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 8 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。ここまでにたどり着くには、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

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。

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

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

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

ここで、a は素数より次のようになる。

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

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

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

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

$$\cdot$$

.

.

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

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

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

1　$c - b = 1, c^n - b^n = a^n$ の場合

$c > a, b$ とする。

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

$c - b = 1$ より、$c = b + 1$。
よって、

$$c^n - b^n = (b+1)^n - b^n$$

$$c^n - b^n = \sum_{r=0}^{n} ({}_nC_r) b^{n-r} 1^r - b^n$$

$$c^n - b^n = \sum_{r=0}^{n} ({}_nC_r) b^{n-r} - b^n$$

ここで、$r = 0$ なら、$({}_nC_0)b^{n-0} = b^n$ よって、

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

$$c^n - b^n = \sum_{r=1}^{n} ({}_nC_r) b^{n-r}$$

また、$r = n$ なら、$({}_nC_n)b^{n-n} = 1$ よって、

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

$$c^n - b^n - 1 = \sum_{r=1}^{n-1} ({}_nC_r) b^{n-r}$$

よって、

$$c^n - b^n - 1 = b\{\sum_{r=1}^{n-1} ({}_nC_r) b^{n-r-1}\}$$

1.1 $g(b)$ と n

$g(b) = \sum_{r=1}^{n-1} ({}_nC_r) b^{n-r-1}$ とすると、

$$c^n - b^n - 1 = bg(b)$$

n が奇数のとき、$g(b)$ は偶数項。そこで、

$$g(-1) =_n C_1(-1)^{n-2} +_n C_2(-1)^{n-3} +_n C_3(-1)^{n-4} + \cdots +_n C_{n-2}(-1)^{n-(n-2)-1} +_n C_{n-1}(-1)^{n-(n-1)-1}$$

$$=_n C_1(-1)^{n-2} +_n C_2(-1)^{n-3} +_n C_3(-1)^{n-4} + \cdots +_n C_{n-2}(-1) +_n C_{n-1}(-1)^0$$

$$= -_nC_1 +_n C_2 -_n C_3 + \cdots -_n C_{n-2} +_n C_{n-1}$$

パスカルの三角形より、${}_nC_1 =_n C_{n-1}$　${}_nC_2 =_n C_{n-2}$　${}_nC_3 =_n C_{n-3}$　$\cdots$ であるから、

$$= -_nC_1 +_n C_2 -_n C_3 + \cdots -_n C_{n-2} +_n C_{n-1}$$

$$= 0$$

したがって、

$$g(b) = (b+1)g'(b)$$

ゆえに、

$$c^n - b - n - 1 = b(b+1)g'(b)$$

1.2 $a^n - 1$

さて、

$$c^n - b^n - 1 = a^n - 1$$

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

1.3 a が奇数

a が素数なので、奇数とすると、$a-1$ は偶数である。

1.3.1 n が偶数

n が偶数なら、

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

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

$1 + a + a^2 + a^3 + \cdots + a^{n-2} + a^{n-1}$ は、a が奇数なので、項数は $n-1$ より奇数なので、総和は奇数であるが、$+1$ があるので、偶数である。したがって、右辺は偶数同士の積であるから、左辺も偶数同士の積である。よって、b は偶数より、

$$a - 1 = b$$

$$a = b + 1$$

ここで、$c = b + 1$ より、$a = c$ である。しかし、$c > a, b$ より矛盾。

1.3.2 n が奇数

n が奇数なら、

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

$$b(b+1)g'(b) = (a-1)(1 + a + a^2 + a^3 + \cdots + a^{n-2} + a^{n-1})$$

$1 + a + a^2 + a^3 + \cdots + a^{n-2} + a^{n-1}$ は、a が奇数なので、項数は $n-1$ より偶数なので、総和は偶数であるが、$+1$ があるので、奇数である。したがって、右辺は偶数と奇数の積であるから、左辺も偶数と奇数の積である。よって、b が偶数ならば、前項と同じになるので、b が奇数だとすると、

$$a - 1 = b + 1$$

$$a = b + 2$$

ここで、$c = b + 1$ より、$a = c + 1$ である。しかし、$c > a, b$ より矛盾。

1.4 a が偶数

a が素数なので、偶数とすると、$a - 1$ は奇数である。

1.4.1 n が偶数

n が偶数なら、

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

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

$1 + a + a^2 + a^3 + \cdots + a^{n-2} + a^{n-1}$ は、a が偶数なので、項数に関係なく、総和は偶数であるが、$+1$ があるので、奇数である。したがって、右辺は奇数同士の積であるから、左辺も奇数同士の積である。よって、b は奇数より、

$$a - 1 = b$$

$$a = b + 1$$

ここで、$c = b + 1$ より、$a = c$ である。しかし、$c > a, b$ より矛盾。

1.4.2 n が奇数

n が奇数なら、

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

$$b(b+1)g'(b) = (a-1)(1 + a + a^2 + a^3 + \cdots + a^{n-2} + a^{n-1})$$

$1+a+a^2+a^3+\cdots+a^{n-2}+a^{n-1}$ は、a が偶数なので、項数に関係なく偶数なので、総和は偶数であるが、$+1$ があるので、奇数である。したがって、右辺は奇数と奇数の積であるから、左辺も奇数と奇数の積である。よって、b は奇数とすると、$b+1$ が偶数で、矛盾。また、b が偶数だと矛盾。
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、

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

$$(c-b)^n=c^n-b^n \quad ----イ$$

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、$(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^3>(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^3>(c-b)^n$　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、$(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^4>(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^4>(c-b)^n$　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、$(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^5>(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^5>(c-b)^n$　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、$(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^{n-1}>(c^n-b^n)^2>(c-b)^n$
$\therefore (c^n-b^n)^{n-1}>(c-b)^n$　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。

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

そこで、

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

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

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

また、

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

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、

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

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、

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

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