A note on the Diophantine equation $x^2 + q^m = c^{2n}$

By Mou-Jie Deng

Department of Applied Mathematics, Hainan University,
No. 58 Renmin Avenue, Haikou 570228, Hainan, P. R. China

(Communicated by Shigefumi Mori, M.J.A., Jan. 13, 2015)

Abstract: Let q be an odd prime. Let $c > 1$ and t be positive integers such that $q^t + 1 = 2c^2$. Using elementary method and a result due to Ljunggren concerning the Diophantine equation $\frac{x^n-1}{x-1} = y^2$, we show that the Diophantine equation $x^2 + q^m = c^{2n}$ has the only positive integer solution $(x, m, n) = (c^2 - 1, t, 2)$. As applications of this result some new results on the Diophantine equation $x^2 + q^m = c^n$ and the Diophantine equation $x^2 + (2c-1)^m = c^n$ are obtained. In particular, we prove that Terai's conjecture is true for $c = 12, 24$. Combining this result with Terai's results we conclude that Terai's conjecture is true for $2 \le c \le 30$.

Key words: Diophantine equations; integer solution; Terai's conjecture.

1. Introduction. Let b, c be positive integers. The Diophantine equation

$$x^2 + b^m = c^n \tag{1.1}$$

has been studied by many authors. For example, when $a^2 + b^2 = c^2$ with $gcd(a, b, c) = 1$ and a an even number, N. Terai [7] conjectured that equation (1.1) has the only positive integer solution $(x, m, n) = (a, 2, 2)$. If $b = q \not\equiv 7 \pmod 8$ is an odd prime and $m \equiv 1 \pmod 2$, Arif and Muriefah [1] and H. L. Zhu [9] have solved the Diophantine equation

$$x^2 + q^m = c^n \tag{1.2}$$

for $n > 3$, $\gcd(6h(q), n) = 1$ and $n = 3$, with $n > 1$ and $n = 3$, $\gcd(h(q), n) = 1$ respectively, where $h(q)$ denotes the class number of the quadratic field $\mathrm{Q(q)}$. Let $c > 1$ and t be positive integers such that $q^t + 1 = 2c^s$ with $s = 1, 2$. In [8], N. Terai gave several results ([8], Theorem 1.2–1.4) on equation (1.2). If $c > 1$ and $b = 2c - 1$, he gave five sufficient conditions for the Diophantine equation

$$x^2 + (2c-1)^m = c^n \tag{1.3}$$

to have only the positive integer solution $(x, m, n) = (c - 1, 1, 2)$, and conjectured that equation (1.3) has no other solution. He show that his conjecture holds for $2 \le c \le 30$ apart from $c = 12, 24$. In what follows we refer to this conjecture as Terai's conjecture.

We note from loc. cit that for equation (1.2), the case where $q \not\equiv 7 \pmod 8$ was treated only in ([8], Theorem 1.3) and ([8], Proposition 2.3(v)). Moreover, in [8] results of Arif and Muriefah [1] and H. L. Zhu [9] were used to resolve some Diophantine equations of the form (1.2). But the related results in [1] and [9] have the restriction $q \not\equiv 7 \pmod 8$. Due to this fact, N. Terai remarked in [8] that it can not be proved that equations $x^2 + 23^m = 12^n$ and $x^2 + 47^m = 24^n$ have no solution in case both m and n are odd. In this paper, we consider the Diophantine equation

$$x^2 + q^m = c^{2n}, \tag{1.4}$$

and the main results we will prove are:

Theorem 1.1. *Let $c > 1$ and t be positive integers such that $q^t + 1 = 2c^2$ with q an odd prime. Then equation (1.4) has only the positive integer solution $(x, m, n) = (c^2 - 1, 1, 2)$.*

Theorem 1.2. *Let $q \equiv 7 \pmod 8$ be an odd prime. Let c be a positive integer such that $q^2 + 1 = 2c^2$ with $c \equiv 1 \pmod 8$ and $c + 1$ has a prime factor p satisfying $p \equiv 5, 7 \pmod 8$. Then equation (1.2) has only the positive integer solution $(x, m, n) = (c^2 - 1, 2, 4)$.*

