方程式 $2^x + p^y = z^2$ の非負整数解

大塚美紀生

［1］において方程式 $2^x + 5^y = z^2$ の非負整数解を求めたが，同様の論法で少し一般化した結果を導くことができる。[注1]

定理　p が $p \equiv \pm 3 \pmod 8$ を満たす素数であるとき，方程式

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

を満たす非負整数の組 $(x,\ y,\ z)$ は

$p = 3$ のとき $(x,\ y,\ z) = (0,\ 1,\ 2),\ (3,\ 0,\ 3),\ (4,\ 2,\ 5)$

$p = 5$ のとき $(x,\ y,\ z) = (3,\ 0,\ 3),\ (2,\ 1,\ 3)$

$p > 5$ のとき $(x,\ y,\ z) = (3,\ 0,\ 3)$

に限られる。[注2]

平方剰余に関するある補題

奇素数 p について，$a^2 \equiv 2 \pmod p$ を満たす整数 a が存在するならば，

$$p \equiv \pm 1 \pmod 8$$

である。[注3]

(証明)　p についての数学的帰納法で証明する。

$p = 3,\ 5$ のとき 2 は平方剰余ではなく，$2 \equiv 3^2 \pmod 7$ であるから，2 が平方剰余である最小の奇素数は 7 である。

$$a^2 = 2 + bp \tag{2}$$

を満たす整数 $a,\ b$ が存在するような奇素数 p について，p より小さい奇素数は補題を満たすものとする。

$$(a - p)^2 \equiv a^2 \pmod p,\quad a - p \not\equiv a \pmod 2$$

であるから，

a は奇数，$3 \leqq a < p$

として一般性を失わない。このとき b も奇数であり，$0 < b < p$ である。

b の任意の素因数(奇素数)を q とすると，(2)より

$$a^2 \equiv 2 \pmod q$$

であり，$q < p$ より

$$q \equiv \pm 1 \pmod 8$$

が成り立つ。したがって，それらの積についても

$$b \equiv \pm 1 \pmod 8$$

が成り立つ。a は奇数で $a^2 \equiv 1 \pmod 8$ であるから，(2)より

$$1 \equiv 2 \pm p \pmod 8$$

であるが，これを満たすには $p \equiv \pm 1 \pmod 8$ の場合に限られ，2 が平方剰余となるすべての奇素数 p について成り立つ。　(証明おわり)

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

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

素因数分解を考えると，

$$z + 1 = p^m,\ \ z - 1 = p^n \tag{3}$$

$$m > n \geqq 0,\ \ m + n = y \tag{4}$$

を満たす整数 $m,\ n$ が存在する。(3) において 2 式の差をとると

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

となるから，素因数分解を考えると

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

(i) $p = 3$ のときは $m = 1$ であり，(4), (3) より

$$y = 1,\ \ z = 2$$

(ii) $p \neq 3$ のとき $p^m = 3$ は素因数分解の一意性に反する。

2° $x = 1$ のとき，(1) は

$$2 + p^y = z^2$$

$y = 0$ ならば $3 = z^2$ となって不成立であり，$y \geqq 1$ ならば $2 \equiv z^2 \pmod{p}$ であり，補題より $p \equiv \pm 1 \pmod 8$ となって仮定に反する。

3° $x = 2$ のとき，(1) は

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

素因数分解を考えると，

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

$$m > n \geqq 0,\ \ m + n = y \tag{6}$$

を満たす整数 $m,\ n$ が存在する。(5) において 2 式の差をとると

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

となるから，素因数分解を考えると

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

(i) $p = 5$ のとき $m = 1$ であり，(6), (5) より

$$y = 1,\ \ z = 3$$

(ii) $p \neq 5$ のとき，$p^m = 5$ は素因数分解の一意性に反する。

4° $x \geqq 3$ のとき，(1) より z は奇数であるから

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

が成り立つ。

y が偶数ならば $p^y \equiv 1 \pmod 8$，y が奇数ならば $p^y \equiv p \equiv \pm 3 \pmod 8$

であるから，

$$y = 2k \quad (k \text{ は非負整数}) \tag{7}$$

と表され，

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

$z,\ p^k$ 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

$$z + p^k = 2^m,\quad z - p^k = 2^n \tag{8}$$

$$m > n \geqq 1,\quad m + n = x \tag{9}$$

を満たす整数 $m,\ n$ が存在する。(8)より

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

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

両辺の素因数分解を考えると

$$2^{n-1} = 1,\quad 2^{m-n} - 1 = p^k \quad (k = 0 \text{ のときも成立})$$

$$\therefore\ n = 1,\quad p^k + 1 = 2^{m-1} \tag{10}$$

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

$$p^k \equiv 1 \text{ または } p \pmod 8,\quad p \equiv \pm 3 \pmod 8$$

に反するから，

$$m \leqq 3$$

に限られる。また，(9), (10)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，(10)より

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

であるから，(9), (7), (8)より

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

(ii) $m = 3$ のとき，(10)より $p^k = 3$ となり，

$p = 3$ ならば $k = 1$ であり，(9), (7), (8)より

$$x = m + n = 4,\quad y = 2k = 2,\quad z = 2^m - p^k = 2^n + p^k = 5$$

$p \neq 3$ ならば，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

$$p = 3 \text{ のとき } (x,\ y,\ z) = (0,\ 1,\ 2),\ (3,\ 0,\ 3),\ (4,\ 2,\ 5)$$

$$p = 5 \text{ のとき } (x,\ y,\ z) = (3,\ 0,\ 3),\ (2,\ 1,\ 3)$$

$$p > 5 \text{ のとき } (x,\ y,\ z) = (3,\ 0,\ 3)$$

に限られる。　　(証明おわり)

注 1　本稿では $p \equiv \pm 3 \pmod 8$ の場合を考えるが，$p \equiv \pm 1 \pmod 8$ の場合はかなり難しくなる。

注 2　$p = 5$ の場合は既に [1]で証明済みであるが，本稿でも再度証明されている。

注 3　本稿では必要条件としてのみ扱っているが，実は $p \equiv \pm 1 \pmod 8$ は 2 が p を法として平方剰余となるための必要十分条件である。[2]などの初等整数論の本を参照されたい。

参考文献

[1] 大塚美紀生，ディオファントス方程式 $2^x + 5^y = z^2$，
早稲田数学フォーラム (2009)　http://wasmath.la.coocan.jp/2x5yz2.pdf

[2] D.E.Flath, *Introduction to Number Theory*, Wiley (1989).

[3] C.E.Pumnea and A.D.Nicoară, *On a diophantine equation of* $a^x + b^y = z^2$ *type*, Educaţia Matematică 4−1, 65-75 (2008).

2009.10.1