ACTA ARITHMETICA
146.2 (2011)

# A note on the Diophantine equation $x^2 + q^m = y^3$

by

HUI LIN ZHU (Jinan and Xiamen)

**1. Introduction.** Many special cases of the Diophantine equation

$$x^2 + q^m = y^n, \quad x, y, m, n \in \mathbb{N},\ n \geq 3, \tag{1.1}$$

where $q$ is a prime, have been studied by many authors. Cohn [11], Arif and Abu Muriefah [3], Cohn [12] and Le [17] considered (1.1) for $q = 2$ and proved $x^2 + 2^m = y^n$, $x, y, m, n \in \mathbb{N}$, $2 \nmid y$, $n > 2$, has only the solutions $(x, y, m, n) = (5, 3, 1, 3), (7, 3, 5, 4), (11, 5, 2, 3)$. Arif and Abu Muriefah [4], [5], Luca [19], Tao [21] considered (1.1) for $q = 3$ and proved $x^2 + 3^m = y^n$, $x, y, m, n \in \mathbb{N}, (x, y) = 1$, $n > 2$, has only the solutions $(x, y, m, n) = (10, 7, 5, 3), (46, 13, 4, 3)$. Abu Muriefah and Arif [2], Abu Muriefah [1] and Tao [22] solved certain special cases of (1.1) for $q = 5$. Luca [20] considered a special case of (1.1) for $q = 7$ and found that all the primitive solutions of $x^2 + 7^{2k} = y^n$, $x, y, k \in \mathbb{N}$, $n \geq 3$, are $(x, y, k, n) = (524, 65, 1, 3), (24, 5, 1, 4)$. Bugeaud, Mignotte and Siksek [10] proved that all solutions of $x^2 + 7 = y^n$, $x, y \in \mathbb{N}$, $n \geq 3$, are $(x, y, n) = (1, 2, 3), (3, 2, 4), (5, 2, 5), (11, 2, 7), (181, 2, 15)$. So there remains the case

$$x^2 + 7^{2k+1} = y^n, \quad x, y, k \in \mathbb{N},\ n \geq 3, \tag{1.2}$$

but it is difficult.

In [6], it has been proved that the equation $x^2 + q^{2k+1} = y^n$, where $q$ is an odd prime, $q \not\equiv 7 \pmod 8$, $n \geq 5$ is an odd integer and $(n, 3h) = 1$, $h$ being the class number of the field $\mathbb{Q}(\sqrt{-q})$, has exactly two families of solutions given by

$$q = 19, \quad n = 5, \quad k = 5M, \quad x = 22434 \cdot 19^{5M}, \qquad y = 55 \cdot 19^{2M},$$
$$q = 341, \quad n = 5, \quad k = 5M, \quad x = 2759646 \cdot 341^{5M}, \quad y = 377 \cdot 341^{2M}.$$

2010 *Mathematics Subject Classification*: Primary 11D61; Secondary 11D41.
*Key words and phrases*: exponential Diophantine equation, quadratic field.

DOI: 10.4064/aa146-2-6

In [8], the authors consider the equation $x^2 + p^{2k} = y^n$ in integer unknowns $x, y, n, k$ satisfying $x \geq 1$, $y > 1$, $n \geq 3$ prime, $k \geq 0$ and $(x, y) = 1$ and suppose that $2 \leq p < 100$ is a prime. Then all solutions are

$$(x, y, p, n, k) \in \{(11, 5, 2, 3, 1), (46, 13, 3, 3, 2), (524, 65, 7, 3, 1), (2, 5, 11, 3, 1), (278, 5, 29, 7, 1), (38, 5, 41, 5, 1), (52, 17, 47, 3, 1), (1405096, 12545, 97, 3, 1)\}.$$

In this paper, we deal with $n = 3$ and prove the following results:

THEOREM 1.1. *The Diophantine equation*

$$x^2 + q^{2k+1} = y^3, \quad x > 0,\ y > 1,\ k > 0,\ (x, y) = 1, \tag{1.3}$$

*where $q > 3$ is an odd prime, $q \not\equiv 7 \pmod 8$, and the class number $h$ of the quadratic field $\mathbb{Q}(\sqrt{-q})$ satisfies $(h, 3) = 1$, has exactly one solution $(q, k, x, y) = (11, 1, 9324, 443)$.*

