P-4

カタラン予想について

前田 雄貴
Yuki Maeda[1]

Abstract: In 1844, E. C. Catalan conjectured that the Diophantine equation $x^p - y^q = 1$ admits no solution other than the one given by $x = 3, p = 2$ and $y = 2, q = 3$ in $x, y \geq 1, p, q \geq 2$ in integers. P. Mihăilescu proved during 2000 and 2006 that this conjecture is true. However, the case in $q = 2$ was already proven by V. A. Lebesgue in 1850. In this article, we give a brief sketch of the proof due to Lebesgue when $q = 2$.

1　導入

カタラン予想は 1844 年に Eugène Charles Catalan が数学の学術雑誌 Crelle (Journal für die reine und angewandte Mathematik) の編集者宛に送った手紙の中に書かれた問題であった.

Conjecture 1 カタラン予想 (E. Catalan,1844)
正の整数の累乗で表される数列
$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, \cdots$
のうち， 差が 1 となる 2 数は 8 と 9 に限る. 即ち，x, y を 1 以上の整数，m, n を 2 以上の整数とすると，これら 4 個を未知数とする方程式

$$x^m - y^n = 1 \tag{1}$$

の整数解 x, y, m, n は，$x = 3$, $y = 2$, $m = 2$, $n = 3$ に限る.

このカタラン予想は 2000 年から 2006 年にかけて P. Mihăilescu [2][3] によって解決された. 以下，この予想が証明された経緯を記そう.
まずもとの方程式 $x^m - y^n = 1$ において指数を素数の範囲に限り，カタラン予想を

$$x^p - y^q = 1$$

を満たす正整数 x, y および正の素数 p, q の範囲で考えても一般性を失わないことが分かる．1850 年に V. A. Lebesgue によって $q = 2$ の場合が証明された. 次の節でその証明を与える.
また，1965 年に Ko Chao によって $p = 2$ の場合も証明された．この考察から $p, q \in \mathbb{Z}$ は奇素数の場合に限って良いことが分かる．さて 1976 年に R. Tijdeman により，下記の A. Baker の定理を用いて解が有限個であることが証明された.

Theorem 1 (A. Baker, 1974)
定められた次数以下の 0 でない代数的数 $\alpha_1, \cdots, \alpha_n$ を考える．このとき，$\alpha_1, \cdots, \alpha_n$ による具体的に計算可能な正定数 C_1 で次をみたすものが存在する．$b_1, \cdots, b_n \in \mathbb{Z}$ を未知数とする不等式

$$0 < |\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| < B^{-C_1}$$

は絶対値が B 以下である整数解 $b_1, \cdots, b_n$ をひとつも持たない.

この Theorem 1 を用いて Tijdeman は次を証明した.

Theorem 2 (R. Tijdeman, 1976)
絶対定数 $C_2 > 0$ で次をみたすものが存在する．x, y を 1 以上の整数，p, q を素数とする.

$$x^p - y^q = 1 \tag{2}$$

が成立するならば,

$$\max\{x, y, p, q\} \leqq C_2$$

である.

Theorem 2 により (2) を満たす可能性のある x, y, p, q の全てが理論的に求まり，その候補者を $x^p - y^q = 1$ に代入して等号が成り立つかどうかを確かめればカタラン予想は完全に解決されたはずであった．しかし C_2 は非常に大きな定数であったため，計算時間がかかりすぎてこの手続きができず，このときにはカタラン予想の完全解決は出来なかった.

2000 年から 2003 年に Mihăilescu によって証明された 3 つの定理の帰結としてカタラン予想は最初に解決されたと言って良い. その定理を以下に順番にあげていく.

Theorem 3 (P. Mihăilescu, 2000)
x, y を 1 以上の整数，p, q を 3 以上の素数とする．このとき方程式 (2) を満たす p, q に対して次の 2 条件が同時に成立する.

$$p^{q-1} \equiv 1 (\mathrm{mod}\ q^2), \quad q^{p-1} \equiv 1 (\mathrm{mod}\ p^2). \tag{3}$$

この条件は Wieferich 素数という概念に関して現れるものであることが知られている． この定理はカタラン予想の方程式を満たす素数 p, q は少ししか存在しないことを説明しているが，この定理を満たす素数として例えば $p = 83, q = 4871$ や $p = 2903, q = 18787$ が存在することが確かめられる．しかしながら，ここに上記の Baker の Theorem 1 を応用すると, 計算機を用いて 2002 年に $x = 3, y = 2, p = 2, q = 3$ 以外の可能性がすべて消された. 従って一度ここでカタラン予想は完全解決された. その後，Mihăilescu は代数的な考察を進めて次の定理を得た.

