Vol. 39 (2019)
No. 2

数 学 杂 志
J. of Math. (PRC)

关于指数 Diophantine 方程 $x^2 = D^{2m} - D^m p^n + p^{2n}$

贺艳峰
(延安大学数学与计算机科学学院, 陕西 延安 716000)

摘 要: 设 $D > 1$ 是正整数, p 是适合 $p \nmid D$ 的素数. 本文研究了指数 Diophantine 方程 $x^2 = D^{2m} - D^m p^n + p^{2n}$ 的满足 $m > 1$ 的正整数解. 根据 Diophantine 方程的性质, 结合已有的结论, 运用初等方法确定了方程满足 $m > 1$ 的所有正整数解 (D, p, x, m, n). 这个结果修正并完整解决了文献 [4] 的猜想.

关键词: 指数 Diophantine 方程; 正整数解; 初等方法
MR(2010) **主题分类号**: 11D61 **中图分类号**: O156.7
文献标识码: A **文章编号**: 0255-7797(2019)02-0279-08

1 引言和结论

设 $\mathbb{Z}$, $\mathbb{N}$ 分别是全体整数和正整数的集合. $D > 1$ 是正整数, p 是适合 $p \nmid D$ 的素数. 50 多年前, 陈景润 [1] 在研究数论中有关本原商高数的 Jeśmanowicz 猜想时, 曾涉及到方程

$$x^2 = D^{2m} - D^m p^n + p^{2n}, \quad x, m, n \in \mathbb{N} \tag{1.1}$$

的求解问题. 这是一类指数型的广义 Ramanujan-Nagell 方程, 它与数论、组合数学和编码理论中的很多重要问题的研究有关 (参考文献 [2]). 对此, 佟瑞洲在文献 [3] 中确定了方程 (1.1) 的所有适合 $m = 1$ 的解 (x, m, n); 在文献 [4] 中提出, 除了

$$(D, p, x, m, n) = (2, 3, 7, 3, 1) \tag{1.2}$$

以外, 方程 (1.1) 适合 $m > 1$ 的解必定满足下列两个条件之一:

(i) D 是奇数, $p \equiv 1 \pmod 8$, $m = 2$, $n = 1$;

(ii) D 是偶数, D 含有 $2kq + 1$ 之形素因数, 其中 q 是 m 的奇素因数.

然而, 方程 (1.1) 除了 (1.2) 以外, 显然还有解

$$(D, p, x, m, n) = (2, 5, 7, 3, 1) \tag{1.3}$$

不满足上述 (i) 和 (ii). 由此可知文献 [4] 的结果是不完整的.

对于非负整数 t, 设

$$u_{2t+1} = \frac{1}{\sqrt{2}}(\alpha^{2t+1} + \beta^{2t+1}), v_{2t+1} = \frac{1}{\sqrt{6}}(\alpha^{2t+1} - \beta^{2t+1}), \tag{1.4}$$

*收稿日期: 2017-09-11 接收日期: 2018-01-02
基金项目: 陕西省科技厅项目 (2013JQ1019); 延安大学自然科学基金项目 (YDK201101).
作者简介: 贺艳峰 (1976–), 女, 陕西神木, 副教授, 主要研究方向: 数论.

其中

$$\alpha=\frac{1}{\sqrt{2}}(1+\sqrt{3}),\beta=\frac{1}{\sqrt{2}}(1-\sqrt{3}). \tag{1.5}$$

本文根据 Diophantine 方程的性质和若干已知结果, 运用初等方法, 完整地确定了方程 (1.1) 适合 $m>1$ 的所有解, 即证明了

定理 除了 (1.2) 和 (1.3) 以外, 方程 (1.1) 适合 $m>1$ 的解仅有

$$(D,p,x,m,n)=(U_{2k+1}V_{2k+1},\ 2V_{2k+1}^2-1,\ 3V_{2k+1}^4-3V_{2k+1}^2+1,\ 2,\ 1),\quad k\in\mathbb{N}. \tag{1.6}$$

2 若干引理

为了证明定理, 首先需要证明下面的几个引理. 为此, 设 $X>1,\ r>1$ 均是正整数, q 是奇素数.

引理 2.1 如果 X^r-1 是素数, 则 $X=2$ 且 r 是素数.

证 参见文献 [5] 的定理 1.10.1.

引理 2.2 如果 X^r+1 是素数, 则 X 是偶数且 $r=2^s$, 其中 s 是正整数.