THEOREM 1.2. *Let $q > 3$ be an odd prime. The Diophantine equation*

$$x^2 + q^{2k} = y^3, \quad x > 0,\ y > 1,\ k > 0,\ (x, y) = 1, \tag{1.4}$$

*has many solutions and they all occur in the case of $k = 1$. All solutions can be parametrized as*

$$(x, y) = (8a^3 - 6a, 4a^2 + 1),$$

*when $a \in \mathbb{N}$ and $q$ is a prime of the form $12a^2 - 1$; or*

$$(x, y) = \left(\frac{8q^2 + 1}{3}\sqrt{\frac{q^2 - 1}{3}}, \frac{4q^2 - 1}{3}\right),$$

*when $r \in \mathbb{N}$, $X_1 = 2$, $X_{2^r} = 2X_{2^{r-1}}^2 - 1$, and $q$ is an odd prime of the form $X_{2^r}$.*

## 2. Preliminaries

LEMMA 2.1 ([7, Theorem 1.1]). *If $n \geq 4$ is an integer and*

$$C \in \{1, 2, 3, 5, 6, 10, 11, 13, 17\},$$

*then the equation*

$$x^n + y^n = Cz^2 \tag{2.1}$$

*has no solutions in nonzero pairwise coprime integers $(x, y, z)$ with, say, $x > y$, unless $(n, C) = (4, 17)$ or*

$$(n, C, x, y, z) \in \{(5, 2, 3, -1, \pm 11), (5, 11, 3, 2, \pm 5), (4, 2, 1, -1, \pm 1)\}.$$

LEMMA 2.2 ([7, Theorem 1.2]). *Suppose that $n \geq 7$ is prime. If*

$$(C, \alpha_0) \in \{(1, 2), (3, 2), (5, 6), (7, 4), (11, 2), (13, 2), (15, 6), (17, 6)\},$$

*then the equation*

$$x^n + 2^\alpha y^n = Cz^2 \tag{2.2}$$

*has no solutions in nonzero pairwise coprime integers* $(x, y, z)$ *with* $xy \neq 1$ *and integers* $\alpha \geq \alpha_0$*, unless, possibly,* $n \leq C$ *or* $(C, \alpha, n) = (11, 3, 13)$.

LEMMA 2.3 ([14], [18], [16]). *The Mordell equations* $Y^2 = X^3 + 27$*,* $Y^2 = X^3 - 27$ *and* $Y^2 = X^3 + 216$ *have only the trivial solutions* $(X, Y) = (-3, 0)$*,* $(X, Y) = (3, 0)$ *and* $(X, Y) = (-6, 0)$*, respectively. The Mordell equation* $Y^2 = X^3 - 216$ *has integer solutions* $(X, Y) = (6, 0), (10, 28), (33, 189)$.

LEMMA 2.4 ([9, Theorem 2]). *Let* $D_1$ *and* $D_2$ *be coprime square-free positive integers and denote by* $h$ *the class number of the quadratic field* $\mathbb{Q}(\sqrt{-D_1 D_2})$*. Let* $m \geq 0$ *and* $n \geq 5$ *be integers with* $n$ *prime and* $\gcd(n, 2h) = 1$*. The equation*

$$D_1 x^2 + 2^{2m} D_2 = y^n \quad \text{in positive integers } x > 0 \text{ and } y > 1 \text{ odd} \tag{2.3}$$

*has only the solutions* $x^2 + 19 = 55^5$ *and* $x^2 + 341 = 377^5$.

