Publ. Math. Debrecen
63/1-2 (2003), 67–78

On the diophantine equation $x^2 + p^2 = y^n$

By MAOHUA LE (Zhanjiang and Shanghai)

Abstract. Let p be an odd prime. In this paper we give some formulas for all positive integer solutions (x, y, n) of the title equation with $n > 2$. Moreover, we completely determine all solutions of the title equation for $p < 100$.

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$ be the sets of all integers and positive integers respectively. Let p be a prime. The solutions (x, y, n) of the equation

$$x^2 + p^2 = y^n, \quad x, y, n \in \mathbb{N}, \quad \gcd(x, y) = 1, \quad n > 2 \tag{1}$$

have been investigated in many papers. In this respect, NAGELL [8] proved that if $p = 2$, then (1) has only the solution $(x, y, n) = (11, 5, 3)$. LJUNGGREN [4] proved that if p is an odd prime satisfying $p^2 - 1 = 2^{2r+1}s$, where r, s are positive integers with $2 \nmid s$, then (1) has only finitely many solutions (x, y, n). LJUNGGREN's result in [4] is incomplete as he himself points out in [5]. For instance, the case $p = 5$ remained and remains unsolved.

In this paper we give some formulas for all solutions (x, y, z) of (1).

Mathematics Subject Classification: 11D61.
Key words and phrases: exponential diophantine equation.
Supported by the National Natural Science Foundation of China (No. 10271104), the Guangdong Provincial Natural Science Foundation (No. 011781) and the Natural Science Foundation of Education Department of Guangdong Province (No. 0161).

We now introduce some notations. For any positive integers m and s, let

$$f(m) = \sum_{i=0}^{[m/2]} \binom{m}{2i} 2^{m-2i} 3^i,$$

$$\bar{f}(m) = \sum_{i=0}^{[(m-1)/2]} \binom{m}{2i+1} 2^{m-2i-1} 3^i, \tag{2}$$

$$g(m) = \sum_{i=0}^{[m/2]} \binom{m}{2i} 2^i,$$

$$\bar{g}(m) = \sum_{i=0}^{[(m-1)/2]} \binom{m}{2i+1} 2^i, \tag{3}$$

$$h(m,s) = \sum_{i=0}^{[m/2]} (-1)^i \binom{m}{2i} (2s)^{m-2i},$$

$$\bar{h}(m,s) = \sum_{i=0}^{[(m-1)/2]} (-1)^i \binom{m}{2i+1} (2s)^{m-2i-1}. \tag{4}$$

We prove a general result as follows.

Theorem. *Let p be an odd prime. If (x, y, n) is a solution of (1), then it satisfies one of the following conditions:*

(I) $p = f(2^r), (x, y, n) = (8\bar{f}(2^r)^3 + 3\bar{f}(2^r), f(2^r)^2 + \bar{f}(2^r)^2, 3)$, *where r is a positive integer.*

(II) $p = g(q), (x, y, n) = ((g(q)^2 - 1)/2, \bar{g}(q), 4)$, *where q is an odd prime.*

(III) $p = 239, (x, y, z) = (28560, 13, 8)$.

(IV) $p = |\bar{h}(q, s)|, (x, y, n) = (|h(q, s)|, 4s^2 + 1, q)$, *where q is an odd prime, s is a positive integer.*

Using the above theorem, we can completely determine all solutions of (1) for some small p.

Corollary. *If p is an odd prime with $p < 100$, then (1) has only the following solutions:*

(i) $p = 7, (x, y, n) = (24, 5, 4), (524, 65, 3)$.

(ii) $p = 11, (x, y, n) = (2, 5, 3)$.

(iii) $p = 29, (x, y, n) = (278, 5, 7)$.

(iv) $p = 41, (x, y, n) = (38, 5, 5), (840, 29, 4)$.

(v) $p = 47, (x, y, n) = (52, 17, 3)$.

(vi) $p = 97, (x, y, n) = (1405096, 12545, 3)$.

As an interesting example, we see from the above corollary that if $p = 5$, then (1) has no solutions (x, y, n).