Theorem 1.3. *Let q be an odd prime. Let c be a positive integer such that $q + 1 = 2c^2$ with $c \equiv 0, 1, 2 \pmod 4$ and $c + 1$ has a prime factor p satisfying $p \equiv 5, 7 \pmod 8$. Then equation (1.2) has only the positive integer solution $(x, m, n) = (c^2 - 1, 1, 4)$.*

Moreover, as Corollaries of Theorem 1.1 we also derive the following

2010 Mathematics Subject Classification. Primary 11D61.

doi: 10.3792/pjaa.91.15

Corollary 1.4 ([8], Theorem 1.3). *Let q be an odd prime. Let c be a positive integers such that $q^2+1=2c^2$ with $c\equiv 5 \pmod 8$. Then equation (1.2) has only the positive integer solution $(x,m,n)=(c^2-1,2,4)$.*

Corollary 1.5 ([8], Theorem 1.4). *Let q be an odd prime. Let c be a positive integers such that $q+1=2c^2$ with $c\equiv 3 \pmod 4$. Then equation (1.2) has only the positive integer solution $(x,m,n)=(c^2-1,1,4)$.*

Corollary 1.6. *Let q be an odd prime. Let $c>1$ be a square and let t be positive integers such that $q^t+1=2c$. Then equation (1.2) has only the positive integer solution $(x,m,n)=(c-1,t,2)$.*

Let us point out that our Theorem 1.2 covers the case that $q\equiv 7 \pmod 8$, which was not dealt with in [8]; that Theorem 1.3 covers the cases that $c\equiv 0,1,2 \pmod 4$ and $c+1$ has a prime factor p satisfying $p\equiv 5,7 \pmod 8$ which were not dealt with in [8]. Note that, in spite of the restriction on $c+1$, our Theorem 1.3 deals with much more cases than that of Theorem 1.4 in [8] (see Remark 1), and when $c\equiv 0,1,2 \pmod 4$ Theorem 1.3 covers the case that $q\equiv 7 \pmod 8$. Furthermore, comparing with ([8], Proposition 3.2,(v)), Corollary 1.6 shows that Terai's conjecture is true for more $c\equiv 0 \pmod 4$.

In the last section, we give 3 examples, which can not be treated by the methods used in [8], to illustrate that these cases can be settled by using a result due to Z. Cao [3] and Theorem 1.1.

2. Lammas. In the next two sections we need the following lemmas to prove the main results and give relevant examples and remarks. Lemma 2.1–2.2 belong to W. Ljunggren ([5], [6]) and Lemma 2.3 is a corollary of Theorem 3.2.1 of Z. Cao [3]. Because reference [3] is written in Chinese, it is not readable for many readers. For the convenience of the reader, we will give a simple proof of Lemma 2.3 by using result of [4].

Lemma 2.1. *The Diophantine equation*

$$\frac{x^n-1}{x-1}=y^2$$

has no solutions in integers x, y, n with $|x|>1$ and $n\geq 3$, except for $(n,x,y)=(4,7,\pm 20),(5,3,\pm 11)$.

Lemma 2.2. *The only positive integer solution of the Diophantine equation*

$$x^3+1=2y^2$$

are $(x,y)=(1,1),(23,78)$.

Lemma 2.3. *Let d,k be integer such that $d\equiv 2,3 \pmod 4$, $|d|$ is not a square, $\gcd(d,k)=1$ and $|k|>1$. Suppose $x,y,z\in \mathrm{Z}, z>0$ and $\gcd(x,y)=1$. If the Diophantine equation*

$$x^2-dy^2=k^z$$

has solution (x,y,z) with $2\nmid z$, then it must has a solution (x_0,y_0,z_0) such that $h(d)\equiv 0 \pmod{z_0}$, where $h(d)$ denote the class number of the quadratic field $Q(\sqrt{d})$.

