\{r^{n-1} - q^{n-1}\} +_n C_2 2^{n-2}\{r^{n-2} - q^{n-2}\} + \cdots$$
$$+_n C_{n-2}2^2(r^2 - q^2) +_n C_{n-1}2(r-q)$$

つまり、$2(r-q) = 2^{un}$ である。

$$2(r-q) = 2^{un}$$

$$2r + 1 - (2q+1) = 2^{un}$$

$$2r + 1 - (2q+1) = 2^{un}$$

$$c - b = 2^{un}$$

$$c = b + 2^{un}$$

ところで、

$$a^n = c^n - b^n$$

$$c^n - b^n = (b + 2^{un})^n - b^n$$

ここで、

$$g(x) = (x + 2^{un})^n - x^n$$

とすると、n は奇数だから、グラフにすると、$(x + 2^{un})^n$ と $x^n$ は単調増加で、平行である。したがって、$(x+2^{un})^n$ と $x^n$ は交点をもたない。また、$(x+2^{un})^n > x^n$ より、$g(x) > 0$。つまり、いかなる $x$ においても $g(x) \neq 0$ なので、$g(y) = (x-y)g'(y) = 0$ とできない。つまり、$g(x)$ は因数分解できない。$c^n - b^n = a^n$ は、左辺は因数分解できないので、右辺の様にできない。
よって、矛盾。
式 1 から、$c^n - b^n = a^n$ は、因数分解できるように、思われるかもしれないが、この式は、$a = b$ である時、$a^n - b^n = a^n - a^n = b^n - b^n = 0$ の場合であって、$a$ は $b$ お互い独立なので、

$$a^n - b^n = (a-b)\{a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\}$$

右辺を展開すると、左辺となるが、$c = b + 2^{un}$ のときは、$c$ と $b$ はお互い従属関係にあるので、

$$c^n - b^n = (c-b)\{c^{n-1} + c^{n-2}b + \cdots + cb^{n-2} + b^{n-1}\}$$

$$(b + 2^{un})^n - b^n = ((b + 2^{un}) - b)\{(b + 2^{un})^{n-1} + (b + 2^{un})^{n-2}b + \cdots + (b + 2^{un})b^{n-2} + b^{n-1}\}$$

$$(b + 2^{un})^n - b^n = 2^{un}(b + 2^{un})^{n-1} + 2^{un}(b + 2^{un})^{n-2}b + \cdots + 2^{un}(b + 2^{un})b^{n-2} + 2^{un}b^{n-1}$$

展開しても、右辺と左辺は一致しない。つまり、式 1 は因数分解に使えない。
したがって、この右辺は $2(r-q)$ で割り切れるので、左辺も $2(r-q)$ で割り切れ、左辺は奇数になることはない。

## 2　a：奇数，b：奇数，c：偶数の場合

$a = 2p + 1, b = 2q - 1, c = 2^v r$　　$(p, q, r, v$ は自然数で、$r$ は奇数とする$)$ として、$a^n + b^n = c^n$ に代入すると、

$$(2p+1)^n + (2q-1)^n = (2^v r)^n$$

これを二項定理で展開すると、

$$2^{vn}r^n = (2p)^n +_n C_1(2p)^{n-1} +_n C_2(2p)^{n-2} + \cdots +_n C_{n-2}(2p)^2 +_n C_1(2p) + 1$$

$$+\{(2q)^n +_n C_1(2q)^{n-1}(-1) +_n C_2(2q)^{n-2}(-1)^2 + \cdots +_n C_2(2q)^2(-1)^{n-2} +_n C_1(2q)(-1)^{n-1} + (-1)^n\}$$

$n$ は奇数より $1^n$ と $(-1)^n$ は相殺されて 0 になるので、

$$= 2^n(p^n + q^n) +_n C_1 2^{n-1}\{p^{n-1} - q^{n-1}\} +_n C_2 2^{n-2}\{p^{n-2} + q^{n-2}\} + \cdots +$$

$$_nC_{n-2}2^2(p^2 - q^2) +_n C_{n-1}2(p+q)$$

∴

$$2^{vn}r^n = 2^n(p^n + q^n) +_n C_1 2^{n-1}\{p^{n-1} - q^{n-1}\} +_n C_2 2^{n-2}\{p^{n-2} + q^{n-2}\} + \cdots +$$
$$_nC_{n-2}2^2(p^2 - q^2) +_n C_{n-1}2(p+q) ———☆$$