2. Preliminaries

Lemma 1 ([7, pp. 120–122])**.** *Let n be an odd integer with $n > 1$. Every solution (X, Y, Z) of the equation*

$$X^2 + Y^2 = Z^n, \quad X, Y, Z \in \mathbb{N}, \quad \gcd(X, Y) = 1, \tag{5}$$

can be expressed as

$$Z = X_1^2 + Y_1^2, X + Y\sqrt{-1} = \left(\lambda_1 X_1 + \lambda_2 Y_1 \sqrt{-1}\right)^n, \quad \lambda_1, \lambda_2 \in \{-1, 1\},$$

where X_1, Y_1 are coprime positive integers.

Lemma 2 ([3])**.** *The equation*

$$X^2 - 2Y^4 = -1, \quad X, Y \in \mathbb{N} \tag{6}$$

has only the solutions $(X, Y) = (1, 1)$ and $(239, 13)$.

Lemma 3 ([2])**.** *The equation*

$$4X^4 - 5Y^2 = -1, \quad X, Y \in \mathbb{N} \tag{7}$$

has only the solution $(X, Y) = (1, 1)$.

Lemma 4 ([9])**.** *The equation*

$$1 + X^2 = 2Y^n, \ X, Y, n \in \mathbb{N}, \ X > 1, \ Y > 1, \ n > 2, \ 2 \nmid n \tag{8}$$

has no solutions (X, Y, n).

Lemma 5. *Let m, s be positive integers, and let $\bar{h}(m,s)$ be defined as in* (4). *If*

$$2s \geq \operatorname{ctg}\frac{\pi}{m+1}, \tag{9}$$

then

$$\bar{h}(m,s) \geq (4s^2+1)^{(m-1)/2}. \tag{10}$$

Proof. Let

$$\alpha = 2s + \sqrt{-1}, \quad \beta = 2s - \sqrt{-1}. \tag{11}$$

Then there exist a real number θ such that

$$\alpha = \sqrt{t}e^{\theta\sqrt{-1}}, \quad \beta = \sqrt{t}e^{-\theta\sqrt{-1}}, \quad t = 4s^2+1, \tag{12}$$

$$\operatorname{tg}\theta = \frac{1}{2s}, \quad 0 < \theta < \frac{\pi}{2}. \tag{13}$$

By (4), (11) and (12), we get

$$\bar{h}(m,s) = \frac{\alpha^m - \beta^m}{\alpha - \beta} = t^{(m-1)/2}\frac{\sin(m\theta)}{\sin\theta}. \tag{14}$$

If (9) holds, then from (13) we obtain

$$\operatorname{tg}\theta = \frac{1}{2s} \leq \operatorname{tg}\frac{\pi}{m+1}. \tag{15}$$

Since $0 < \theta < \pi/2$ and $0 < \pi/(m+1) \leq \pi/2$, we see from (15) that $\theta \leq \pi/(m+1)$, whence we get

$$m\theta \leq \pi - \theta. \tag{16}$$

Since $0 < \theta < m\theta$ and $\sin(\pi - \theta) = \sin\theta$, we get from (16) that $\sin(m\theta) \geq \sin\theta$. Thus, by (14), we obtain (10). The lemma is proved. □

Let α, β be algebraic integers. If $\alpha+\beta$ and $\alpha\beta$ are nonzero coprime integers and α/β is not a root of unity, then (α,β) is called a Lucas pair. Further, let $a = \alpha+\beta$ and $c = \alpha\beta$. Then we have

$$\alpha = \frac{1}{2}\left(a + \lambda\sqrt{b}\right), \quad \beta = \frac{1}{2}\left(a - \lambda\sqrt{b}\right), \quad \lambda \in \{-1, 1\}, \tag{17}$$

where $b = a^2 - 4c$. Such pair (a,b) is called the parameters of Lucas pair (α,β). Two Lucas pairs (α_1,β_1) and (α_2,β_2) are equivalent if $\alpha_1/\alpha_2 =$

$\beta_1/\beta_2 = \pm 1$. Given a Lucas pair (α,β), one defines the corresponding sequence of Lucas numbers by

$$u_m = u_m(\alpha,\beta) = \frac{\alpha^m-\beta^m}{\alpha-\beta}, \quad m=0,1,2,\cdots. \tag{18}$$

For equivalent Lucas pairs (α_1,β_1) and (α_2,β_2), we have $u_m(\alpha_1,\beta_1) = \pm u_m(\alpha_2,\beta_2)$ for any $m \geq 0$.

