A NOTE ON THE DIOPHANTINE EQUATION $x^2 + q^m = c^n$

NOBUHIRO TERAI

(Received 4 September 2013; accepted 3 October 2013; first published online 26 November 2013)

Abstract
Let $q$ be an odd prime such that $q^t + 1 = 2c^s$, where $c, t$ are positive integers and $s = 1, 2$. We show that the Diophantine equation $x^2 + q^m = c^n$ has only the positive integer solution $(x, m, n) = (c^s - 1, t, 2s)$ under some conditions. The proof is based on elementary methods and a result concerning the Diophantine equation $(x^n - 1)/(x - 1) = y^2$ due to Ljunggren. We also verify that when $2 \leq c \leq 30$ with $c \neq 12, 24$, the Diophantine equation $x^2 + (2c - 1)^m = c^n$ has only the positive integer solution $(x, m, n) = (c - 1, 1, 2)$.

Keywords and phrases: Diophantine equation, integer solution.

1. Introduction
In 1956, Sierpiński [S] showed that the equation $3^x + 4^y = 5^z$ has only the positive integer solution $(x, y, z) = (2, 2, 2)$. Jeśmanowicz [J] conjectured that if $a, b, c$ are Pythagorean numbers, that is, positive integers satisfying $a^2 + b^2 = c^2$, then the Diophantine equation

$$a^x + b^y = c^z$$

has only the positive integer solution $(x, y, z) = (2, 2, 2)$. As an analogue of Jeśmanowicz’s conjecture, the author [T] proposed the following conjecture.

Conjecture 1.1. If $a^2 + b^2 = c^2$ with $\gcd(a, b, c) = 1$ and $a$ even, then the Diophantine equation

$$x^2 + b^m = c^n$$

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

In [T], we proved that if $p$ and $q$ are primes such that (i) $q^2 + 1 = 2p$ and (ii) $d = 1$ or even if $q \equiv 1 \pmod{4}$, then the Diophantine equation $x^2 + q^m = p^n$ has only the positive integer solution $(x, m, n) = (p - 1, 2, 2)$, where $d$ is the order of a prime divisor of $(p)$ in the ideal class group of $\mathbb{Q}((\sqrt{-q})$. Conjecture 1.1 has been verified to be true in

© 2013 Australian Mathematical Publishing Association Inc. 0004-9727/2013 $16.00

doi:10.1017/S0004972713000981
many special cases:

- $b > 8 \cdot 10^6$, $b \equiv 5 \pmod{8}$, $c$ is a prime power (Le [Le1]);
- $b^2 + 1 = 2c$, $b \not\equiv 1 \pmod{16}$, $b$, $c$ are both odd primes (Chen and Le [CL]);
- $b \equiv 7 \pmod{8}$, either $b$ is a prime or $c$ is a prime (Le [Le2]);
- $c \equiv 5 \pmod{8}$, $b$ or $c$ is a prime power (Cao and Dong [CD]);
- $b \equiv \pm 5 \pmod{8}$, $c$ is a prime (Yuan and Wang [YW]).

Cenberci and Senay also showed that the Diophantine equation $x^2 + b^m = c^n$ has only the positive integer solution $(x, m, n) = (a, 2, 4)$ in the following two cases:

- $a^2 + b^2 = c^4$, $c \equiv 5 \pmod{8}$, $c$ is a prime power [CS1];
- $b^2 + 1 = 2c^2$, $b$, $c$ are both odd primes, $d = 1$ or even [CS2].

In this paper, using elementary methods, when $q^t + 1 = 2c^s$ with $q$ prime and $s = 1, 2$, we prove the following theorems.

**Theorem 1.2.** Let $q$ be a prime with $q \equiv 3, 5 \pmod{8}$. Let $c$ be a positive integer such that $q^t + 1 = 2c$, where $t$ is a positive integer. Then the Diophantine equation

$$x^2 + q^m = c^n$$

(1.1)

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

**Theorem 1.3.** Let $q$ be an odd prime. Let $c$ be a positive integer such that $q^2 + 1 = 2c^2$ and $c \equiv 5 \pmod{8}$. Then (1.1) has only the positive integer solution $(x, m, n) = (c^2 - 1, 2, 4)$.

