

# フェルマーの最終定理の証明（制限付きの一般の $n$ の場合）

壊れた扉さん、愛犬ベルのために

最新 2021 年 8 月 6 日

## はじめに

これは、BBS「数の不思議世界」で、壊れた扉さんとの共同作業によってできた共同作品です。なお、これは、壊れた扉さんの 2021-8-6 の投稿を清書したものです。

### 更新履歴

2021.8.6 新規作成

## 1 証明

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。

### 1.1 $a^n = (a + j)^n - (a + k)^n$

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

$$a^n + (a + k)^n = (a + j)^n \quad (\text{ただし、} b = a + k, c = a + j)$$

と置ける。ゆえに、

$$a^n = (a + j)^n - (a + k)^n$$

## 1.2 二項定理で展開

これを二項定理で展開すると、

$$\begin{aligned} a^n &= a^n + {}_n C_1 a^{n-1} j + {}_n C_2 a^{n-2} j^2 + {}_n C_3 a^{n-3} j^3 + \cdots + {}_n C_{n-1} a j^{n-1} + j^n \\ &\quad - (a^n + {}_n C_1 a^{n-1} k + {}_n C_2 a^{n-2} k^2 + {}_n C_3 a^{n-3} k^3 + \cdots + {}_n C_{n-1} a k^{n-1} + k^n) \\ &= {}_n C_1 a^{n-1} (j-k) + {}_n C_2 a^{n-2} (j^2 - k^2) + {}_n C_3 a^{n-3} (j^3 - k^3) + \cdots + {}_n C_{n-1} a (j^{n-1} - k^{n-1}) + j^n - k^n \end{aligned}$$

よって、

$$\begin{aligned} a^n &= (j-k) \{ {}_n C_1 a^{n-1} + {}_n C_2 a^{n-2} (j+k) + {}_n C_3 a^{n-3} (j^2 + jk + k^2) + \cdots \\ &\quad + {}_n C_{n-1} a (j^{n-2} + j^{n-3} k + j^{n-4} k^2 + \cdots + k^{n-2}) + (j^{n-1} + j^{n-2} k + j^{n-3} k^2 + \cdots + k^{n-1}) \} \end{aligned}$$

## 1.3 $j - k = m$ とすると

ここで、 $j - k = m$  とすると、 $j = k + m$

$$\begin{aligned} a^n &= m \{ {}_n C_1 a^{n-1} + {}_n C_2 a^{n-2} (j+k) + {}_n C_3 a^{n-3} (j^2 + jk + k^2) + \cdots \\ &\quad + {}_n C_{n-1} a (j^{n-2} + j^{n-3} k + j^{n-4} k^2 + \cdots + k^{n-2}) \\ &\quad + (j^{n-1} + j^{n-2} k + j^{n-3} k^2 + \cdots + k^{n-1}) \} \end{aligned}$$

## 1.4 $(a - m)^n$

ここで、 $(a - m)^n$  を展開して、

$$\begin{aligned} (a-m)^n &= a^n + {}_n C_1 a^{n-1} (-m) + {}_n C_2 a^{n-2} (-m)^2 + {}_n C_3 a^{n-3} (-m)^3 + \cdots + {}_n C_{n-1} a (-m)^{n-1} + (-m)^n \\ &= a^n - {}_n C_1 m a^{n-1} + {}_n C_2 m^2 a^{n-2} - {}_n C_3 m^3 a^{n-3} + \cdots + {}_n C_{n-1} m^{n-1} a - m^n \end{aligned}$$

の両辺に、

$$- {}_n C_1 m a^{n-1} + {}_n C_2 m^2 a^{n-2} - {}_n C_3 m^3 a^{n-3} + \cdots + {}_n C_{n-1} m^{n-1} a - m^n$$

を加えると、

$$\begin{aligned} (a-m)^n &= m \{ {}_n C_2 a^{n-2} (j+k+m) + {}_n C_3 a^{n-3} (j^2 + jk + k^2 - m^2) + \cdots \\ &\quad + {}_n C_{n-1} a (j^{n-2} + j^{n-3} k + j^{n-4} k^2 + \cdots + k^{n-2} + m^{n-2}) \\ &\quad + (j^{n-1} + j^{n-2} k + j^{n-3} k^2 + \cdots + k^{n-1} - m^{n-1}) \} \end{aligned}$$

## 1.5 ${}_nC_r$ は $n$ の倍数

ところで、 $n$  は奇素数より、 ${}_nC_r$  は  $n$  でくくれる。よって、右辺が  $n$  でくくれるには、

$$j^{n-1} + j^{n-2}k + j^{n-3}k^2 + \cdots + k^{n-1} - m^{n-1}$$

が  $n$  でくくれれば良い。これに、 $j = k + m$  を代入すると、

$$(k + m)^{n-1} + (k + m)^{n-2}k + (k + m)^{n-3}k^2 + \cdots + k^{n-1} - m^{n-1}$$