Lemma 6. *If $m>1, 2\nmid m, a=2s$ and $b=-4$, where s is a positive integer, then $u_m(\alpha,\beta)\neq\pm 1$.*

Proof. If $u_m(\alpha,\beta)=\pm1$, then from (17) and (18) we get

$$4s^2\sum_{i=0}^{(m-3)/2}(-1)^i\binom{m}{2i+1}(4s^2)^{(m-3)/2-i}+(-1)^{(m-1)/2}=\pm1. \tag{19}$$

Clearly, the right side of (19) must be $(-1)^{(m-1)/2}$. Since

$$\binom{m}{k}=\binom{m}{m-k}, \quad k=0,1,\ldots,m,$$

we get from (19) that

$$\binom{m}{2}=4s^2\sum_{j=2}^{(m-1)/2}(-1)^j\binom{m}{2j}(4s^2)^{j-2}. \tag{20}$$

It implies that $m\equiv 1 \pmod 8$. Let $2^u \| m-1$ and $2^{v_j}\| j$ for $j=2,\ldots,(m-1)/2$. Since

$$v_j \leq \frac{\log j}{\log 2} \leq j-1, \quad j=2,\ldots,\frac{m-1}{2}, \tag{21}$$

we obtain

$$\begin{aligned}\binom{m}{2j}(4s^2)^{j-1} &= m(m-1)\binom{m-2}{2j-2}\frac{(4s^2)^{j-1}}{2j(2j-1)}\\ &\equiv 0 \pmod{2^{u+j-2}}, \quad j=2,\ldots,\frac{m-1}{2}.\end{aligned} \tag{22}$$

We see from (22) that the right side of (20) is a multiple of 2^u. However, since

$$2^{u-1} \,\Big\|\, \binom{m}{2},$$

(20) is impossible. Thus, the lemma is proved. □

For any positive integer m with $m > 1$, a prime p is a primitive divisor of $u_m(\alpha, \beta)$ if $p \mid u_m$ and $p \nmid bu_1 \cdots u_{m-1}$. A Lucas pair (α, β) such that $u_m(\alpha, \beta)$ has no primitive divisors will be called m-defective Lucas pair.

Lemma 7 ([10]). *Let m satisfy $4 < m \leq 30$ and $m \neq 6$. Then, up to equivalence, all parameters of m-defective Lucas pairs are given as follows:*

(i) $m = 5,\ (a, b) = (1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76), (12, -1364)$.

(ii) $m = 7,\ (a, b) = (1, -7), (1, -19)$.

(iii) $m = 8,\ (a, b) = (2, -24), (1, -7)$.

(iv) $m = 10,\ (a, b) = (2, -8), (5, -3), (5, -47)$.

(v) $m = 12,\ (a, b) = (1, 5), (1, -7), (1, -11), (2, -56), (1, -15), (1, -19)$.

(vi) $m \in \{13, 18, 30\},\ (a, b) = (1, -7)$.

Lemma 8 ([1, Theorem 1.4]). *If $m > 30$, then no Lucas pair is m-defective.*

Lemma 9 ([6]). *If p is an odd primitive divisor of $u_m(\alpha, \beta)$, then $p \equiv (b/p) \pmod{m}$, where (b/p) is the Legendre symbol.*

3. Proof of Theorem

Let (x, y, n) be a solution of (1). Since p is an odd prime, we get $2 \mid x$ and $2 \nmid y$. If $2 \mid n$, then from (1) we get $y^{n/2} + x = p^2$ and $y^{n/2} - x = 1$. It implies that

$$x = \frac{1}{2}(p^2 - 1) \tag{23}$$

and

$$1 + p^2 = 2y^{n/2}. \tag{24}$$

Since $n > 2$, by Lemma 4, (24) is false if $n/2$ has an odd prime divisor. So we have $n = 2^t$, where t is a positive integer with $t > 1$. Further, by Lemma 2, we see from (24) that either $t = 2$ or $t = 3$. When $t = 2$, we find from (24) that $(u, v) = (p, y)$ is a positive integer solution of the Pell equation