Proof. Since $d\equiv 2,3 \pmod 4$, the discriminant of quadratic field $Q(\sqrt{d})$ is $4d$. Let $\hbar(4d)$ denote the class number of the binary quadratic form with discriminant $4d$. By Theorem 6.1 of [4] we have $\hbar(4d)\equiv 0 \pmod{z_0}$, thus $h(d)\equiv 0 \pmod{z_0}$ or $2h(d)\equiv 0 \pmod{z_0}$. By Theorem 6.2 of [4], $z_0 \mid z$. Since $2\nmid z$, it follows that $h(d)\equiv 0 \pmod{z_0}$. □

3. Proof of main results.

Proof of Theorem 1.1. From (1.3) we have

$$q^m=(c^n+x)(c^n-x).$$

Because q is an odd prime and $\gcd(c^n+x,c^n-x)=1$, we have

$$q^m=c^n+x, c^n-x=1,$$

hence

$$q^m+1=2c^n. \tag{3.1}$$

From $q^t+1=2c^2$ we deduce that $m\geq t$. Suppose $m<t$, then we have $n=1, 2c-1\mid 2c^2-1$ and thereby $2c-1\mid 2(2c^2-1)=(2c-1)(2c+1)-1$, which contradicts $c>1$. Thus $m\geq t$. Now we prove $t\mid m$. We need only consider the case $t>1$. Suppose $m=t\cdot 2^s r+l$ with $2\nmid r$ and $0\leq l<t$. If $s>0$, then from $q^m+1=q^l(q^{t2^s r}-1)+q^l+1$, $q^{t2^s}-1\mid q^{t2^s r}-1$ and $q^t+1\mid q^{t2^s}-1$ we have $q^t+1\mid q^l+1$, which is impossible. Hence $s=0$. Then from $q^m+1=ql(q^{tr}+1)-q^l+1$ and $q^t+1\mid q^{tr}+1$ we obtain $q^t+1\mid q^l-1$, which implies $l=0$ and thus $m=tr$. Since q^t+12c^2, (3.1) leads to

$$(2c^2-1)^r+1=2c^n. \tag{3.2}$$

If $c=3$, taking modulo 17, from (3.2) we get $1\equiv 2\cdot 3^n \pmod{17}$. Then we have

$$1=\left(\frac{1}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)^n=(-1)^n,$$

where $(\frac{\cdot}{\cdot})$ is Legendre's symbol. Hence $n\equiv 0 \pmod 2$. If $c\neq 3$, taking modulo $c+1$, (3.2) gives

$$2 \equiv 2(-1)^n \pmod{c+1}.$$

Then we have $n \equiv 0 \pmod 2$. Let $n = 2N$. If $N = 1$, then from (3.2) we have $r = 1$. Therefore we may suppose $r \geq 3$ and $N > 1$. Then equation (3.2) can be written as

$$\frac{(-2c^2+1)^r - 1}{(-2c^2+1) - 1} = (c^{N-1})^2. \tag{3.3}$$

It follows from Lemma 2.1 that equation (3.3) has no solution. This completes the proof of Theorem 1.1. □

Proof of Theorem 1.2. Since $x^2 \equiv 0 \pmod 4$, taking (1.2) modulo 4 gives $(-1)^m \equiv 1 \pmod 4$ and thus we have $m \equiv 0 \pmod 2$. Now we prove n is even. Suppose n is odd, then taking (1.2) modulo p implies that $x^2 \equiv -2 \pmod p$ since $q^2 + 1 = 2c^2$, $c \equiv -1 \pmod p$, and we thus reach a contradiction that

$$1 = \left(\frac{x^2}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Hence $n \equiv 0 \pmod 2$. Let $n = 2N$. Then equation $x^2 + q^m = c^{2N}$ has only the positive integer solution $(x, m, N) = (c^2 - 1, 2, 2)$ by Theorem 1.1. Thus equation (1.2) has only the positive integer solution $(x, m, n) = (c^2 - 1, 2, 4)$. This completes the proof of Theorem 1.2. □

Proof of Theorem 1.3. We can prove n is even in a similar way as in the proof of Theorem 1.2. Let $n = 2N$. Then equation $x^2 + q^m = c^{2N}$ has only the positive integer solution $(x, m, N) = (c^2 - 1, 1, 2)$ by Theorem 1.1. Thus equation (1.2) has only the positive integer solution $(x, m, n) = (c^2 - 1, 1, 4)$. This completes the proof of Theorem 1.3. □

Proof of Corollary 1.4. By the proof of Theorem 1.3 in [8] we know that n is even. Let $n = 2N$. Since $t = 2$, by Theorem 1.1, equation $x^2 + q^m = c^{2N}$ has only the positive integer solution $(x, m, N) = (c^2 - 1, 2, 2)$. Thus equation (1.2) has only the positive integer solution $(x, m, n) = (c^2 - 1, 2, 4)$. This completes the proof of Corollary 1.4. □