**Theorem 1.4.** Let $q$ be an odd prime. Let $c$ be a positive integer such that $q + 1 = 2c^2$ and $c \equiv 3 \pmod{4}$. Then (1.1) has only the positive integer solution $(x, m, n) = (c^2 - 1, 1, 4)$.

We note that the relations on $q$ and $c$ in Theorems 1.2–1.4 yield the following identities, respectively:

- $q^t + 1 = 2c \implies (c - 1)^2 + q^t = c^2$,
- $q^2 + 1 = 2c^2 \implies (c^2 - 1)^2 + q^2 = c^4$,
- $q + 1 = 2c^2 \implies (c^2 - 1)^2 + q = c^4$.

In Section 3, combining Theorems 1.2–1.4 with Proposition 3.2, we also verify that when $2 \leq c \leq 30$ with $c \neq 12, 24$, the Diophantine equation

$$x^2 + (2c - 1)^m = c^n$$

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

**2. Proof of Theorems 1.2–1.4**

We use the following lemma to prove Theorems 1.2–1.4.
Lemma 2.1 (Ljunggren [Lj]). 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 \((n, x, y) = (4, 7, 20), (5, 3, 11)\).

2.1. Proof of Theorem 1.2. Let \((x, m, n)\) be a solution of (1.1).

In view of \(q \equiv 3, 5 \pmod{8}\) and \(q^t + 1 = 2c\), we see that \((2/q) = (c/q) = -1\), where \((*/*)\) is the Jacobi symbol. Hence \(n\) is even from (1.1). Put \(n = 2N\). Then, from (1.1),

\[
q^m = (c^N + x)(c^N - x).
\]

Since \(q\) is an odd prime and \(\gcd (c^N + x, c^N - x) = 1\),

\[
q^n = c^N + x, \quad 1 = c^N - x,
\]

so

\[
q^m + 1 = 2c^N.
\]

Our goal is to show that (2.1) has only the solution \((m, N) = (t, 1)\). Note that \(N\) is odd from (2.1), since \((2/q) = (c/q) = -1\).

Now we show that \(m \equiv 0 \pmod{t}\). It follows from \(q^t + 1 = 2c\) that \(q^t \equiv -1 \pmod{c}\), so \(q\) has order \(2t\) modulo \(c\). From (2.1), we have \(q^m \equiv -1 \pmod{c}\) and hence \(q^{2m} \equiv 1 \pmod{c}\). Thus we see that \(2m \equiv 0 \pmod{2t}\), that is, \(m \equiv 0 \pmod{t}\). Put \(m = tM\). Since \(q^t + 1 = 2c\), (2.1) can be written as

\[
(2c - 1)^M + 1 = 2c^N.
\]

Taking (2.2) modulo \(2c\) implies that \((-1)^M + 1 \equiv 0 \pmod{2c}\) and so \(M\) is odd. If \(N = 1\), then we obtain \(M = 1\) from (2.2). Thus we may suppose that \(M\) and \(N\) are odd and greater than 1. Then (2.2) leads to

\[
\frac{(-2c + 1)^M - 1}{(-2c + 1) - 1} = (c^{(N-1)/2})^2.
\]

It follows from Lemma 2.1 that the above equation has no solutions. This completes the proof of Theorem 1.2. \(\Box\)

2.2. Proof of Theorem 1.3. Let \((x, m, n)\) be a solution of (1.1).

We first show that \(m\) and \(n\) are even. Since \(q^2 + 1 = 2c^2\),

\[
(c^2 - 1)^2 + q^2 = c^4.
\]

This implies that

\[
c^2 - 1 = 2uv, \quad q = u^2 - v^2, \quad c^2 = u^2 + v^2,
\]
where \( u, v \) are positive integers such that \( \gcd(u, v) = 1 \), \( u > v \) and \( u \not\equiv v \pmod{2} \). From the third relation above,

\[
u = 2hk, \quad v = h^2 - k^2, \quad c = h^2 + k^2,
\]
or

\[
u = 2hk, \quad u = h^2 - k^2, \quad c = h^2 + k^2,
\]

where \( h, k \) are positive integers such that \( \gcd(h, k) = 1 \), \( h > k \) and \( h \not\equiv k \pmod{2} \). Then

\[
q = \pm((h^2 - k^2)^2 - (2hk)^2) = \pm(h^4 - 6h^2k^2 + k^4).
\]

Since \( c \equiv 5 \pmod{8} \),

\[
\left(\frac{c}{q}\right) = \left(\frac{q}{c}\right) = \left(\frac{h^4 - 6h^2k^2 + k^4}{h^2 + k^2}\right) = \left(\frac{8h^4}{h^2 + k^2}\right) = \left(\frac{2}{c}\right) = -1.
\]

We therefore conclude that \( m \) and \( n \) are even from (1.1).