$$u^2 - 2v^2 = -1, \quad u, v \in \mathbb{Z}. \tag{25}$$

Notice that $1 + \sqrt{2}$ is the fundamental solution of (25) and p is an odd prime. We get

$$p + y\sqrt{2} = \left(1 + \sqrt{2}\right)^q, \tag{26}$$

where q is an odd prime. Thus, by (3), (23), (24) and (26), the solution (x, y, n) satisfies the condition (II). When $t = 3$, by Lemma 2, the solution (x, y, n) satisfies the condition (III).

By Lemma 1, if $2 \nmid n$, then from (1) we get

$$x + p\sqrt{-1} = \left(\lambda_1 X_1 + \lambda_2 Y_1 \sqrt{-1}\right)^n, \quad \lambda_1, \lambda_2 \in \{-1, 1\}, \tag{27}$$

where X_1, Y_1 are positive integers satisfying

$$X_1^2 + Y_1^2 = y, \quad \gcd(X_1, Y_1) = 1. \tag{28}$$

From (27), we obtain

$$x = X_1 \Big| \sum_{i=0}^{(n-1)/2} (-1)^i \binom{n}{2i} X_1^{n-2i-1} Y_1^{2i} \Big| \tag{29}$$

and

$$p = Y_1 \Big| \sum_{i=0}^{(n-1)/2} (-1)^i \binom{n}{2i+1} X_1^{n-2i-1} Y_1^{2i} \Big|. \tag{30}$$

We see from (30) that either $Y_1 = 1$ or $Y_1 = p$. Since $2 \nmid y$, we get from (28) that $2 \mid X_1$. So we have

$$X_1 = 2s, \quad s \in \mathbb{N}. \tag{31}$$

If $n = 3$ and $Y_1 = p$, then from (30) and (31) we get

$$p^2 - 3(2s)^2 = 1. \tag{32}$$

It implies that $(u', v') = (p, 2s)$ is a positive integer solution of the Pell equation

$$u'^2 - 3v'^2 = 1, \quad u', v' \in \mathbb{Z}. \tag{33}$$

Notice that $2+\sqrt{3}$ is the fundamental solution of (33) and p is an odd prime. We get

$$p+2s\sqrt{3}=\left(2+\sqrt{3}\right)^{2^r}, \quad r\in\mathbb{N}. \tag{34}$$

Thus, by (2), (28), (29) and (34), the solution (x,y,n) satisfies the condition (I).

If $n=5$ and $Y_1=p$, then we have

$$5X_1^4-10X_1^2p^2+p^4=5(X_1^2-p^2)^2-4p^4=1. \tag{35}$$

It implies that $(X,Y)=(p,|X_1^2-p^2|)$ is a solution of (7). Therefore, by Lemma 3, (35) is impossible.

If $n>5$ and $Y_1=p$, let

$$\alpha_1=2s+p\sqrt{-1}, \quad \beta_1=2s-p\sqrt{-1}. \tag{36}$$

Then (α_1,β_1) is a Lucas pair. Further, let

$$u_m(\alpha_1,\beta_1)=\frac{\alpha_1^m-\beta_1^m}{\alpha_1-\beta_1}, \quad m\geq 0 \tag{37}$$

be the corresponding sequence of Lucas numbers. By (30), (31), (36) and (37), we get $u_n(\alpha_1,\beta_1)=\pm 1$. It implies that $u_n(\alpha_1,\beta_1)$ has no primitive divisors. But, by Lemmas 7 and 8, it is impossible.

If $Y_1=1$ and n is an odd prime, by (4), (28), (29) and (30), then the solution (x,y,n) satisfies the condition (IV).