Proof of Corollary 1.5. Similar to the proof of Corollary 1.4, because $t = 1$, we deduce that equation (1.2) has only the positive integer solution $(x, m, n) = (c^2 - 1, 1, 4)$ by Theorem 1.1. □

Proof of Corollary 1.6. Since $q^t + 1 = 2d^2$, equation (1.2) can be written as

$$x^2 + q^m = d^{2n}. \tag{3.4}$$

By Theorem 1.1 equation (3.4) has the only positive integer solution $(x, m, n) = (d^2 - 1, t, 2)$. Hence equation (1.2) has only the positive integer solution $(x, m, n) = (c - 1, t, 2)$. □

Remark 1. For $2 \leq c \leq 200$, we find 44 values of c that satisfy the conditions of Theorem 1.2 or Theorem 1.3, in which there are two cases according to $t = 1$, or 2.

Case 1. $t = 1$. In this case we have $c \in \{4, 6, 13, 22, 24, 25, 28, 34, 36, 38, 41, 45, 46, 49, 52, 62, 64, 69, 73, 76, 92, 102, 108, 109, 118, 125, 126, 132, 134, 137, 140, 141, 153, 154, 157, 158, 160, 164, 172, 181, 185, 188, 196\}$.

Case 2. $t = 2$. In this case $c = 169$, and we have $239^2 + 1 = 2 \cdot 169^2$. It is clear that all the 44 cases can not be treated by Theorem 1.2–1.4 of [8]. Note that, if $t = 1$, there are 43 values of c satisfying the condition of Theorem 1.3. On the other hand, there are only 19 values of c that satisfy the condition of Theorem 1.4 of [8], that is: $c \in \{3, 7, 11, 15, 39, 43, 59, 63, 87, 91, 95, 115, 127, 143, 155, 171, 179, 183, 199\}$.

4. Examples. In this section we give three example.

Example 1. The Diophantine equation

$$x^2 + 23^m = 78^n \tag{4.1}$$

has only the positive integer solution $(x, m, n) = (78^2 - 1, 3, 4)$.

Proof. In fact, taking modulo 4 (4.1) gives $1 + (-1)^m \equiv 0 \pmod 4$, and hence m is odd. Suppose n is odd. Then (4.1) can be written as

$$x^2 - 78 \cdot y^2 = (-23)^m, \tag{4.2}$$

where $y = 78^{\frac{n-1}{2}}$. It follows from Lemma 2.3 that (4.2) must have a solution (x_0, y_0, m_0) such that $h(78) \equiv 0 \pmod{m_0}$. Hence $m_0 = 1$ since $h(78) = 2$ and m_0 is odd. But, by taking modulo 7, it follows that (4.2) has no solution when $m = m_0 = 1$. Thus n is even. Let $n = 2N$. By Theorem 1.1, equation $x^2 + 23^m = 78^{2N}$ has only the positive integer solution $(x, m, N) = (78^2 - 1, 3, 2)$. Hence equation (4.1) has only the positive integer solution $(x, m, n) = (78^2 - 1, 3, 4)$. □

Remark 2. For $t = 3$, the only pair (q, c) satisfying equation $q^3 + 1 = 2 \cdot c^2$ is $(q, c) = (23, 78)$ by Lemma 2.2. If $t > 3$, there is no pair (q, c) satisfying the equation $q^t + 1 = 2 \cdot c^2$ by a result

due to Bennett and Skinner [2]. It is quite natural to ask whether there are only finitely many pairs (q, c) satisfying the equation $q^2 + 1 = 2 \cdot c^2$? For $2 \le c \le 200$, we find only 3 pairs: $(q, c) = (7, 5), (41, 29), (239, 169)$. For $200 < c \le 10^{50}$, by a computer searching (using Maple 18) we find only four more pairs, namely: $(q, c) =$ (9369319, 6625109), (63018038201, 44560482149), (489133282872437279, 345869461223138161), (1917 5002942688032928599, 13558774610046711780701).

Example 2. The Diophantine equation

$$x^2 + 23^m = 12^n, \tag{4.3}$$

has only the positive integer solution $(x, m, n) = (11, 1, 2)$.