Put \( m = 2M \) and \( n = 2N \). Then, from (1.1),

\[
q^m = (c^N + x)(c^N - x).
\]

Since \( q \) is an odd prime and \( \gcd(c^N + x, c^N - x) = 1 \),

\[
q^m = c^N + x, \quad 1 = c^N - x,
\]

so

\[
q^m + 1 = 2c^N. \tag{2.3}
\]

Our goal is to show that (2.3) has only the solution \( (m, N) = (2, 2) \). Note that \( N \) is even from (2.3), since \( (2/q) = 1 \) and \( (c/q) = -1 \). Since \( q^2 + 1 = 2c^2 \), (2.3) can be written as

\[
(2c^2 - 1)^M + 1 = 2c^N. \tag{2.4}
\]

Taking (2.4) modulo \( c \) implies that \((-1)^M + 1 \equiv 0 \pmod{c} \) and so \( M \) is odd. If \( N = 2 \), then we obtain \( M = 1 \) from (2.4). Thus we may suppose that \( M \) is odd and greater than 1, and \( N \) is even and greater than 2. Then (2.4) leads to

\[
\frac{(-2c^2 + 1)^M - 1}{(-2c^2 + 1) - 1} = (c^{(N-2)/2})^2.
\]

It follows from Lemma 2.1 that the above equation has no solution. This completes the proof of Theorem 1.3. \( \square \)
2.3. Proof of Theorem 1.4. Let \((x, m, n)\) be a solution of \((1.1)\).

We first show that \(n\) is even. Since \(q + 1 = 2c^2\) and \(c \equiv 3 \pmod{4},\)
\[
\left(\frac{c}{q}\right) = \left(\frac{q}{c}\right) = \left(\frac{2c^2 - 1}{c}\right) = \left(\frac{-1}{c}\right) = -1.
\]

We therefore conclude that \(n\) is even from \((1.1)\). Put \(n = 2N\). Then, from \((1.1)\),
\[
q^m = (c^N + x)(c^N - x).
\]
Since \(q\) is an odd prime and \(\gcd(c^N + x, c^N - x) = 1,\)
\[
q^m = c^N + x, \quad 1 = c^N - x,
\]
so
\[
q^m + 1 = 2c^N. \quad (2.5)
\]

Our goal is to show that \((2.5)\) has only the solution \((m, N) = (1, 2)\). Note that \(N\) is even from \((2.5)\), since \((2/q) = 1\) and \((c/q) = -1\). Since \(q + 1 = 2c^2\), \((2.5)\) can be written as
\[
(2c^2 - 1)^M + 1 = 2c^N
\]
with \(M = m\). In the same way as in the proof of Theorem 1.3, we see that the above equation has only the solution \((M, N) = (1, 2)\). This completes the proof of Theorem 1.4. \(\square\)

3. Conjecture on the equation \(x^2 + (2c - 1)^m = c^n\)

In connection with Conjecture 1.1 and Theorems 1.2–1.4, we propose the following conjecture.

**Conjecture 3.1.** Let \(c \geq 2\) be a positive integer. Then the Diophantine equation
\[
x^2 + (2c - 1)^m = c^n \quad (3.1)
\]
has only the positive integer solution \((x, m, n) = (c - 1, 1, 2)\).

We first show the following criteria, which are easy to handle and are useful to Conjecture 3.1.

**Proposition 3.2.** Suppose that at least one of the following conditions holds:

(i) \(2c - 1 \equiv 3 \pmod{8};\)
(ii) \(2c - 1 = 3p\), where \(p\) is a prime such that \(p \equiv 7 \pmod{8}, p \equiv 3, 5 \pmod{16}\) or \(p \equiv 3 \pmod{5};\)
(iii) \(2c - 1 = 5p\), where \(p\) is a prime such that \(p \equiv 3 \pmod{8}\) and \(5 + p \equiv 0 \pmod{32};\)
(iv) \(2c - 1 = 9p\), where \(p\) is a prime with \(p \equiv 5 \pmod{8};\)
(v) \(2c - 1 = q\) and \(c = 4^s\), where \(q\) is a prime and \(s\) is a positive integer.