证 参见文献 [5] 的定理 1.10.2.

引理 2.3 设 $X>1,\ r>1$ 均是正整数, q 是奇素数, 则

(i)

$$\gcd(X+1,\frac{X^q+1}{X+1})=\begin{cases}q, \text{如果 } X+1\equiv 0 \pmod q,\\ 1, \text{否则}.\end{cases}$$

(ii) 当 $X+1\equiv 0 \pmod q$ 时, $q\parallel (X^q+1)/(X+1)$, 且 $(X^q+1)/q(X+1)$ 的素因数 p 满足 $p\equiv 1 \pmod{2q}$; 当 $X+1\not\equiv 0 \pmod q$ 时, $(X^q+1)/(X+1)$ 的素因数 p 满足 $p\equiv 1 \pmod{2q}$.

证 参见文献 [6].

引理 2.4 当 U_{2t+1},V_{2t+1} 适合 (1.4) 和 (1.5) 式时, $(U,V)=(U_{2t+1},\ V_{2t+1})$ $(t=0,1,\cdots)$ 是方程

$$U^2-3V^2=-2,\quad U,V\in\mathbb{N} \tag{2.1}$$

的全部解.

证 因为 $(U,V)=(1,1)$ 是方程 (2.1) 的最小解, 所以从文献 [7] 第 5.3 节直接可得本引理.

引理 2.5 方程组

$$X^2-2Y^2=-1,\ Z^2-3Y^2=-2,\quad X,Y,Z\in\mathbb{N} \tag{2.2}$$

仅有解 $(X,Y,Z)=(1,1,1)$.

证 参见文献 [4] 的引理 6.

引理 2.6 方程

$$X^4-3Y^4=-2,\quad X,Y,\in\mathbb{N} \tag{2.3}$$

仅有解 $(X,Y)=(1,1)$.

证 参见文献 [7] 第 6.2 节.

引理 2.7 方程

$$2X^2-1=Y^r,\quad X,Y,r\in\mathbb{N},\ X>1,Y>1,r>2 \tag{2.4}$$

仅有解 $(X,Y,r)=(78,23,3)$.

证 参见文献 [8] 的定理 8.1.

引理 2.8 方程

$$2^r+1=3X^s,\quad X,r,s\in\mathbb{N},\ \min(X,r,s)>1 \tag{2.5}$$

无解 (X,r,s).

证 参见文献 [9].

引理 2.9 方程

$$X^r-Y^s=1,\quad X,Y,r,s\in\mathbb{N},\ \min(X,Y,r,s)>1 \tag{2.6}$$

仅有解 $(X,Y,r,s)=(3,2,2,3)$.

证 参见文献 [10].

引理 2.10 对于奇素数 p, 方程

$$X^r+1=3p^s,\quad X,r,s\in\mathbb{N},\ r>1 \tag{2.7}$$

仅有解 $(p,X,r,s)=(3,2,3,1)$ 和 $(\frac{1}{3}(2^q+1),2,q,1)$, 其中 q 是大于 3 的奇素数.

证 设 (p,X,r,s) 是方程 (2.7) 的一组解. 此时显然 $X>1$. 因为当 r 是偶数时, $3\nmid X^r+1$, 所以 r 必为奇数; 又因 $r>1$, 所以 r 必为奇素数 q.

根据引理 2.9 可知, 方程 (2.7) 仅有解 $(p,X,r,s)=(3,2,3,1)$ 适合 $p=3$. 当 $p\neq 3$ 时, 因为从方程 (2.7) 可知 $3\mid X^r+1$ 且 $3^2\nmid X^r+1$, 所以 $q>3$. 设

$$d=\gcd\left(X^{r/q}+1,(X^r+1)/(X^{r/q}+1)\right).$$

根据引理 2.3, 从 (2.7) 式可知 $d=1$ 或 p 且 $q=p$.

如果 $d=1$, 则从 (2.7) 式可知

$$X^{r/q}+1=3,\quad \frac{(X^{r/q})^q+1}{X^{r/q}+1}=p^s. \tag{2.8}$$

由于从 (2.8) 式中第一个等式可得 $X=2$, 且 $r=q$, 又结合引理 2.8 和 (2.8) 式的第二个等式可得 $s=1$, 故有 $(p,X,r,s)=\left(\frac{1}{3}(2^q+1),2,q,1\right)$, 其中 q 是大于 3 的奇素数.