LEMMA 2.5 ([13], [15]). *Apart from* $(x, y) = (1, 0)$*, the equation*

$$x^n = Dy^2 + 1, \qquad x, y, n, D \in \mathbb{Z},\ n \geq 3,\ D \leq 100, \tag{2.4}$$

*has the solutions*

$$\begin{array}{ll} (x, y) = (5, \pm 12) & \text{if } (n, D) = (3, 31), \\ (x, y) = (2, \pm 1) & \text{if } (n, D) = (5, 31), \\ (x, y) = (7, \pm 3) & \text{if } (n, D) = (3, 38), \\ (x, y) = (13, \pm 6) & \text{if } (n, D) = (3, 61), \\ \text{none} & \text{if } (n, D) = (5, 71), \\ \text{none} & \text{if } (n, D) = (7, 71). \end{array}$$

**3. Proof of Theorem 1.1.** We consider the equation $x^2 + q^{2k+1} = y^3$, $x > 0$, $y > 1$, $k > 0$, $(x, y) = 1$, where $q > 3$ is an odd prime, $q \not\equiv 7 \pmod 8$. If $2 \nmid x$, then $2 \mid y$. By considering the equation modulo 8, we obtain $1 + q \equiv 0 \pmod 8$. This is impossible for $q \not\equiv 7 \pmod 8$. So $2 \mid x$, $2 \nmid y$.

CASE 1. If $q \equiv 1 \pmod 4$, then

$$x + q^k \sqrt{-q} = (a + b\sqrt{-q})^3, \qquad a, b \in \mathbb{Z},\ y = a^2 + qb^2. \tag{3.1}$$

Comparing the imaginary parts of the two sides in (3.1), we get

$$q^k = b(3a^2 - qb^2). \tag{3.2}$$

Hence $b \mid q^k$. If $b = \pm q^l$, where $0 \leq l < k$, then $\pm q^{k-l} = 3a^2 - q^{2l+1}$. Thus we obtain $q \mid 3a^2$, $q \mid a$, $q \mid y$, $q \mid x$. This is impossible since $(x, y) = 1$. Therefore, $b = \pm q^k$ and $\pm 1 = 3a^2 - q^{2k+1}$. We rewrite this equation as

$$q^{2k+1} + (\pm 1)^{2k+1} = 3a^2. \tag{3.3}$$

From Lemma 2.1, we know that when $2k+1 \geq 4$, the equation (3.3) has no solutions. So $2k+1=3$ and $q^3 \pm 1 = 3a^2$. Let $X=3q, Y=9a$. Then $Y^2 = X^3 \pm 27$. From Lemma 2.3, we know that (3.3) has no solutions.

CASE 2. If $q \equiv 3 \pmod 8$, then

$$x + q^k\sqrt{-q} = \left(\frac{A+B\sqrt{-q}}{2}\right)^3, \quad A, B \in \mathbb{Z},\ y = \frac{A^2+qB^2}{4},\ A \equiv B \pmod 2. \tag{3.4}$$

Comparing the imaginary parts of the two sides in (3.4), we get

$$2^3 q^k = B(3A^2 - qB^2). \tag{3.5}$$

If $2 \mid B$, then $2 \mid A$. Letting $A = 2a, B = 2b$, we obtain

$$q^k = b(3a^2 - qb^2), \qquad y = a^2 + qb^2. \tag{3.6}$$

If $b = \pm q^l$, $0 \leq l < k$, then $\pm q^{k-l} = 3a^2 - q^{2l+1}$. Thus we get $q \mid 3a^2$, $q \mid a$, $q \mid y$, $q \mid x$, contrary to $(x, y) = 1$. Therefore, $b = \pm q^k$ and $\pm 1 = 3a^2 - q^{2k+1}$. As in Case 1, the equation has no nontrivial solutions.

If $2 \nmid B$, then $2 \nmid A$. From $2^3 q^k = B(3A^2 - qB^2)$, we get $B \mid q^k$. When $B = \pm q^l$, we have $0 \leq l < k$, $\pm 2^3 q^{k-l} = 3A^2 - q^{2l+1}$ and $q \mid 3A^2$, $q \mid A$, $q \mid y$, $q \mid x$, which is impossible. So $B = \pm q^k$ and $\pm 2^3 = 3A^2 - q^{2k+1}$. We rewrite the equation as

$$q^{2k+1} \pm 2^3 = 3A^2. \tag{3.7}$$

From Lemma 2.2, we know that $2k+1 = 3$ or $2k+1 = 5$.

