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 16 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
2021.11.10　第 6 版修正
2021.11.12　第 7 版修正
2021.11.12　第 8 版修正
2021.11.15　第 9 版修正
2021.11.16　第 10 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。また、n は奇素数とする。

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

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

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

ここで、a は素数より次のようになる。

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

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

$a^n + b^n = c^n$ 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、$a \geqq 1, b \geqq 2$ または $a \geqq 2, b \geqq 1$ の場合について考察する。

1　$c - b = 1, c^n - b^n = a^n$ の場合

$a^n + b^n = c^n$ において、お互い素な自然数 a, b, c を素因数分解すると、$a = st, b = uv, c = yz$ であったとすると、a, b, c がお互い素な自然数なので、s, t, u, v, y, z は皆違う素数である。したがって、a, b, c 皆偶数はありえない。また、a, b, c の 2 つが偶数もありえない。よって、a, b, c のすべてが奇数か、a, b, c のいずれか一つが偶数である。しかし、a, b, c のすべてが奇数なら、$a^n + b^n = c^n$ より、ありえない。したがって、a, b, c のいずれか一つが偶数だけを考えればよい。

さて、

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

$c - b = 1$ より、$c = b + 1$。
よって、

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

ここで、a が、偶数の素数とすると、b, c は、共に、奇数であるが、$c = b + 1$ より、矛盾する。よって、a は、奇素数である。

$(b + 1)^n$ は、b を含む n 項と $+1$ からなるので、$n + 1$ の数の和である。b が奇数なら、$(b + 1)^n$ は、偶数であり、したがって、c は、偶数である。

bが偶数であると、bを含むn項はすべて偶数であり、総和は偶数であるが、それと$+1$からなるので、$(b+1)^n$は、奇数である。よって、cが奇数となる。

また、

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

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

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、

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

1.1 a^n

さて、等比級数の和の公式より、

$$\frac{a^n - 1}{a-1} = 1 + a + a2 + a^3 + \cdots + a^{n-2} + a^{n-1}$$

$$a^n - 1 = (a-1)(1 + a + a2 + a^3 + \cdots + a^{n-2} + a^{n-1})$$

$$a^n = (a-1)(1 + a + a2 + a^3 + \cdots + a^{n-2} + a^{n-1}) + 1$$

$$a^n = (a-1) \sum_{r=0}^{n-1} a^r + 1$$

1.2 $c^n - b^n = a^n$

よって、

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

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

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

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

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

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

右辺自然数より、$\frac{b}{a-1}$ はある自然数である。そこで、その自然数を m とすると、

$$\frac{b}{a-1}=m$$

ところが a は奇素数であり、b が奇数ならば、そんな自然数 m はない。
ゆえに、b は、偶数である。

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

ここで、$r=n-1$ のとき、$({}_nC_r)b^{n-r-1}=({}_nC_{n-1})b^{n-(n-1)-1}={}_n\,C_{n-1}=n$ であるので、

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

n は奇素数なので、$a^{n-1}+a^{n-2}+\cdots+a^2+a+1$ は、因数分解できない。

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

左辺の $\sum_{r=1}^{n-1}({}_nC_r)b^{n-r-1}$ は、b が偶数なので、偶数である。しかし、$+n$ があるので、左辺の $\sum_{r=1}^{n-1}({}_nC_r)b^{n-r-1}+n$ は、奇数である。
右辺の $(a^{n-1}+a^{n-2}+\cdots+a^2+a+1)$ の a が奇数なので、a を含む項は、奇数であり、$n-1$ 個あるので、偶数であるが、$+1$ があるので、右辺のこの式は、奇数である。したがって、偶数同士の b、$a-1$ はお互いに対応するので、$b=a-1$ つまり、$a=b+1=c$ となる。これは矛盾。

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、

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

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