

フェルマーの最終定理（制限付きの一般の n の場合）の証明

c が素数の場合

希暮竜輔

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、 $(a^5)^3 + (b^5)^3 = (c^5)^3$ とすれば成り立つ a, b, c が存在しない事は自明なので、あとは n が奇素数の場合のみを考えれば良い。そこで、

$a^n + b^n = c^n$ (n は奇素数) が成り立つ自然数 a, b, c が存在すると仮定して、 $a = 1, b = 1$ とすると $c^n = 2$ となり、自然数 c は存在しない。よって、以後、 $a \geq 1, b \geq 2$ または $a \geq 2, b \geq 1$ の場合を考察する。 n が奇数より、

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

ここで、 c が素数より、次のように $n + 1$ 通りに場合分け出来る。

(1) $a + b = 1, a^n + b^n = c^n$ の場合、 a, b は自然数より矛盾。

(2) $a + b = c, a^n + b^n = c^n$ の場合、第 1 式を第 2 式に代入すると、 $a^n + b^n = (a + b)^n$ ところで、 a, b は自然数より $a^n + b^n < (a + b)^n$ よって、矛盾。

(3) $a + b = c^2, a^n + b^n = c^n$ の場合、 $(a + b)^n = c^{2n}$ ——① また、 $(a^n + b^n)^2 = c^{2n}$ ——② ①, ②より、 $(a^n + b^n)^2 = (a + b)^n$ ところで、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、 $(a + b)^n = c^{3n}$ ——① また、 $(a^n +$

$b^n)^3 = c^{3n}$ ———② ①, ②より、 $(a^n + b^n)^3 = (a + b)^n$ ところで、補題より、

$$(a^n + b^n)^2 > (a + b)^n \quad \therefore (a^n + b^n)^3 > (a^n + b^n)^2 > (a + b)^n$$

$\therefore (a^n + b^n)^3 > (a + b)^n$ よって、矛盾。

(5) $a + b = c^4, a^n + b^n = c^n$ の場合、 $(a + b)^n = c^{4n}$ ———① また、 $(a^n +$

$b^n)^4 = c^{4n}$ ———② ①, ②より、 $(a^n + b^n)^4 = (a + b)^n$ ところで、補題より、

$$(a^n + b^n)^2 > (a + b)^n \quad \therefore (a^n + b^n)^4 > (a^n + b^n)^2 > (a + b)^n$$

$\therefore (a^n + b^n)^4 > (a + b)^n$ よって、矛盾。

.

.

.

(n) $a + b = c^{n-1}, a^n + b^n = c^n$ の場合、 $(a + b)^n = c^{n(n-1)}$ ———① また、

$(a^n + b^n)^{n-1} = c^{n(n-1)}$ ———② ①, ②より、 $(a^n + b^n)^{n-1} = (a + b)^n$ ところ

で、補題より、 $(a^n + b^n)^2 > (a + b)^n \quad \therefore (a^n + b^n)^{n-1} > (a^n + b^n)^2 > (a + b)^n$

$\therefore (a^n + b^n)^{n-1} > (a + b)^n$ よって、矛盾。

(n + 1) $a + b = c^n, a^n + b^n = c^n$ の場合、 $a + b = a^n + b^n$ ところで、 a, b は

$a \geq 1, b \geq 2$ または $a \geq 2, b \geq 1$ の自然数より矛盾。

(1) ~ (n + 1) より、背理法により c が素数の場合、フェルマーの最終定理
が示された。

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 $a \geq 2, b \geq 1$

証明

$a = 1, b = 2$ の場合、 $(a^n + b^n)^2 - (a + b)^n = (1^n + 2^n)^2 - (1 + 2)^n = (2^n + 1)^2 -$

$$3^n = 2^{2n} + 2 \cdot 2^n + 1 - 3^n = 4^n - 3^n + 2^{n+1} + 1 > 0$$

$\therefore (a^n + b^n)^2 - (a + b)^n > 0 \quad \therefore (a^n + b^n)^2 > (a + b)^n$ ($a = 2, b = 1$ の場合も同様。)

