

フェルマーの最終定理の証明 (a, b いずれかだけが素数)

愛犬ベルのために

最新 2021 年 11 月 12 日

はじめに

これは、BBS「数の不思議世界」で、壊れた扉さんと議論しながら、完成したものです。ここまでにとどり着くには、壊れた扉さんのご尽力があったからこそで、改めてお礼を申し上げます。

更新履歴

- 2021.11.6 新規作成
- 2021.11.6 第 2 版補題追加 間違い修正
- 2021.11.7 第 3 版修正
- 2021.11.8 第 4 版修正
- 2021.11.8 第 5 版修正
- 2021.11.10 第 6 版修正
- 2021.11.12 第 7 版修正
- 2021.11.12 第 8 版修正

フェルマーの最終定理 (ただし、 a は素数とする。しかし、 a, b を入れ替えても一般性に欠けることはない)

$a^n + b^n = c^n$ が成り立つお互いに素である自然数 a, b, c が存在すると仮定する。ただし、 n は奇数とする。

$$a^n + b^n = c^n$$

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

$$a^n = (c - b)\{c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1}\}$$

ここで、 a は素数より次のようになる。

$$1 = c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = a^n$$

$$a = c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = a^{n-1}$$

$$a^2 = c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = a^{n-2}$$

$$\begin{aligned}
a^3 &= c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = a^{n-3} \\
&\cdot \\
&\cdot \\
&\cdot \\
a^{n-2} &= c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = a^2 \\
a^{n-1} &= c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = a \\
a^n &= c - b, c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1} = 1
\end{aligned}$$

$a^n + b^n = c^n$ となる自然数 a, b, c が存在すると仮定して、 $a = 1, b = 1$ を代入すると、 $c^n = 2$ より、自然数 c は存在しない。

よって、以後、 $a \geq 1, b \geq 2$ または $a \geq 2, b \geq 1$ の場合について考察する。

1 $c - b = 1, c^n - b^n = a^n$ の場合

$c - b = 1$ より、 $c = b + 1$ である。

$$\begin{aligned}
c^n - b^n &= a^n \\
(b + 1)^n - b^n &= a^n
\end{aligned}$$

さて、 n が奇数なので、 $(b + 1)^n$ と b^n は、グラフで考えると、単調増加のグラフで平行である。また、 $(b + 1)^n > b^n$ であるから、 $g(x) = (x + 1)^n - x^n > 0$ で、いかなる x においても、 $g(x) = 0$ にならない。つまり、 $g(u) = (x - u)g'(u) = 0$ とはできない。ゆえに、因数分解できない。

よって、 $c^n - b^n = a^n$ 左辺は因数分解できないので、右辺のようにはならない。であるから、 $c^n - b^n = a^n$ は、成り立たない。

したがって、 $c - b = 1, c^n - b^n = a^n$ の場合は、ありえない。

2 $c - b = a, c^n - b^n = a^n$ の場合

$(c - b)^n = a^n$ より、

$$\begin{aligned}
(c - b)^n &= a^n \\
(c - b)^n &= c^n - b^n \quad \text{-----イ}
\end{aligned}$$

ここで、

$$(c-b)^n - (c^n - b^n)$$

また、 $c = b + j$ と置くと

$$= j^n - (b+j)^n + b^n$$

二項定理より

$$= j^n - \sum_{r=0}^n (nC_r) b^{n-r} j^r + b^n$$

さて、 $r = 0$ なら、 $(nC_0)b^{n-0} = b^n$ よって、

$$= j^n - \sum_{r=1}^n (nC_r) c^{n-r} j^r - b^n + b^n$$

$$= j^n - \sum_{r=1}^n (nC_r) c^{n-r} j^r$$

また、 $r = n$ なら、 $(nC_n)c^{n-n}j^n = j^n$ よって、

$$= j^n - \sum_{r=1}^{n-1} (nC_r) c^{n-r} j^r - j^n$$

$$= - \sum_{r=1}^{n-1} (nC_r) c^{n-r} j^r < 0$$

ゆえに、

$$(c-b)^n < (c^n - b^n)$$

よって、イと矛盾。

3 $c - b = a^2, c^n - b^n = a^n$ の場合

$(c-b)^n = a^{2n}$, $(c^n - b^n)^2 = a^{2n}$ より、
 $(c-b)^n = (c^n - b^n)^2$ 補題より $(c^n - b^n)^2 > (c-b)^n$
よって、矛盾。