If $Y_1=1$ and n is not a prime, let q be the least prime divisor of n. Then we have $n=qt$, where t is an odd integer with $t\geq q$. Let

$$\alpha_2=2s+\sqrt{-1}, \qquad \beta_2=2s-\sqrt{-1}, \tag{38}$$

$$\alpha_3=\left(2s+\sqrt{-1}\right)^q, \qquad \beta_3=\left(2s-\sqrt{-1}\right)^q. \tag{39}$$

Then both (α_2,β_2) and (α_3,β_3) are Lucas pairs. Further, let

$$u_m(\alpha_j,\beta_j)=\frac{\alpha_j^m-\beta_j^m}{\alpha_j-\beta_j}, \quad m\geq 0,\ j=2,3 \tag{40}$$

be the corresponding sequences of Lucas numbers, respectively. By (38), (39) and (40), we get

$$\alpha_3=k+l\sqrt{-1}, \quad \beta_3=k-l\sqrt{-1}, \tag{41}$$

where k, l are integers satisfying

$$k = \frac{1}{2}(\alpha_3 + \beta_3) = \frac{1}{2}(\alpha_2^q + \beta_2^q) \equiv 0 \pmod{2} s, \tag{42}$$

$$l = \frac{\alpha_3 - \beta_3}{2\sqrt{-1}} = \frac{\alpha_2^q - \beta_2^q}{2\sqrt{-1}} = \frac{\alpha_2^q - \beta_2^q}{\alpha_2 - \beta_2} = u_q(\alpha_2, \beta_2). \tag{43}$$

Since $Y_1 = 1$, we see from (30), (38), (39) and (40) that

$$p = \left| \frac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2} \right| = \left| \frac{\alpha_2^q - \beta_2^q}{\alpha_2 - \beta_2} \cdot \frac{\alpha_3^t - \beta_3^t}{\alpha_3 - \beta_3} \right| = |u_q(\alpha_2, \beta_2)|\,|u_t(\alpha_3, \beta_3)|. \tag{44}$$

By (44), we get either

$$|u_q(\alpha_2, \beta_2)| = 1 \tag{45}$$

or

$$|u_q(\alpha_2, \beta_2)| = p. \tag{46}$$

By Lemma 6, we find from (38) that (45) is impossible. If (46) holds, then from (44) we get

$$|u_t(\alpha_3, \beta_3)| = \pm 1. \tag{47}$$

Further, by Lemmas 7 and 8, we see from (41), (42) and (43) that if (47) holds, then $t \le 5$. By the same argument as in the proof of the case $n = 5$ and $Y_1 = p$, we can prove that (47) is impossible for $t = 5$. So we have $t = 3$. Since $t \ge q$, we get $q = 3$ and $n = 9$. Then, by (38), (40), (43) and (46), we obtain

$$\begin{aligned} p = l = |u_3(\alpha_2, \beta_2)| &= |\alpha_2^2 + \alpha_2\beta_2 + \beta_2^2| \\ &= |(\alpha_2 + \beta_2)^2 - \alpha_2\beta_2| = |(4s)^2 - (4s^2 + 1)| = 12s^2 - 1. \end{aligned} \tag{48}$$

Similarly, by (39)–(41), (47) and (48), we get

$$\begin{aligned} |u_3(\alpha_3, \beta_3)| &= |\alpha_3^2 + \alpha_3\beta_3 + \beta_3^2| = |(\alpha_3 + \beta_3)^2 - \alpha_3\beta_3| \\ &= |(2k)^2 - (k^2 + p^2)| = |3k^2 - p^2| = 1. \end{aligned}$$

This implies that

$$p^2 - 3k^2 = 1. \tag{49}$$

Since $2s \mid k$ by (42), we get $k = 2sk_1$, where k_1 is an integer. Substitute (48) into (49), we get $12s^2 = k_1^2 + 2$, a contradiction. Thus, (1) has no other solutions (x, y, n). The theorem is proved.

4. Proof of Corollary

Let p be an odd prime with $p < 100$. By Theorem, if (x, y, n) is a solution of (1), then it satisfies one of conditions (I), (II) and (IV).