如果 $d=p$, 且 $q=p$, 则根据引理 2.3 的结论 (ii), 从 (2.7) 式可得 $X^{r/q}+1=3p^{s-1}\geq 3p$, 以及 $p=(X^r+1)/(X^{r/q}+1)>X^{r/q}+1>p$, 这就得出一对矛盾不等式, 故 $d=p$ 不成立. 引理证完.

引理 2.11 对于奇素数 p 和 q, 方程

$$X^q+Y^q=2p^Z,\quad X,Y,Z\in\mathbb{N},\ \gcd(X,Y)=1 \tag{2.9}$$

无解 (X,Y,Z).

证 设 (X,Y,Z) 是方程 (2.9) 的一组解. 因为 $p>1$, 所以 $(X,Y)\neq(1,1)$, 故有 $X+Y>2$. 由于 $(X^q+Y^q)/(X+Y)$ 是大于 1 的奇数, 所以从 (2.9) 式可得

$$X+Y=2p^r,\ \frac{X^q+Y^q}{X+Y}=p^s,\quad Z=r+s,\ r,s\in\mathbb{N}, \tag{2.10}$$

因为从 (2.10) 式可知 $p\mid\gcd(X+Y,\ (X^q+Y^q)/(X+Y))$, 所以 $q=p$. 然而, 由于 $q\parallel(X^q+Y^q)/(X+Y)$, 所以 (2.10) 式中的 $s=1$, 并且可得 $q=p=(X^q+Y^q)/(X+Y)>q$, 矛盾. 因此方程 (2.9) 无解. 引理证完.

引理 2.12 当 r 是大于 2 的正整数时, 方程

$$X^r+Y^r=2^tZ^r,\quad X,Y,Z\in\mathbb{N},\ XYZ>1,\ \gcd(X,Y)=1,\ t\in\mathbb{Z},\ t\geq 0 \tag{2.11}$$

无解 (X,Y,Z,t).

证 参见文献 [11].

3 定理的证明

设 (x,m,n) 是方程 (1.1) 的一组满足 $m>1$ 的解.

首先讨论 $p=2$ 时的情况. 此时 D 是大于 1 的奇数, 方程 (1.1) 可表示成

$$x^2=D^{2m}-2^nD^m+2^{2n}. \tag{3.1}$$

因为 D 是奇数, 所以从 (3.1) 式可知 x 也是奇数, 故从 $x^2\equiv D^{2m}\equiv 1\pmod 8$ 以及 $0\equiv x^2-D^{2m}\equiv -2^n(D^m-2^n)\pmod 8$ 可知 $n\geq 3$.

从 (3.1) 式可得

$$x^2-(D^m-2^{n-1})^2=(x+|D^m-2^{n-1}|)(x-|D^m-2^{n-1}|)=2^{2n-2}\cdot 3. \tag{3.2}$$

因为 $\gcd(x+|D^m-2^{n-1}|,\ x-|D^m-2^{n-1}|)=2$, 所以从 (3.2) 式可得

$$x+|D^m-2^{n-1}|=2^{2n-3}\cdot 3,\ x-|D^m-2^{n-1}|=2 \tag{3.3}$$

或

$$x+|D^m-2^{n-1}|=2^{2n-3},\ x-|D^m-2^{n-1}|=6. \tag{3.4}$$

当 (3.3) 式成立时, 在其中消去 x 可得

$$|D^m-2^{n-1}|=2^{2n-4}\cdot 3-1. \tag{3.5}$$

由于 $n\geq 3$, 所以 $2^{2n-4}\cdot 3-1>2^{2n-3}>2^{n-1}$, 故从 (3.5) 式可知 $D^m>2^{n-1}$ 以及

$$D^m=2^{2n-4}\cdot 3+2^{n-1}-1. \tag{3.6}$$

从 (3.6) 式可得

$$D^m + 1 = 2^{n-1}(2^{n-3} \cdot 3 + 1). \tag{3.7}$$

因为 $n \geq 3$, 所以从 (3.7) 式可知 m 必为奇数, 故有 $m \geq 3$. 又因 $(D^m+1)/(D+1)$ 是奇数, 所以从 (3.7) 式可得 $D + 1 \geq 2^{n-1}$, 以及 $2^{n-1} > 2^{n-3} \cdot 3 + 1 \geq (D^m+1)/(D+1) \geq (D^3+1)/(D+1) = D^2 - D + 1 > D + 1 \geq 2^{n-1}$ 这一矛盾.