ところで、$n$ が奇数の時、公式

$$a^n + b^n = (a+b)\{a^{n-1} - a^{n-2}b + \cdots + b^{n-1}\} \text{ 式 } 2$$

また、$n$ が偶数の時、公式

$$a^n - b^n = (a+b)\{a^{n-1} - a^{n-2}b + \cdots - b^{n-1}\}$$

を利用すると、$n$ は奇素数より☆の右辺は $2(p+q)$ で割り切れるので、☆の左辺も $p+q$ で割り切れ、左辺は偶数となる。

ところが、$n$ が奇素数 $_nC_{n-1} = n$ より☆の右辺は 偶数＋奇数 となり奇数となる。 よって、矛盾が生じる。

### 2.0.1 左辺が奇数になった場合

$n$ は奇素数より☆の右辺は $2(p+q)$ で割り切れるので、☆の左辺も $p+q$ で割り切れ、左辺は奇数になった場合を考える。
この右辺は $2(p+q)$ で割り切れるので、左辺も $2(p+q)$ で割り切れ、左辺は奇数になったとする。

$$2^{vn}r^n = 2^n(p^n + q^n) +_n C_1 2^{n-1}\{p^{n-1} - q^{n-1}\} +_n C_2 2^{n-2}\{p^{n-2} + q^{n-2}\} + \cdots +$$
$$_nC_{n-2}2^2(p^2 - q^2) +_n C_{n-1}2(p+q)$$

つまり、$2(p+q) = 2^{vn}$ である。

$$2(p+q) = 2^{vn}$$
$$2p + 1 + (2q - 1) = 2^{vn}$$
$$2p + 1 + (2q - 1) = 2^{vn}$$
$$a + b = 2^{vn}$$
$$a = b - 2^{vn}$$

ところで、

$$a^n + b^n = c^n$$
$$a^n + b^n = (b - 2^{vn})^n + b^n$$

ここで、

$$g(x) = (x - 2^{vn})^n + x^n$$

とすると、n は奇数だから、グラフにすると、$(x-2^{vn})^n$ と $x^n$ は単調増加で、平行である。したがって、$(x-2^{vn})^n$ と $x^n$ は交点をもたない。また、$(x-2^{vn})^n < x^n$ より、$g(x) < 0$。つまり、いかなる $x$ においても $g(x) \neq 0$ なので、$g(z) = (x-z)g'(z) = 0$ とできない。つまり、$g(x)$ は因数分解できない。$a^n + b^n = c^n$ は、左辺は因数分解できないので、右辺の様にできない。
よって、矛盾。
式 2 から、$a^n + b^n = c^n$ は、因数分解できるように、思われるかもしれないが、この式は、$a = -b$ である時、$a^n + b^n = a^n - a^n = -b^n + b^n = 0$ の場合であって、$a$ は $b$ お互い独立なので、

$$a^n + b^n = (a+b)\{a^{n-1} - a^{n-2}b + \cdots + b^{n-1}\}$$

右辺を展開すると、左辺となるが、$a = b - 2^{vn}$ のときは、$a$ は $b$ お互い従属関係があるので、

$$(b-2^{vn})^n + b^n = ((b-2^{vn}) + b)\{(b-2^{vn})^{n-1} - (b-2^{vn})^{n-2}b + \cdots + b^{n-1}\}$$

$$(b-2^{vn})^n + b^n = (2b-2^{vn})(b-2^{vn})^{n-1} - (2b-2^{vn})(b-2^{vn})^{n-2}b + \cdots + (2b-2^{vn})b^{n-1}$$

展開しても、右辺と左辺は一致しない。式 2 は因数分解に使えない。
$n$ は奇素数より☆の右辺は $2(p+q)$ で割り切れるので、☆の左辺も $p+q$ で割り切れ、左辺は奇数になることはない。

よって、背理法により、$a^n + b^n = c^n$ は成り立たない。よって、フェルマーの最終定理が初等的に示された。