If (x, y, n) satisfies the condition (I), then from (34) we obtain $n = 3$ and

$$100 > p = \frac{1}{2}\left(\left(2+\sqrt{3}\right)^{2^r} + \left(2-\sqrt{3}\right)^{2^r}\right) > \frac{1}{2}\left(2+\sqrt{3}\right)^{2^r}, \quad r \in \mathbb{N}, \tag{50}$$

whence we get $r \leq 2$ and

$$(p, x, y) = \begin{cases} (7, 528, 65), & \text{if } r = 1, \\ (97, 1405096, 12545), & \text{if } r = 2. \end{cases} \tag{51}$$

If (x, y, n) satisfies the condition (II), then from (26) we obtain $n = 4$ and

$$100 > p = \frac{1}{2}\left(\left(1+\sqrt{2}\right)^{q} + \left(1-\sqrt{2}\right)^{q}\right), \tag{52}$$

where q is an odd prime. Therefore, by (52), we get $q \leq 5$ and

$$(p, x, y) = \begin{cases} (7, 24, 5), & \text{if } q = 3, \\ (41, 840, 29), & \text{if } q = 5. \end{cases} \tag{53}$$

If (x, y, n) satisfies the condition (IV), then

$$p = \left|\bar{h}(q, s)\right| = \left|u_q(\alpha_1, \beta_1)\right|, \tag{54}$$

where q is an odd prime, α_1, β_1 and $u_q(\alpha_1, \beta_1)$ are defined as in (36) and (37), respectively. Since q is a prime, we see from (54) that p is a primitive prime divisor of $u_q(\alpha_1, \beta_1)$. Therefore, by Lemma 9, we get from (36) that

$$p \equiv (-1)^{(p-1)/2} \pmod{4q}. \tag{55}$$

Since $p < 100$, we see from (55) that $q \leq 17$. Further, by Lemma 5, if

$$s \geq \begin{cases} 1, & \text{if } q = 3, 5, \\ 2, & \text{if } q = 7, 11, \\ 3, & \text{if } q = 13, 17, \end{cases} \tag{56}$$

then

$$100 > p > (4s^2 + 1)^{(q-1)/2}. \tag{57}$$

By (56) and (57), we get the following solutions

$$(p, x, y, n) = \begin{cases} (11, 2, 5, 3), & \text{if } q = 3,\ s = 1, \\ (47, 52, 17, 3), & \text{if } q = 3,\ s = 2, \\ (41, 38, 5, 5), & \text{if } q = 5,\ s = 1. \end{cases} \tag{58}$$

Finally, we check the remaining cases $(q, s) = (7, 1), (11, 1), (13, 1), (17, 1), (13, 2), (17, 2)$ and get the following solution

$$(p, x, y, n) = (29, 278, 5, 7). \tag{59}$$

Thus, by (51), (53), (58) and (59), the corollary is proved.

Acknowledgement. The author would like to thank the referees for their valuable suggestions.

References

[1] Y. Bilu, G. Hanrot and P. M. Voutier (with an appendix by M. Mignotte), Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122.

[2] J. H. E. Cohn, Eight diophantine equations, *Proc. London Math. Soc.* **16** (1966), 153–166.

[3] W. Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo* **1**, no. 5 (1942), 27.

[4] W. Ljunggren, On the diophantine equation $x^2 + p^2 = y^2$, *Norske Vid. Selsk. forh. Trondhjem* **16** (1943), 8, 27–30.

[5] W. Ljunggren, On the diophantine equation $x^2 + D = y^n$, *Norske Vid. Selsk. Forh. Trondhjem* **17** (1944), 23, 93–96.

[6] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240.

[7] L. J. Mordell, Diophantine equations, *Academic Press*, *London*, 1969.

[8] T. Nagell, Verallgemeinerung eines Fermatschen Satzes, *Arch. Math.* **5** (1954), 153–159.

[9] C. Störmer, L'équation m arc $\tan(1/x) + n$ arc tan $(1/y) = k\pi/4$, *Bull. Soc. Math. France* **27** (1899), 160–170.

[10] P. M. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.* **64** (1995), 869–888.

MAOHUA LE
DEPARTMENT OF MATHEMATICS
ZHANJIANG NORMAL COLLEGE
POSTAL CODE 524048
ZHANJIANG, GUANGDONG
P.R. CHINA
AND
DEPARTMENT OF MATHEMATICS
SHANGHAI TEACHERS UNIVERSITY
POSTAL CODE 200234
SHANGHAI
P.R. CHINA

(Received July 17, 2001; revised August 15, 2002)