当 (3.4) 式成立时, 在其中消去 x 可得

$$|D^m - 2^{n-1}| = 2^{2n-4} - 3. \tag{3.8}$$

如果 $n = 3$, 则从 (3.8) 式可得 $|D^m - 4| = 1$. 然而, 因为 $m > 1$, 这是不可能的. 如果 $n > 3$, 则因 $2^{2n-4} - 3 > 2^{n-1}$, 所以从 (3.8) 式可知 $D^m > 2^{n-1}$ 以及

$$D^m = 2^{2n-4} + 2^{n-1} - 3 = (2^{n-2} - 1)(2^{n-2} + 3). \tag{3.9}$$

由于 $\gcd(2^{n-2} - 1, 2^{n-2} + 3) = 1$, 故从 (3.9) 式可得

$$2^{n-2} - 1 = a^m,\ 2^{n-2} + 3 = b^m,\ D = ab,\ a, b \in \mathbb{N}, \tag{3.10}$$

然而因为 $m > 1$, 所以根据引理 2.9, 从 (3.10) 式中第一个等式可知 $n = 3$, 又从第二个等式可得 $b^m = 5$ 这一矛盾.

从以上分析可知, 当 $p = 2$ 时, 方程 (1.1) 没有适合 $m > 1$ 的解 (x, m, n).

其次讨论 p 是奇素数时的情况. 此时从 (1.1) 式可知

$$4x^2 - (2D^m - p^n)^2 = (2x + |2D^m - p^n|)(2x - |2D^m - p^n|) = 3p^{2n}. \tag{3.11}$$

因为 $p \nmid D$, 所以 $p \nmid x$ 且 $\gcd(2x + |2D^m - p^n|,\ 2x - |2D^m - p^n|) = 1$, 故从 (3.11) 式可得

$$2x + |2D^m - p^n| = 3p^{2n},\ 2x - |2D^m - p^n| = 1 \tag{3.12}$$

或

$$2x + |2D^m - p^n| = p^{2n},\ 2x - |2D^m - p^n| = 3,\ p \neq 3. \tag{3.13}$$

现分别按照 $(3, 12)$ 式和 (3.13) 式成立这两种情况进行讨论.

情况 I (3.12) 式成立. 从 (3.12) 式可得

$$x = \frac{1}{4}(3p^{2n} + 1) \tag{3.14}$$

和

$$|2D^m - p^n| = \frac{1}{2}(3p^{2n} - 1). \tag{3.15}$$

因为 $\frac{1}{2}(3p^{2n} - 1) > p^{2n} > p^n$, 所以从 (3.15) 式可知 $2D^m > p^n$, 以及

$$D^m = \frac{1}{4}(3p^{2n} + 2p^n - 1) = \frac{1}{4}(p^n + 1)(3p^n - 1). \tag{3.16}$$

如果 $p^n \equiv 1 \pmod 4$, 则因 $\dfrac{1}{2}(p^n+1)$ 与 $\dfrac{1}{2}(3p^n-1)$ 是互素的奇数, 故从 (3.16) 式可得

$$\frac{1}{2}(p^n+1)=a^m,\ \frac{1}{2}(3p^n-1)=b^m,\ D=ab,\ a,b\in\mathbb{N}, \tag{3.17}$$

从 (3.17) 式可得

$$a^m+b^m=2p^n \tag{3.18}$$

和

$$b^m-3a^m=-2. \tag{3.19}$$

由于 $m>1$, 根据引理 2.11, 从 (3.18) 式可知 m 没有奇素因数, 所以 $m=2^s$, 其中 s 是正整数. 同时, 因为从 (3.18) 式可知 $(a,b)\neq(1,1)$, 所以根据引理 2.6, 结合 (3.19) 式可知 $s<2$. 因此 $s=1$, 即 $m=2$. 将此代入 (3.17) 式中第一个等式, 可得

$$2a^2-1=p^n. \tag{3.20}$$

当 $n>2$ 时, 根据引理 2.7, 结合 (3.20) 式可知, 仅有 $(a,p,n)=(78,23,3)$, 然而, 此时从 (3.17) 式中第二个等式可得 $b^m=b^2=\dfrac{1}{2}(3p^n-1)=18250$, 故这是不可能的.