4 $c - b = a^3, a^n + b^n = a^n$ の場合

$(c-b)^n = a^{3n}$, $(c^n - b^n)^3 = a^{3n}$ より、
 $(c^n - b^n)^3 = (c-b)^n$ ところで、補題より、 $(c^n - b^n)^2 > (c-b)^n$
 $(c^n - b^n)^3 > (c^n - b^n)^2 > (c-b)^n$
 $(c^n - b^n)^3 > (c-b)^n$ よって、矛盾。

5 $c - b = a^4, a^n + b^n = a^n$ の場合

$(c - b)^n = a^{4n}, (c^n - b^n)^4 = a^{4n}$ より、
 $(c^n - b^n)^4 = (c - b)^n$ ところで、補題より、 $(c^n - b^n)^2 > (c - b)^n$
 $(c^n - b^n)^4 > (c^n - b^n)^2 > (c - b)^n$
 $(c^n - b^n)^4 > (c - b)^n$ よって、矛盾。

6 $c - b = a^5, a^n + b^n = a^n$ の場合

$(c - b)^n = a^{5n}, (c^n - b^n)^5 = a^{5n}$ より、
 $(c^n - b^n)^5 = (c - b)^n$ ところで、補題より、 $(c^n - b^n)^2 > (c - b)^n$
 $(c^n - b^n)^5 > (c^n - b^n)^2 > (c - b)^n$
 $(c^n - b^n)^5 > (c - b)^n$ よって、矛盾。

•

•

•

•

•

$c - b = a^{n-1}, c^n - b^n = a^n$ の場合

$(c - b)^n = a^{n(n-1)}, (c^n - b^n)^{n-1} = a^{n(n-1)}$ より、
 $(c^n - b^n)^{n-1} = (c - b)^n$
ところで、補題より、 $(c^n - b^n)^2 > (c - b)^n$
 $(c^n - b^n)^{n-1} > (c^n - b^n)^2 > (c - b)^n$
 $(c^n - b^n)^{n-1} > (c - b)^n$ よって、矛盾。

$c - b = a^n, c^n - b^n = a^n$ の場合

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

$$c - b = (c - b)\{c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \cdots + cb^{n-2} + b^{n-1}\}$$

$c - b \neq 0$ より、両辺を割って、

$$1 = c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \cdots + cb^{n-2} + b^{n-1}$$

ここで、 c, b は自然数よりあり得ない。

以上より、 a が素数の場合、フェルマーの最終定理は証明された。

補題

$(c^n - b^n)^2 > (c - b)^n$ の証明 (ただし、 c, b は $c > b$ の自然数)

$c = 2, b = 1$ の時、

$$((c^n - b^n)^2 - (c - b)^n) = (2^n - 1^n)^2 - 1^n = (2^n - 1)^2 - 1 = (2^n)^2 - 2(2^n) + 1 - 1 = 2^{2n} - 2^{n+1} > 0$$

より、 $(c^n - b^n)^2 > (c - b)^2$ が成り立つ。

$$\begin{aligned} c^n - b^n &= (c - b)\{c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1}\} \\ (c^n - b^n)^2 &= (c - b)^2\{c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1}\}^2 \end{aligned}$$

そこで、

$$(c^n - b^n)^2 - (c - b)^n = (c - b)^2\{(c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1})^2 - (c - b)^{n-2}\}$$

ここで、 $c = b + j$ とおくと $c - b = j$ であるから、

$$(c^n - b^n)^2 - (c - b)^n = j^2\{(c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1})^2 - j^{n-2}\}$$

また、

$$\begin{aligned} &(c^{n-1} + c^{n-2}b + c^{n-3}b^2 + \dots + cb^{n-2} + b^{n-1})^2 \\ &= ((b + j)^{n-1} + (b + j)^{n-2}b + (b + j)^{n-3}b^2 + \dots + (b + j)b^{n-2} + b^{n-1})^2 \end{aligned}$$

これは、 b, j の多項式であり、展開すると各項にプラスの係数がつく。よって、

$$(c^n - b^n)^2 - (c - b)^n = j^2\{((b + j)^{n-1} + (b + j)^{n-2}b + (b + j)^{n-3}b^2 + \dots + (b + j)b^{n-2} + b^{n-1})^2 - j^{n-2}\}$$

は、 j^{n-2} の項だけ係数 -1 となるが、係数は 1 より大きいので、係数 $-1 > 0$ である。

ゆえに、

$$(c^n - b^n)^2 - (c - b)^n = j^2\{((b + j)^{n-1} + (b + j)^{n-2}b + (b + j)^{n-3}b^2 + \dots + (b + j)b^{n-2} + b^{n-1})^2 - j^{n-2}\} > 0$$

$$(c^n - b^n)^2 > (c - b)^n$$