よって、以後、 $a \geq 2, b \geq 2$ の場合を示す。

$(a^n + b^n)^2 > (a + b)^n$ 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、

$$(a + j)^{2n} - (2a + j)^n$$

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

$$+ \cdots + j^{2n}$$

$$- \left\{ (2a)^n + {}_nC_1 (2a)^{n-1} j + {}_nC_2 (2a)^{n-2} j^2 + \cdots + {}_nC_r (2a)^{n-r} j^r \right.$$

$$\left. + \cdots + j^n \right\}$$

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、

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

を示す。

$$\begin{aligned} {}_{2n}C_r a^{2n-r} j^r - {}_nC_r (2a)^{n-r} j^r &= \frac{(2n)!}{(2n-r)! r!} a^{2n-r} j^r - \frac{n!}{(n-r)! r!} 2^{n-r} a^{n-r} j^r \\ &= \left\{ \frac{(2n)! a^n}{(2n-r)! r!} - \frac{n! 2^{n-r}}{(n-r)! r!} \right\} a^{n-r} j^r = \left\{ \frac{(2n)! a^n}{(2n-r)!} - \frac{n! 2^{n-r}}{(n-r)!} \right\} \frac{a^{n-r} j^r}{r!} \\ &= \left\{ 2n(2n-1)(2n-2) \cdots (2n-r+1) a^n \right. \\ &\quad \left. - n(n-1)(n-2) \cdots (n-r+1) 2^{n-r} \right\} \frac{a^{n-r} j^r}{r!} \end{aligned}$$

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、 $a^n \geq 2^{n-r}$ (等号成立は $a=2, r=0$ の時。) よって、

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

よって、 $2n(2n-1)(2n-2) \cdots (2n-r+1) a^n - n(n-1)(n-2) \cdots$

$(n-r+1) 2^{n-r} > 0$ よって、

$$\begin{aligned} &\left\{ 2n(2n-1)(2n-2) \cdots (2n-r+1) a^n \right. \\ &\quad \left. - n(n-1)(n-2) \cdots (n-r+1) 2^{n-r} \right\} \frac{a^{n-r} j^r}{r!} \geq 0 \end{aligned}$$

(等号成立は $j = 0$ の時。)

$\therefore {}_{2n}C_r a^{2n-r} j^r - {}_nC_r (2a)^{n-r} j^r \geq 0$ よって、

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

よって、

$$\begin{aligned} & (a+j)^{2n} - (2a+j)^n \\ &= a^{2n} + {}_{2n}C_1 a^{2n-1} j + {}_{2n}C_2 a^{2n-2} j^2 + \cdots + {}_{2n}C_r a^{2n-r} j^r \\ &+ \cdots + j^{2n} \\ &- \left\{ (2a)^n + {}_nC_1 (2a)^{n-1} j + {}_nC_1 (2a)^{n-2} j^2 + \cdots + {}_nC_r (2a)^{n-r} j^r \right. \\ &\left. + \cdots + j^n \right\} \geq 0 \end{aligned}$$

(等号成立は $a = 2, r = 0$ の時。)

$$r > 0 \text{ より、 } (a+j)^{2n} - (2a+j)^n > 0 \quad \therefore b^{2n} - (a+b)^n > 0 \quad \therefore b^{2n} > (a+b)^n$$

$$\therefore a^{2n} + 2a^n b^n + b^{2n} > (a+b)^n \quad \therefore (a^n + b^n)^2 > (a+b)^n$$

ところで、 $b = a + j$ ($j \geq 0$) で $a \geq 2$ より、 $b \geq 2$

よって、 $a \geq 2, b \geq 2$ の場合が示され、初めの $a = 1, b = 2$ の場合と合わせると、

$a \geq 1, b \geq 2$ または $a \geq 2, b \geq 1$ で、 $(a^n + b^n)^2 > (a+b)^n$ が成り立つ。

よって、示された。