Proof. We first prove that m is odd. In fact, taking modulo 4, (4.3) gives $x^2 + (-1)^m \equiv 0 \pmod 4$, and hence m is odd. If n is odd, then equation (4.3) can be written as

$$x^2 - 3y^2 = (-23)^m, \tag{4.4}$$

where $y = 2^n \cdot 3^{\frac{n-1}{2}}$. If (4.4) has positive integer solution, then from Lemma 2.3 it must have a solution (x_0, y_0, m_0) such that $h(3) \equiv 0 \pmod{m_0}$, and we then obtain that $m_0 = 1$ since $h(3) = 1$. But, taking modulo 13, (4.4) gives $x^2 \equiv 2 \pmod{13}$, which is impossible. Hence n is even. Let $n = 2N$. Then equation (4.3) implies $2 \cdot 12^N = 23^m + 1$. If $N = 1$, then we get $m = 1$ and thus $x = 11$. If $N > 1$, since $2 \cdot 12^N \equiv 0 \pmod{16}$ but $23^m + 1 \equiv 8 \pmod{16}$, thus $2 \cdot 12N = 23^m + 1$ has no solution. □

Example 3. The Diophantine equation

$$x^2 + 47^m = 24^n, \tag{4.5}$$

has only the positive integer solution $(x, m, n) = (23, 1, 2)$.

Proof. As in the proof of Example 2 we deduce that m is odd. If n is odd, equation (4.5) can be written as

$$x^2 - 6y^2 = (-47)^m, \tag{4.6}$$

$y = 2^n \cdot 3^{\frac{n-1}{2}}$. If equation (4.6) has positive integer solution, then from Lemma 2.3 it must have a solution (x_0, y_0, m_0) such that $h(6) \equiv 0 \pmod{m_0}$, and we then obtain that $m_0 = 1$ since $h(6) = 1$. But, taking modulo 5, (4.6) gives $x^2 \equiv 2 \pmod 5$, which is impossible. Hence n is even. Let $n = 2N$. Then (4.5) gives $2 \cdot 24^N = 47^m + 1$. If $N = 1$, then we get $m = 1$ and thus $x = 23$. If $N > 1$, since $2 \cdot 24^N \equiv 0 \pmod{32}$ but $47^m + 1 \equiv 16 \pmod{32}$, thus $2 \cdot 24^N = 47^m + 1$ has no solution. □

Remark 3. Combining Example 2–3 with the results in [8] we conclude that Terai's conjecture is true for $2 \le c \le 30$.

Acknowledgments. The author would like to express his gratitude to the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper. The author want to sincerely thank Prof. Zhenfu Cao for his valuable suggestions. This work is supported by the Natural Science Foundation of Hainan Province (No. 113002).

References

[1] S. A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + q^{2k+1} = y^n$, J. Number Theory **95** (2002), no. 1, 95–100.

[2] M. A. Bennett and C. M. Skinner, Ternary Diophantine equations via Galois representations and modular forms, Canad. J. Math. **56** (2004), no. 1, 23–54.

[3] Z. Cao, *Diophantine equation and its applications.* (in Chinese), Shanghai Jio Tong Univ. Press, Shanghai, 2000.

[4] C. Heuberger and M. Le, On the generalized Ramanujan-Nagell equation $x^2 + D = p^z$, J. Number Theory **78** (1999), no. 2, 312–331.

[5] W. Ljunggren, Some theorems on indeterminate equations of the form $x^n - 1/x - 1 = y^q$, Norsk Mat. Tidsskr. **25** (1943), 17–20.

[6] W. Ljunggren, Eine elementare Auflösung der diophantischen Gleichung $x^3 + 1 = 2y^2$, Acta Math. Acad. Sci. Hungar. **3** (1952), 99–101.

[7] N. Terai, The Diophantine equation $x^2 + q^m = p^n$, Acta Arith. **63** (1993), no. 4, 351–358.

[8] N. Terai, A note on the Diophantine equation $x^2 + q^m = c^n$, Bull. Aust. Math. Soc. **90** (2014), no. 1, 20–27.

[9] H. L. Zhu, A note on the Diophantine equation $x^2 + q^m = y^3$, Acta Arith. **146** (2011), no. 2, 195–202.