Then Conjecture 3.1 is true.
**Proof.** (i) Since $2c - 1 \equiv 3 \pmod{8}$, $c \equiv 2 \pmod{4}$. If $n \geq 3$, then (3.1) leads to

$$1 + 3^n \equiv 0 \pmod{8},$$

which is impossible. We therefore obtain $n = 2$, $m = 1$ and $x = c - 1$.

(ii) Since $2c - 1 \equiv 0 \pmod{3}$, $c \equiv 2 \pmod{3}$. Taking (3.1) modulo 3 implies that $n$ is even, say $n = 2N$. From (3.1), we have the following two cases:

$$(2c - 1)^n + 1 = 2c^N \quad (3.2)$$

or

$$3^m + p^m = 2c^N. \quad (3.3)$$

We can solve (3.2) in the same way as in the proof of Theorem 1.2.

We now show that (3.3) has no solutions in each case.

- $p \equiv 7 \pmod{8}$: Then $c \equiv 3 \pmod{4}$. Hence $m$ is odd from (3.3). Thus $c = (3p + 1)/2$ is divisible by an odd prime divisor $r$ of $(3 + p)/2 \equiv 1 \pmod{4})$. This leads to a contradiction. Indeed, $r$ satisfies $3p + 1 \equiv 0 \pmod{r}$, that is, $-3^2 + 1 = -8 \equiv 0 \pmod{r}$, which is impossible.

- $p \equiv 3 \pmod{16}$: Then $c \equiv 5 \pmod{8}$. Taking (3.3) modulo 16 implies that $2 \cdot 3^m \equiv 2 \cdot 5^N \pmod{16}$ and so $3^m \equiv 5^N \pmod{8}$. Hence $m$ and $N$ are even. Taking (3.3) modulo 3 implies that $1 \equiv 2^{N+1} \pmod{3}$, which is impossible.

- $p \equiv 5 \pmod{16}$: Then $c \equiv 0 \pmod{8}$. Hence $2c^N \equiv 0 \pmod{16}$, while $3^m + p^m \equiv 2 \pmod{8}$ if $m$ is even, and $\equiv 8 \pmod{16}$ if $m$ is odd. This is a contradiction.

- $p \equiv 5 \pmod{16}$: Then $c \equiv 3 \pmod{8}$. Taking (3.3) modulo 5, since $2c - 1 = 3p$. Taking (3.3) modulo 5 implies that $2 \cdot 3^m \equiv 0 \pmod{5}$, which is impossible.

(iii) Since $2c - 1 \equiv 0 \pmod{5}$, $c \equiv 3 \pmod{5}$. Taking (3.1) modulo 5 implies that $n$ is even, say $n = 2N$. As in the proof of (ii), it suffices to show that

$$5^m + p^m = 2c^N \quad (3.4)$$

has no solutions. Since $p \equiv 3 \pmod{8}$, $c \equiv 0 \pmod{4}$. Thus $m$ is odd from (3.4). Note that $(5^m + p^m)/2 \not\equiv 0 \pmod{16}$, since $5 + p \not\equiv 0 \pmod{32}$. This implies that $N = 1$. Then $5^m + p^m = 5p + 1$, which is impossible.

(iv) Since $2c - 1 \equiv 0 \pmod{3}$, $c \equiv 2 \pmod{3}$. Taking (3.1) modulo 3 implies that $n$ is even, say $n = 2N$. As in the proof of (ii), it suffices to show that

$$9^m + p^m = 2c^N \quad (3.5)$$

has no solutions. Since $2c - 1 = 9p$ and $p \equiv 5 \pmod{8}$, $c \equiv 3 \pmod{4}$. Hence $m$ is odd from (3.5). Since $(9 + p)/2 \equiv 3 \pmod{4}$, there is an odd prime $r$ such that $(9 + p)/2 \equiv 0 \pmod{r}$ and $r \equiv 3 \pmod{4}$. This leads to a contradiction. Indeed, $r$ satisfies $9p + 1 \equiv 0 \pmod{r}$, that is, $-9^2 + 1 = -80 = -2^4 \cdot 5 \equiv 0 \pmod{r}$, which is impossible.