当 $n=2$ 时, 联合 (3.19) 式和 (3.20) 式可知, 方程组 (2.2) 有解 $(X,Y,Z)=(p,a,b)\neq(1,1,1)$. 然而, 根据引理 2.5 可知这是不可能的.

当 $n=1$ 时, 根据引理 2.4, 联合 (3.14), (3.19) 和 (3.20) 式可得形如 (1.6) 式的解.

如果 $p^n\equiv 3 \pmod 8$, 则因 $\dfrac{1}{4}(p^n+1)$ 是与 $3p^n-1$ 互素的奇数, 后者是偶数, 所以从 (3.16) 式可得

$$\frac{1}{4}(p^n+1)=a^m,\ 3p^n-1=2^mb^m,\ D=2ab,\ a,b\in\mathbb{N}, \tag{3.21}$$

因为 $m>1$, 所以根据引理 2.10, 从 (3.21) 式中第二个等式可得

$$b=1,\ m=3,\ p=3,\ n=1 \tag{3.22}$$

或

$$b=1,\ m=q,\ p=\frac{1}{3}(2^q+1),\ n=1,\ q\text{是大于 3 的奇素数}. \tag{3.23}$$

当 (3.22) 式成立时, 联合 (3.14) 和 (3.21) 式可得解 (1.2). 当 (3.23) 式成立时, 从 (3.21) 式中第一个等式可得

$$\frac{1}{3}(2^{q-2}+1)=a^q. \tag{3.24}$$

然而, 由于 $q>3$, 故有 $1<\dfrac{1}{3}(2^{q-2}+1)<2^q$, 所以 (3.24) 式是不成立的.

如果 $p^n\equiv 7 \pmod 8$, 则因 $\dfrac{1}{4}(3p^n-1)$ 是与 p^n+1 互素的奇数, 后者是偶数, 所以从 (3.16) 式可得

$$\frac{1}{4}(3p^n-1)=a^m,\ p^n+1=2^mb^m,\ D=2ab,\ a,b\in\mathbb{N}, \tag{3.25}$$

因为 $m > 1$, 所以根据引理 2.9, 从 (3.25) 式中的第二个等式可知 $n = 1$, 以及

$$p = (2b)^m - 1. \tag{3.26}$$

再根据引理 2.1, 从 (3, 26) 式可知 $b = 1$. 将此代入 (3.25) 式中的第一个等式可得

$$3 \cdot 2^{m-2} - 1 = a^m. \tag{3.27}$$

然而, 由于 $1 < 3 \cdot 2^{m-2} - 1 < 2^m$, 所以 (3.27) 式不可能成立.

从以上分析可知: 方程 (1.1) 仅有解 (1.2) 和 (1.6), 满足 $m > 1$ 和 (3.12) 式.

情况 II (3.13) 式成立. 从 (3.13) 式可得

$$x = \frac{1}{4}(p^{2n} + 3) \tag{3.28}$$

和

$$|2D^m - p^n| = \frac{1}{2}(p^{2n} - 3). \tag{3.29}$$

因为 $\frac{1}{2}(p^{2n} - 3) \geq \frac{1}{2}(p^{2n} - p^n) \geq p^n$, 所以从 (3.29) 式可知 $2D^m > p^n$, 以及

$$D^m = \frac{1}{4}(p^{2n} + 2p^n - 3) = \frac{1}{4}(p^n - 1)(p^n + 3). \tag{3.30}$$

如果 $p^n \equiv 1 \pmod 8$, 则因 $\frac{1}{4}(p^n+3)$ 是与 p^n-1 互素的奇数, 后者是偶数, 所以从 (3.30) 式可得

$$\frac{1}{4}(p^n + 3) = a^m,\ p^n - 1 = 2^m b^m,\ D = 2ab,\ a, b \in \mathbb{N}, \tag{3.31}$$

因为 $m > 1$, 而且从 (3.13) 式可知 $p \neq 3$, 所以根据引理 2.9, 从 (3.31) 式中第二个等式可得 $n = 1$, 以及

$$p = (2b)^m + 1. \tag{3.32}$$

再根据引理 2.2, 从 (3.32) 式可知 m 必为偶数. 然而, 此时在 (3.31) 式中消去 p^n, 可得 $1 = a^m - 2^{m-2}b^m \geq a^{m/2} + 2^{m/2-1}b^{m/2} > 1$, 矛盾.