[1]日大理工・院 (前)・数学

Theorem 4 (P. Mihăilescu, 2003)
x, y を 1 以上の整数，p, q を 3 以上の素数とする．このとき方程式 (2) をみたす p, q に対して次の 2 条件の少なくとも一方が成立する．

$$p < 4q^2, \quad q < 4p^2. \tag{4}$$

Theorem 3，Theorem 4 および，次の Theorem 5 を組み合わせれば，計算機の膨大な計算に無関係に，カタラン予想を完全解決に導くことが出来たのである．

Theorem 5 (P. Mihăilescu, 2004)
p, q を 3 以上 41 以下の素数とする．このとき方程式 (2) をみたす正整数 x, y は存在しない．

2　q=2 の場合

以下 (2) において $q = 2$ のときについて Lebesgue の証明 [1] を与えよう．p を素数とする．

Definition 1 $x \in \mathbb{Z}$ に対し，$x = mp^n (m \notin p\mathbb{Z}, n \in \mathbb{Z})$ と表す．このとき$\mathrm{ord}_p x = n$ と定める．

Proposition 1 (V. A. Lebesgue,1850)
素数 p，$x, y \in \mathbb{Z} (x \geq 1, y \geq 1)$ に対し，方程式

$$x^p = y^2 + 1 \tag{5}$$

は整数解 x, y, p を持たない．

証明
p の偶奇を考える．(4) を満たす $x, y \in \mathbb{Z}$ を考える.p が偶数ならば $(x^{\frac{p}{2}} + y)(x^{\frac{p}{2}} - y) = 1$ と変形できる．$x^{\frac{p}{2}} + y, x^{\frac{p}{2}} - y \in \mathbb{Z}$ より $x^{\frac{p}{2}} + y = x^{\frac{p}{2}} + y = \pm 1$（複号同順）となり,$y = 0$ である．これは $y \neq 0$ に矛盾. したがって p は奇数である．
次に x, y の偶奇を考える.mod 4 で考えると,
(i) y が偶数のとき $y \equiv 0$ or $2 (\mathrm{mod}\ 4)$ より $y^2 \equiv 0 (\mathrm{mod}\ 4)$ となるので $y^2 + 1 \equiv 1$ となる．(4) より $x^p \equiv 1 (\mathrm{mod}\ 4)$ となるので $x \equiv 1 (\mathrm{mod}\ 4)$ となり x は奇数に限る．
(ii) y が奇数のとき $y \equiv \pm 1 (\mathrm{mod}\ 4)$ より $y^2 \equiv 1 (\mathrm{mod}\ 4)$ となるので $y^2 + 1 \equiv 2 (\mathrm{mod}\ 4)$ 即ち $x^p \equiv 2 (\mathrm{mod}\ 4)$ となるが, 奇数 p に対して $x^p \equiv 0$ or 1 となるので不適. 従って x は奇数で y は偶数である．
一意分解整域 $\mathbb{Z}[i]$ 上で $1 + iy$ と $1 - iy$ は互いに素であることを示す．
$Q | 1 + iy, p | 1 - iy$ となる $\mathbb{Z}[i]$ の素元 Q を考える.$Q | (1 + iy) + (1 - iy) = 2$ であるが，$Q = 1 \pm i$ ならば $(1 \pm i)(\alpha + \beta i) = 1 + iy$ となる $\alpha, \beta \in \mathbb{Z}$ が存在して $\alpha = \dfrac{1 \pm y}{2}, \beta = \dfrac{1 \mp y}{2}$ となる．これは y が偶数であることに矛盾する．一意分解整域では素元と既約元は同値なので，2 を割る既約元が $1 \pm i$ に限ることから，互いに素である証明は終．
p が奇数なので $p \equiv 1 or 3 (\mathrm{mod} 4)$ である．一方 $\mathbb{Z}[i]$ の 4 個のみの単元 $1, -1, i, -i$ はそれぞれ単元の p 乗の $1^p, (-1)^p, i^p$ or $(i^3)^p, (-i)^p$ or $((-i)^3)^p$ で表せる．また (5) より $(1 + iy)(1 - iy)$ は p 乗の数で表せるので, 一意分解整域において $i + iy$ と $1 - iy$ は互いに素であることと併せると $1 + iy, 1 - iy$ はそれぞれ p 乗の数で表せる．即ちある $c \in \mathbb{Z}[i]$ に対して