(v) Since $2c - 1 = q$ and $c = 4^s$, (3.1) can be reduced to solving the equation

$$q^m + 1 = 2^{m+1}.$$
We easily see that the above equation has only the solution \((m, n) = (1, 2)\) and so \(x = c - 1\). This completes the proof of Proposition 3.2.

Combining Theorems 1.2–1.4 with Proposition 3.2, we verify that when \(2 \leq c \leq 30\) with \(c \neq 12, 24\), Conjecture 3.1 is true.

**Proposition 3.3.** Let \(c\) be a positive integer with \(2 \leq c \leq 30\) and \(c \neq 12, 24\). Then Conjecture 3.1 is true.

**Proof.** Cases \(c = 3, 5, 6, 7, 10, 13, 14, 15, 19, 22, 27, 30\): Our assertions follow from Theorem 1.2.

Case \(c = 25\): Our assertion follows from Theorem 1.3.

Cases \(c = 2, 18, 26\): Our assertions follow from Proposition 3.2(i).

Cases \(c = 8, 11, 20, 29\): Our assertions follow from Proposition 3.2(ii).

Cases \(c = 28\): Our assertion follows from Proposition 3.2(iii).

Cases \(c = 23\): Our assertion follows from Proposition 3.2(iv).

Cases \(c = 4, 16\): Our assertions follow from Proposition 3.2(v).

Case \(c = 17\): Equation (3.1) becomes
\[
x^2 + 33^m = 17^n.
\]
Taking the above equation modulo 3 implies that \(n\) is even, say \(n = 2N\). As in the proof of Proposition 3.2(ii), it suffices to show that
\[
3^m + 11^m = 2 \cdot 17^N
\]
has no solutions. Note that an odd prime divisor \(r\) of \(a^{2^k} + b^{2^k}\) with \(\gcd(a, b) = 1\) satisfies \(r \equiv 1 \pmod{2^k+1}\), since \((ab^{-1})^{2^k} \equiv -1 \pmod{r}\) and \((ab^{-1})^{2^k+1} \equiv 1 \pmod{r}\). Hence \(m \neq 0 \pmod{16}\). Put \(m = 2^k s\) with \(s\) odd and \(k = 0, 1, 2, 3\). But when \(k = 0, 1, 2, 3\), the right-hand side of (3.6) is indivisible by 3 + 11 = 2 \cdot 7, 3^2 + 11^2 = 2 \cdot 5 \cdot 13, 3^4 + 11^4 = 2 \cdot 17 \cdot 433, 3^8 + 11^8 = 2 \cdot 107182721\), respectively.

Case \(c = 21\): Equation (3.1) becomes
\[
x^2 + 41^m = 21^n.
\]
If \(n\) is even, then (3.7) has only the positive integer solution \((x, m, n) = (20, 1, 2)\), in the same way as in the proof of Theorem 1.2.

When \(n\) is odd, we need the following lemma due to Zhu [Z] and Arif and Muriefah [AM].

**Lemma 3.4.** The Diophantine equation
\[
x^2 + 41^m = y^n
\]
has no positive integer solutions \(x, m, n\) with \(m\) odd and \(n\) odd and greater than 1.
For the proof of Lemma 3.4, see Zhu [Z] when $n = 3$, and Arif and Muriefah [AM] when $n > 3$. Note that the class number of the quadratic field $\mathbb{Q}(\sqrt{-41})$ is equal to eight. It follows from Lemma 3.4 that (3.7) has no solutions $x, m, n$ with $n$ odd.

This completes the proof of Proposition 3.3. □

**Remark 3.5.** In the cases $c = 12, 24$, we could not show that (3.1) has no solutions $x, m, n$ with $m, n$ odd. The difficulty is that $h(\mathbb{Q}(\sqrt{-23})) = 3, h(\mathbb{Q}(\sqrt{-47})) = 5$, and $23 \equiv 47 \equiv 7 \pmod{8}$ (that is, $c \equiv 0 \pmod{4}$), where $h(\mathbb{Q}(\sqrt{-d}))$ denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{-d})$.

**References**


NOBUHIRO TERAI, Division of Information System Design, Ashikaga Institute of Technology, 268-1 Omae, Ashikaga, Tochigi 326-8558, Japan
e-mail: terai@ashitech.ac.jp