如果 $p^n \equiv 3 \pmod 4$, 则因 $\frac{1}{2}(p^n - 1)$ 与 $\frac{1}{2}(p^n + 3)$ 是互素的奇数, 所以从 (3.30) 式可得

$$\frac{1}{2}(p^n - 1) = a^m,\ \frac{1}{2}(p^n + 3) = b^m,\ D = ab,\ a, b \in \mathbb{N}, \tag{3.33}$$

然而, 因为 $m > 1$, 又从 (3.33) 式可知 $b > a \geq 1$, 所以在 (3.33) 式中消去 p^n, 可得

$$2 = b^m - a^m \geq b^{m-1} + ab^{m-2} + \cdots + a^{m-1} \geq b + a > 2,$$

矛盾.

如果 $p^n \equiv 5 \pmod 8$, 则因 $\frac{1}{4}(p^n-1)$ 是与 p^n+3 互素的奇数, 后者是偶数, 所以从 (3.30) 式可得

$$\frac{1}{4}(p^n - 1) = a^m,\ p^n + 3 = 2^m b^m,\ D = 2ab,\ a, b \in \mathbb{N}, \tag{3.34}$$

在 (3.34) 式中消去 p^n, 可得

$$a^m + 1 = 2^{m-2}b^m. \tag{3.35}$$

显然, 从 (3.35) 式可知 m 必为奇数. 又因 $m > 1$, 所以根据引理 2.12, 从 (3.35) 式可知, 仅有 $m = 3$ 以及 $a = b = 1$. 将此代入 (3.28) 和 (3.34) 式即得解 (1.3). 由此可知, 方程 (1.1) 仅有解 (1.3) 满足 $m > 1$ 以及 (3.13) 式.

综合以上所有, 定理证完.

参 考 文 献

[1] 陈景润. 关于 Jeśmanowicz 猜想 [J]. 四川大学学报 (自然科学版), 1962, (2): 19–25.
[2] 乐茂华, 胡永忠. 广义 Lebesgue-Ramanujan-Nagell 方程研究的新进展 [J]. 数学进展, 2012, 41(4): 385–396.
[3] 佟瑞洲. 关于丢番图方程 $P^{2z} - P^zD^m + D^{2m} = X^2(I)$ [J]. 沈阳农业大学学报 (自然科学版), 2004, 35(3): 283–285.
[4] 佟瑞洲. 一个丢番图方程的求解 [J]. 沈阳师范大学学报 (自然科学版), 2005, 23(2): 133–136.
[5] 华罗庚. 数论导引 [M]. 北京: 科学出版社, 1979.
[6] Birkhoff G D, Vandivier H S. On the integral divisors of $a^n - b^n$ [J]. Ann. Math., 1904, 5(2): 173–180.
[7] 曹珍富. 丢番图方程引论 [M]. 哈尔滨: 哈尔滨工业大学出版社, 1989.
[8] Bennett M A, Skinner C M. Ternary Diophantine equations via Galois representations and modular forms[J]. Canad. J. Math., 2004, 56(1): 23–54.
[9] Bugeaud Y, Mignotte M. On the Diophantine equation $(x^n - 1)/(x - 1) = y^q$ with nagative x [A]. Bennet M A. Number theory for the millennium I[C]. MA: Peters A. K., 2002: 145–151.
[10] Mihăilescu P. Primary cyclotomic units and a proof of Catalan's conjecture [J]. J. Reine Angew. Math., 2004, 572: 167–195.
[11] Darmon M, Merel L. Winding quotients and some variants of Fermat's last theorem [J]. J. Reine Angew. Math., 1997, 490: 81–100.

ON THE EXPONENTIAL DIOPHANTINE EQUATION $x^2 = D^{2m} - D^mp^n + p^{2n}$

HE Yan-feng

(*College of Mathematics and Computer Science, Yan'an University, Yan'an 716000, China*)

Abstract: Let D be a positive integer with $D > 1$, and p be a prime with $p \nmid D$. In this paper, we study the positive integer solutions of the Diophantine equation $x^2 = D^{2m} - D^mp^n + p^{2n}$ with $m > 1$. By using properties and several known results of Diophantine equations with some elementary methods, all positive integer solutions (D, P, x, m, n) of the equations $x^2 = D^{2m} - D^mp^n + p^{2n}$ are determined, which corrects and completely solves the presumption in [4].

Keywords: exponential Diophantine equation; positive integer solution; elementary method

2010 MR Subject Classification: 11D61