ディオファントス方程式 $2^x + 5^y = z^2$ について

大塚美紀生

定理 方程式

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

を満たす非負整数の組 $(x,\ y,\ z)$ は $(3,\ 0,\ 3),\ (2,\ 1,\ 3)$ に限られる。

指数型不定方程式問題を背景とするこの定理は，論文[1]において，カタラン予想が肯定的に解決した[*注]ことを用いて証明されたが，それは鶏を割くのに牛刀を用いるようなものである。本稿では，この定理を初等的な手法のみで証明したい。

定理の証明

$x,\ y,\ z$ は(1)を満たす非負整数であるとする。奇数の平方が 8 で割ると 1 余ることに注目して，$x \geqq 3$ の場合と $x < 3$ の場合に分けて考える。

1° $x = 0$ のとき，(1)は

$$5^y = z^2 - 1 = (z+1)(z-1)$$

素因数分解を考えると，

$$z + 1 = 5^m,\ \ z - 1 = 5^n \ \ (m > n \geqq 0,\ \ m + n = y)$$

を満たす整数 $m,\ n$ が存在する。2 式の差をとると

$$2 = 5^m - 5^n = 5^n(5^{m-n} - 1)$$

となるから，素因数分解を考えると

$$5^n = 1,\ \ 5^{m-n} - 1 = 2 \qquad \therefore\ \ n = 0,\ \ 5^m = 3$$

ところが，m は正の整数であるから，$5^m = 3$ は素因数分解の一意性に反する。

2° $x = 1$ のとき，(1)は

$$2 + 5^y = z^2$$

$y = 0$ ならば $3 = z^2$ となって不成立であり，$y \geqq 1$ ならば $2 \equiv z^2 \pmod 5$ となり，2 が 5 を法として平方剰余でないことと矛盾する。

3° $x = 2$ のとき，(1)は

$$5^y = z^2 - 4 = (z+2)(z-2)$$

素因数分解を考えると，

$$z + 2 = 5^m,\ \ z - 2 = 5^n \tag{2}$$

$$m > n \geqq 0,\ \ m + n = y \tag{3}$$

を満たす整数 $m,\ n$ が存在する。(2)の 2 式の差をとると

$$4 = 5^m - 5^n = 5^n(5^{m-n} - 1)$$

となるから，素因数分解を考えると

$$5^n = 1,\ \ 5^{m-n} - 1 = 4 \qquad \therefore\ \ n = 0,\ \ m = 1$$

このとき，(2)より $z = 3$，(3)より $y = 1$ と定まる。

4° $x \geqq 3$ のとき，(1)より z は奇数であり，

$$5^y \equiv z^2 \equiv 1 \pmod 8$$

が成り立つ。ここで，奇数の平方を 8 で割ると 1 余ることは，

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$$

により確かめられる。(隣り合う整数の一方は偶数である。)

$$y \text{が偶数ならば } 5^y \equiv 1 \pmod 8, \quad y \text{が奇数ならば } 5^y \equiv 5 \pmod 8$$

であるから，

$$y = 2k \quad (k \text{は非負整数}) \tag{5}$$

と表され，

$$2^x = z^2 - 5^{2k} = (z + 5^k)(z - 5^k)$$

$z,\ 5^k$ がともに奇数であることに注意して素因数分解を考えると

$$z + 5^k = 2^m, \quad z - 5^k = 2^n \tag{6}$$

$$m > n \geqq 1, \quad m + n = x \tag{7}$$

を満たす整数 $m,\ n$ が存在する。(6)より

$$(z + 5^k) - (z - 5^k) = 2^m - 2^n$$

$$\therefore \ 5^k = 2^{m-1} - 2^{n-1} = 2^{n-1}(2^{m-n} - 1)$$

両辺の素因数分解を考えると

$$2^{n-1} = 1, \quad 2^{m-n} - 1 = 5^k \quad (k = 0 \text{の場合も含む})$$

$$\therefore \ n = 1, \quad 5^k + 1 = 2^{m-1} \tag{8}$$

ここで，$m \geqq 4$ であるとすれば $5^k + 1 \equiv 0 \pmod 8$ となるが，

$$5^k \equiv 1 \text{ または } 5 \pmod 8$$

に反するから，

$$m \leqq 3$$

に限られる。また，(7), (8)と場合分けの前提より

$$x = m + 1 \geqq 3$$

であるから，

$$m = 2 \text{ または } m = 3$$

(i) $m = 2$ のとき，(8)より

$$(m,\ n,\ k) = (2,\ 1,\ 0)$$

であるから，(7), (5), (6)より

$$x = m + n = 3, \quad y = 2k = 0, \quad z = 2^m - 5^k = 2^n + 5^k = 3$$

(ii) $m = 3$ のとき，(8)より $5^k = 3$ となるが，これは($k = 0$ の場合も含めて)素因数分解の一意性に反する。

以上より，(1)を満たす非負整数の組は

$$(x,\ y,\ z) = (2,\ 1,\ 3),\ (3,\ 0,\ 3)$$

に限られる。 (証明おわり)

注　カタラン予想 (Catalan's conjecture)とは，

$$X^U - Y^V = 1,\ U > 1,\ V > 1$$

を満たす自然数 $X,\ Y,\ U,\ V$ が $3^2 - 2^3 = 1$ 以外にはないという予想のことであるが，プレダ・ミハイレスク(Preda Mihăilescu) により肯定的に解決された(→ [3])。その証明には円分体の深い理論が用いられている。論文[3]が雑誌に掲載されたのは 2004 年であるが，内容が発表されたのは 2002 年のことである。

参考文献

[1] D. Acu, *On a diophantine equation*, General Math. 15, 145 - 148 (2007).

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

[3] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math 572, 167-195 (2004).

2009.2.3