$$1 + iy = c^p (c \in \mathbb{Z}[i])$$

と表せる.c の複素共役を $\bar{c}$ とすると

$$2 = c^p + \bar{c}^p = (c + \bar{c})(c^{p-1} - c^{p-2}\bar{c} + \cdots + \bar{c}^{p-1}).$$

それゆえ $c + \bar{c} \in \mathbb{Z}$ は 2 を割りきるので $c + \bar{c} = \pm 2$ 即ち $c = \pm(1 + bi)(b \in \mathbb{Z})$ である．$a + bi \in \mathbb{Z}[i]$ が $1 + i$ で割りきれるのは $a \equiv b (\mathrm{mod}\ 2)$ の場合に限ることから $b \equiv 1 (\mathrm{mod}\ 2)$ が従うが, y が偶数であるから c が $1 + i$ で割りきれないことより b は偶数でなければならない．$c + \bar{c} = \pm 2$ より

$$(1 + bi)^p + (1 - bi)^p = \pm 2 \tag{6}$$

である．(6) の右辺が -2 と仮定すると，$\mathrm{mod}\ 8\mathbb{Z}[i]$ において $2 \equiv -2$ となり矛盾する．従って (6) の右辺は 2 である. 二項展開により, 二項係数 $\binom{p}{k}$ に対し

$$\binom{p}{2}(bi)^2 + \binom{p}{4}(bi)^4 + \cdots + \binom{p}{p-1}(bi)^{p-1} = 0 \tag{7}$$

となる．
$b \neq 0$ と仮定すると,$\forall k (k$: 偶数,$4 \leq k \leq p - 1)$ に対して

$$\mathrm{ord}_2 \left(\binom{p}{k}(bi)^k \right) > \mathrm{ord}_2 \left(\binom{p}{2}(bi)^2 \right)$$

が成り立つ.$\binom{p-2}{k-2} \in \mathbb{Z}$ より

$$\binom{p}{k}\binom{p}{2}^{-1}(bi)^{k-2} = \binom{p-2}{k-2}\frac{2}{k(k-1)}(bi)^{k-2}$$

の 2 進附値は正である. 実際

$$\mathrm{ord}_2(2(bi)^{k-2}) \geq k-1 > \frac{\log k}{\log 2} \geq \mathrm{ord}_2(k) = \mathrm{ord}_2(k(k-1))$$

であるが，$\mathrm{ord}_2 \left(\binom{p}{2}(bi)^2 \right)$ は有限素点での附値の性質より，(7) 式の 2 進附値つまりこの和すべての ord_2 と等しくなる. ところが (7) よりこの和は 0 なので，2 進附値は ∞ となり矛盾. したがって $b = 0$ でなければならない．
$\therefore c = \pm 1$ となり $c = 1$ ならば $1 - iy = (1 + iy)(1 - iy) = x^p$ となり右辺 $\in \mathbb{R}$,左辺 $\notin \mathbb{R}$ より $y = 0$ となる．$c = -1$ のときも同様に矛盾する．
$\therefore$ (2) の解は存在しない．

References

[1] V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, Nouv. Ann. Math., 9, 1850, 178–181.

[2] P. Mihăilescu, A class number free criterion for Catalan's conjecture, J. Number Theory, 99, 2003, 225–231.

[3] P. Mihăilescu, On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation, J. Number Theory, 118, 2006, 123–144.

[4] R. Schoof, Catalan's Conjecture, Universitext, Springer, 2008.