When $2k+1 = 3$, we get

$$q^3 \pm 2^3 = 3A^2. \tag{3.8}$$

Let $X = 3q, Y = 9A$. So $Y^2 = X^3 \pm 216$. By Lemma 2.3, the Mordell equation $Y^2 = X^3 + 216$ are no nontrivial solutions, and the integer solutions of the Mordell equation $Y^2 = X^3 - 216$ are $(X, Y) = (6, 0), (10, 28), (33, 89)$. Therefore, $X = 3q = 33, Y = 9A = 189$. Hence $q = 11$, $A = 21$, $k = 1$, $B = \pm 11$. So the equation (1.3) has the solution $(q, k, x, y) = (11, 1, 9324, 443)$.

When $2k+1 = 5$, we have

$$3A^2 \pm 8 = q^5. \tag{3.9}$$

By Lemma 2.4, we know that the equation $3A^2 + 8 = q^5$ has no solutions. Now we will prove that $3A^2 - 8 = q^5$ has no solutions either. We will study the equation $6A^2 - 16 = 2q^5$ in the real quadratic field $\mathbb{Q}(\sqrt{6})$. The class number of $\mathbb{Q}(\sqrt{6})$ is 1 and we rewrite the equation as

$$\begin{aligned}&(A\sqrt{6}+4)(A\sqrt{6}-4)\\ &\quad = (\sqrt{6}+2)(\sqrt{6}-2)(5+2\sqrt{6})^j(5-2\sqrt{6})^j(u+v\sqrt{6})^5(u-v\sqrt{6})^5,\end{aligned}$$

where $u,v\in\mathbb{Z}$, $q=u^2-6v^2$, $j\in\{0,\pm1,\pm2\}$, $\varepsilon=5+2\sqrt{6}$ is the fundamental unit of $\mathbb{Q}(\sqrt{6})$ and $2=(\sqrt{6}+2)(\sqrt{6}-2)$. So

$$A\sqrt{6}+4=(\sqrt{6}\pm2)(5+2\sqrt{6})^j(u+v\sqrt{6})^5,\quad A,u,v\in\mathbb{Z},\ j\in\{0,\pm1,\pm2\}.$$

As $\sqrt{6}+2=(\sqrt{6}-2)(5+2\sqrt{6})$, we only need to solve the equation

(3.10)
$$A\sqrt{6}+4=(\sqrt{6}+2)(5+2\sqrt{6})^j(u+v\sqrt{6})^5,\quad A,u,v\in\mathbb{Z},\ j\in\{0,\pm1,\pm2\}.$$

Comparing the rational parts in (3.10) and multiplying by 1/2 leads to some Thue equations. By taking a closer look it follows by symmetry that it suffices to consider the cases with $j\geq0$.

If $j=0$, we get the Thue equation

$$2=u^5+15u^4v+60u^3v^2+180u^2v^3+180uv^4+108v^5. \tag{3.11}$$

If $j=1$, we get the Thue equation

$$2=11u^5+135u^4v+660u^3v^2+1620u^2v^3+1980uv^4+972v^5. \tag{3.12}$$

If $j=2$, we get the Thue equation

$$2=109u^5+1335u^4v+6540u^3v^2+16020u^2v^3+19620uv^4+9612v^5. \tag{3.13}$$

We solved these three Thue equations by applying the **ThueSolve** function in MAGMA, and no solution was found.

This completes the proof of Theorem 1.1.

**4. Proof of Theorem 1.2.** We consider the equation $x^2+q^{2k}=y^3$, where $x>0$, $y>1$, $k>0$, $(x,y)=1$, and $q>3$ is an odd prime. If $2\nmid x$, then $2\,|\,y$. By considering the equation modulo 8, we obtain $1+1\equiv0 \pmod 8$, a contradiction. So $2\,|\,x$, $2\nmid y$. We factor the equation in $\mathbb{Z}[i]$ to obtain

$$(x+q^ki)(x-q^ki)=y^3. \tag{4.1}$$

Now, $x+q^ki$ and $x-q^ki$ are coprime in $\mathbb{Z}[i]$, which is a UFD. The only units of $\mathbb{Z}[i]$ are $\pm1,\pm i$, of multiplicative orders dividing 4 (hence, coprime to 3). This yields the relations

