

フェルマーの最終定理の証明 (c は素数)

愛犬ベルのために

最新 2023 年 4 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。最終的に、まとめ上げてくださったのは、壊れた扉さんです。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

2021.11.1 新規作成

2021.11.1 第 2 版 (4), (5), (6) の修正

2021.11.2 第 3 版 補題順序の修正と些細な修正

2023.4.16 第 4 版 補題の修正

1 フェルマーの最終定理 (ただし、 c は素数とする)

$a^n + b^n = c^n$ 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。

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-1}b + a^{n-3}b^2 - a^{n-4}b^3 + \dots - ab^{n-2} + b^{n-1}) = c^n$$

ここで、 c は素数より次のようになる。

(1) $a + b = 1, a^n + b^n = c^n$ の場合、 a, b は自然数よりあり得ない。

(2) $a + b = c, a^n + b^n = c^n$ の場合、 $(a + b)^n = c^n$ より、 $(a + b)^n = a^n + b^n$ a, b は自然数 より $(a + b)^n > a^n + b^n$ よって、矛盾。

(3) $a + b = c^2, a^n + b^n = c^n$ の場合、 $(a + b)^n = c^{2n}$, $(a^n + b^n)^2 = c^{2n}$ より、 $(a + b)^n = (a^n + b^n)^2$ 補題より $(a^n + b^n)^2 > (a + b)^n$

よって、矛盾。

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

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

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

・
・
・
・
・

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

(n + 1) $a + b = c^n, a^n + b^n = c^n$ の場合、 $a + b = a^n + b^n$ ここで、 a, b は $a \geq 1, b \geq 2$
または $a \geq 2, b \geq 1$ 自然数よりあり得ない。

(1) ~ (n + 1) より、 c が素数の場合、フェルマーの最終定理は証明された。

2 補題

$(a^n + b^n)^2 > (a + b)^n$ の証明 (ただし、 $a \geq 1, b \geq 2$ または $a \geq 2, b \geq 1$)

$a = 1, b = 2$ の時、

$$((a^n + b^n)^2 - (a + b)^n) = (1 + 2^n)^2 - 3^n = 2^{2n} + 2(2^n) + 1 - 3^n = 4^n - 3^n + 2^{n+1} + 1 > 0$$

より、 $(a^n + b^n)^2 > (a + b)^n$ が成り立つ。また、 $a = 2, b = 1$ としても同様である。

以降、 $a \geq 2, b \geq 2$ とする。

$$(a^n + b^n)^2 - (a + b)^n \text{ より、 } a^{2n} + 2a^n b^n + b^{2n} - (a + b)^n$$

ここで、 $b^{2n} - (a + b)^n$ を調べる。そこで、 $b = a + j$ (ただし、 $j \geq 0$) と置くと、 $b^{2n} - (a + b)^n = (a + j)^{2n} - (2a + j)^n$ これを二項定理で展開すると、

$$(a + j)^{2n} - (2a + j)^n = a^{2n} + {}_{2n}C_1 a^{2n-1} j + {}_{2n}C_2 a^{2n-2} j^2 + \cdots + {}_{2n}C_r a^{2n-r} j^r + \cdots + j^{2n} \\ - \{ (2a)^n + {}_n C_1 (2a)^{n-1} j + {}_n C_2 (2a)^{n-2} j^2 + \cdots + {}_n C_r (2a)^{n-r} j^r + \cdots + j^n \}$$

ところで、この式を j の多項式と考えると、 $(2a + j)^n$ の項数は $n + 1$ 個で $(a + j)^{2n}$ の項数は $2n + 1$ 個で、初めの $n + 1$ 個の和との差が正ならば当然全部同士の差も正である。

よって、

$$\sum_{r=0}^n \{ {}_{2n}C_r a^{2n-r} j^r \} - \sum_{r=0}^n \{ {}_n C_r (2a)^{n-r} j^r \} \geq 0$$

を示す。

$${}_{2n}C_r a^{2n-r} j^r - {}_n C_r (2a)^{n-r} j^r = \frac{(2n)!}{(2n-r)! r!} a^{2n-r} j^r - \frac{n!}{(n-r)! r!} 2^{n-r} a^{n-r} j^r \\ = \left\{ \frac{(2n)! a^n}{(2n-r)! r!} - \frac{n! 2^{n-r}}{(n-r)! r!} \right\} a^{n-r} j^r \\ = \left\{ \frac{(2n)! a^n}{(2n-r)!} - \frac{n! 2^{n-r}}{(n-r)!} \right\} \frac{a^{n-r} j^r}{r!}$$

$$= \{ 2n(2n-1)(2n-2) \cdots (2n-r+1) a^n - n(n-1)(n-2) \cdots (n-r+1) 2^{n-r} \} \frac{a^{n-r} j^r}{r!}$$

ところで、 $2n(2n-1)(2n-2) \cdots (2n-r+1)$ と $n(n-1)(n-2) \cdots (n-r+1)$ の項数は共に r 個で等しく、出だしが $2n$ と n なので、

$$2n(2n-1)(2n-2) \cdots (2n-r+1) > n(n-1)(n-2) \cdots (n-r+1)$$

である。

また、 $a \geq 2$ より、 $a^n \geq 2^{n-r}$ ($a = 2, r = 0$ の時等号成立)

$$2n(2n-1)(2n-2)\cdots(2n-r+1)a^n > n(n-1)(n-2)\cdots(n-r+1)2^{n-r}$$

$$2n(2n-1)(2n-2)\cdots(2n-r+1)a^n - n(n-1)(n-2)\cdots(n-r+1)2^{n-r} > 0$$

$$\{2n(2n-1)(2n-2)\cdots(2n-r+1)a^n - n(n-1)(n-2)\cdots(n-r+1)2^{n-r}\} \frac{a^{n-r}j^r}{r!} \geq 0 (j = 0 \text{ の時等号成立})$$

$${}_{2n}C_r a^{2n-r} j^r - {}_n C_r (2a)^{n-r} j^r \geq 0$$

$$\sum_{r=0}^n \{{}_{2n}C_r a^{2n-r} j^r\} - \sum_{r=0}^n \{{}_n C_r (2a)^{n-r} j^r\} \geq 0$$

$$(a+j)^{2n} - (2a+j)^n = a^{2n} + {}_{2n}C_1 a^{2n-1}j + {}_{2n}C_2 a^{2n-2}j^2 + \cdots + {}_{2n}C_r a^{2n-r}j^r + \cdots + j^{2n}$$

$$- \{(2a)^n + {}_n C_1 (2a)^{n-1}j + {}_n C_2 (2a)^{n-2}j^2 + \cdots + {}_n C_r (2a)^{n-r}j^r + \cdots + j^n\} \geq 0 \quad (a = 2, r = 0 \text{ の時等号成立})$$

$$(a^n + b^n)^2 > (a+b)^n$$