### 1.5.1 これらを二項定理で展開

これらを二項定理で展開すると、

$$\begin{aligned} &= k^{n-1} + {}_{n-1}C_1 k^{n-2}m + {}_{n-1}C_2 k^{n-3}m^2 + \cdots + {}_{n-1}C_{n-2} km^{n-2} \\ &+ k^{n-1} + {}_{n-2}C_1 k^{n-2} + {}_{n-2}C_2 k^{n-3} + \cdots + km^{n-2} \\ &+ k^{n-1} + {}_{n-3}C_1 k^{n-2} + {}_{n-3}C_2 k^{n-3} + \cdots + k^2 m^{n-3} \\ &\quad \cdot \\ &\quad \cdot \\ &\quad \cdot \\ &+ k^{n-1} \end{aligned}$$

念のため、一番上の末尾の  $m^{n-1}$  は相殺されて消えています。

$k^{n-1}$  の個数は  $n$  個なので、 $k^{n-1}$  の係数は  $n$ 。

また、 $k^{n-2}m$  の係数は、

$${}_{n-1}C_1 + {}_{n-2}C_1 + {}_{n-3}C_1 + \cdots + {}_1C_1$$

$n - 1$  個である。これを (ア) 式とする。

$k^{n-3}$  の係数は、

$${}_{n-1}C_2 + {}_{n-2}C_2 + {}_{n-3}C_2 + \cdots + {}_2C_2$$

$n - 2$  個である。これを (イ) 式とする。

以後、 $\cdots k^2 m^{n-3}$  は 3 個、 $km^{n-2}$  は 2 個となり、 $km^{n-2}$  と  $k^{n-1}$ 、 $k^2 m^{n-3}$  と  $k^{n-2}m$  などの係数はペアで等しくなる。

ところで、(ア) より、

$${}_1C_1 + {}_2C_1 + {}_3C_1 + \cdots + {}_{n-1}C_1 = 1 + 2 + 3 + \cdots + (n-1) = n(n-1)/2$$

(イ) より、

$${}_2C_2 + {}_3C_2 + {}_4C_2 + \cdots + {}_{n-1}C_2 = 1 + 3 + 6 + \cdots + (n-1)(n-2)/2$$

この係数は、実はパスカルの三角形を斜めに読んだ数列となっている<sup>1</sup>。よって、こちら<sup>2</sup>より、

$$1 + 3 + 6 + \dots + (n-1)(n-2)/2 = n(n-1)(n-2)/6$$

など、全て  $n$  で括れる。(他のも全て成り立つ。)<sup>3</sup>

よって、 $(a-m)^n = nm \text{ P}(a, k, m)$  と置ける。ここで、 $a-m$  を素数とすると、 $n$  は奇素数より  $a-m = n$  である。

### 1.6 $a+b-c$ が素数である場合

また、 $m = j - k = (a+j) - (a+k) = c - b$  よって、 $a - m = a - (c - b) = a + b - c$  つまり、 $a + b - c$  が素数である場合を考える。

ところで、 $a^n + b^n = b^n$  ( $n$  は奇素数) の偶奇性を考えると、

- i.  $a$  : 偶数,  $b$  : 偶数,  $c$  : 偶数の場合
- ii.  $a$  : 偶数,  $b$  : 奇数,  $c$  : 奇数 ( $a$  : 奇数,  $b$  : 偶数,  $c$  : 奇数) の場合
- iii.  $b$  : 奇数,  $b$  : 奇数,  $c$  : 偶数の場合

の場合しかない。今、 $a - m = n$  より、 $a - m = a - (c - b) = a + b - c = n$  よって、 $a + b = c + n$  ( $n$  は奇数) である。

- i. の場合、偶数+偶数=偶数+奇数より、偶数=奇数 よって、矛盾。
- ii. の場合、偶数+奇数=奇数+奇数より、奇数=偶数 よって、矛盾。
- iii. の場合、奇数+奇数=偶数+奇数より、偶数=奇数 よって、矛盾。

よって、全ての場合で矛盾が生じるので、背理法により、 $a^n + b^n = b^n$  が成り立つ自然数  $a, b, c$  は存在しない。

よって、フェルマーの最終定理の制限付きの一般の  $n$  の場合が示された。

<sup>1</sup><https://ja.wikipedia.org/wiki/パスカルの三角形>

<sup>2</sup><http://hyonemitsu.web.fc2.com/Oumrawasanno40.pdf>

<sup>3</sup><http://hyonemitsu.web.fc2.com/Katuyousanpo.pdf> ( 7 , 8 ページ )