$$x+q^ki=(u+vi)^3,\qquad x-q^ki=(u-vi)^3, \tag{4.2}$$

for some integers $u,v$ and $y=u^2+v^2, x=|u^3-3uv^2|$. From (4.2), we have $q^k=v(3u^2-v^2)$. Note that $u$ and $v$ are coprime since any common prime factor would also divide both $x$ and $y$, which is impossible. If $v=\pm q^l$, $0<l<k$, then $\pm q^{k-l}=3u^2-q^{2l}$, hence $q\,|\,3u^2$. Since $q>3$, we obtain $q\,|\,u$. This is impossible as $(u,v)=1$. So the only possibilities are $v=\pm1$ or $v=\pm q^k$. This leads to the equations

$$3u^2=1\pm q^k \tag{4.3}$$

and

$$3u^2 = \pm 1 + q^{2k}. \tag{4.4}$$

The equation (4.3) is impossible if the sign is $-$, because then the right hand side is negative but the left hand side is positive. If the sign is $+$, then by Lemma 2.1, we have $k < 4$. The case $k = 2$ is impossible by considering the equation modulo 3. When $k = 3$, we have $(3q)^3 + 27 = (9u)^2$. This is a Mordell equation without solutions, by Lemma 2.2. So $k = 1$, $q = 3u^2 - 1$. Since $q > 3$ is an odd prime, we have $2 \mid u$. Letting $u = 2a$, $a \in \mathbb{N}$, we get $q = 12a^2 - 1$. Obviously, there are many such $q$ and the first seven are $11, 47, 107, 191, 431, 587, 971$. So $y = 4a^2 + 1$ and $x = 8a^3 - 6a$.

The sign of the equation (4.4) must be $-$ by considering modulo 3. We get $(q^k)^2 - 3u^2 = 1$. By Lemma 2.5, when $k \geq 2$, this equation has no solutions. Thus $k = 1$. Since the Pell equation $X^2 - 3Y^2 = 1$ has the smallest positive integer solution $(X_1, Y_1) = (2, 1)$ and all positive solutions are $X_t + Y_t\sqrt{3} = \varepsilon^t = (2+\sqrt{3})^t$, $t \in \mathbb{N}$, we only need to find all odd primes $q$ in the sequence $(X_t)_{t\geq 1}$. Suppose $p$ is an odd prime and $t = pl$, $l \in \mathbb{N}$. Then $X_t + Y_t\sqrt{3} = \varepsilon^t = \varepsilon^{pl} = (X_l + Y_l\sqrt{3})^p$ and

$$\begin{aligned} X_t = X_l\Bigg[&\binom{p}{0}X_l^{p-1} + \binom{p}{2}X_l^{p-3}(3Y_l^2) + \cdots + \binom{p}{2i}X_l^{p-1-2i}(3Y_l^2)^i + \cdots \\ &+\binom{p}{p-3}X_l^2(3Y_l^2)^{(p-3)/2} + \binom{p}{p-1}(3Y_l^2)^{(p-1)/2}\Bigg]. \end{aligned}$$

Obviously, $X_l \geq X_1 = 2$ and the expression in square brackets is $\geq 2$, so $X_t$ is not a prime. Therefore, $t$ only has the prime divisor 2, that is, an odd prime $q$ may only occur as $X_{2^r}$, $r \in \mathbb{N}$. Since

$$\begin{aligned} X_{2l} + Y_{2l}\sqrt{3} = \varepsilon^{2l} = (X_l + Y_l\sqrt{3})^2 &= (X_l^2 + 3Y_l^2) + 2X_lY_l\sqrt{3} \\ &= (2X_l^2 - 1) + 2X_lY_l\sqrt{3}, \end{aligned}$$

we know $X_{2l} = 2X_l^2 - 1$. Hence by induction, we have $X_{2^r} = 2X_{2^{r-1}}^2 - 1$, $r \in \mathbb{N}$, $X_1 = 2$ and $q = X_{2^r}$,

$$u^2 = \frac{q^2-1}{3}, \quad v^2 = q^2, \quad y = \frac{4q^2-1}{3}, \quad x = \frac{8q^2+1}{3}\sqrt{\frac{q^2-1}{3}}.$$

One can check $X_{2^r}, 1 \leq r \leq 6$, by Calculator and Mathematica:

$$\begin{aligned} X_2 = 7, \quad X_4 = 97, \quad &X_8 = 18817 = 31 \cdot 607, \quad X_{16} = 708158977, \\ &X_{32} = 1002978\ldots = 127 \cdot 7897\ldots, \\ &X_{64} = 20119\ldots = 22783 \cdot 265471 \cdot 592897\ldots. \end{aligned}$$

Therefore, the first three primes are $q = 7, 97, 708158977$.

This completes the proof of Theorem 1.2.

**Acknowledgements.** The author would like to thank the referee for his valuable suggestions. The author expresses his gratitude to Professor Jianya Liu for his help. The author thanks Professors Ákos Pintér, Alain Togbé, Florian Luca, Attila Pethő and Dr. Tünde Kovács for their help.

This research was partly supported by the Fundamental Research Funds for the Central Universities (No. 010121003).

## References

[1] F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 5^{2k} = y^n$, Demonstratio Math. 319 (2006), 285–289.

[2] F. S. Abu Muriefah and S. A. Arif, *The Diophantine equation* $x^2 + 5^{2k+1} = y^n$, Indian J. Pure Appl. Math. 30 (1999), 229–231.

[3] S. A. Arif and F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 2^k = y^n$, Int. J. Math. Math. Sci. 20 (1997), 299–304.

[4] —, —, *The Diophantine equation* $x^2 + 3^m = y^n$, ibid. 21 (1998), 610–620.

[5] —, —, *On a Diophantine equation*, Bull. Austral. Math. Soc. 57 (1998), 189–198.

[6] —, —, *On the Diophantine equation* $x^2 + q^{2k+1} = y^n$, J. Number Theory 95 (2002), 95–100.

[7] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equation via Galois representations and modular forms*, Canad. J. Math. 56 (2004), 23–54.

[8] A. Bérczes and I. Pink, *On the Diophantine equation* $x^2 + p^{2k} = y^n$, Arch. Math. (Basel) 91 (2008), 505–517.

[9] Y. Bugeaud, *On some exponential Diophantine equations*, Monatsh. Math. 132 (2001), 93–97.

[10] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compos. Math. 142 (2006), 31–62.

[11] J. H. E. Cohn, *The Diophantine equation* $x^2 + 2^k = y^n$, Arch. Math. (Basel) 59 (1992), 341–344.

[12] —, *The Diophantine equation* $x^2 + 2^k = y^n$*, II*, Int. J. Math. Math. Sci. 22 (1999), 459–462.

[13] —, *The Diophantine equation* $x^n = Dy^2 + 1$, Acta Arith. 106 (2003), 73–83.

[14] J. Gebel, A. Pethő and H. G. Zimmer, *On Mordell's equation*, Compos. Math. 110 (1998), 335–367.

[15] E. Herrmann, I. Járási and A. Pethő, *Note on J. H. E. Cohn's paper "The Diophantine equation* $x^n = Dy^2 + 1$*"*, Acta Arith. 113 (2004), 69–76.

[16] M. Lal, M. F. Jones and W. J. Blundon, *Numerical solutions of* $y^3 - x^2 = k$, Math. Comp. 20 (1996), 322–325.

[17] M. Le, *On Cohn's conjecture concerning the Diophantine equation* $x^2 + 2^m = y^n$, Arch. Math. (Basel) 78 (2002), 26–35.

[18] J. London and M. Finkelstein, *On Mordell's equation* $y^2 - k = x^3$, Bowling Green State Univ., Bowling Green, OH, 1973.

[19] F. Luca, *On a Diophantine equation*, Bull. Austral. Math. Soc. 61 (2000), 241–246.

[20] —, *On the Diophantine equation* $x^2+7^{2k} = y^n$, Fibonacci Quart. 45 (2007), 322–326.

[21] L. Tao, *On the Diophantine equation* $x^2 + 3^m = y^n$, Electron. J. Combin. Number Theory 8 (2008), 1–7.

[22] —, *On the Diophantine equation* $x^2 + 5^m = y^n$, Ramanujan J. 19 (2009), 325–338.

Hui Lin Zhu
School of Mathematics
Shandong University
250100 Jinan, P.R. China
and
School of Mathematical Sciences
Xiamen University
361005 Xiamen, P.R. China
E-mail: hlzhu@xmu.edu.cn

*Received on 29.11.2009*
*and in revised form on 21.4.2010* (6231)