The Diophantine Equation $x^2 + q^m = p^n$

Selin (INAG) CENBERCI and Hasan SENAY

Mathematics Teaching Program Graduate School of Natural and Applied Sciences Education Faculty Selcuk University, Konya, Turkey

Abstract. In this paper, considering the Terai’s conjecture, we put a new conjecture and with this conjecture whether the equation $x^2 + q^m = p^n$ has other positive integral solutions $(x; m; n)$ than $(p^2 - 1); 2; 4$ or not.

In this connection, with following Terai, we proved our conjecture. Finally, we give examples where $b$ and $c$ in the our conjecture are such that $b^2 + 1 = 2c^2$; $b < 20.000$ $c < 157.000$. In these cases, the conjecture certainly holds.

Mathematics Subject Classification: 11D61

Keywords: Diophantine equation, Algebraic Numbers, Terai Conjecture

Introduction

In 1956, Jesmonowicz [3] conjectured that if $a$, $b$, $c$ are pythagorean triple i.e. positive integers satisfying $a^2 + b^2 = c^2$, then the diophantine equation

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

has the only solution $(x, y, z) = (2, 2, 2)$.

In 1993, as an analogue of above conjecture, Terai [6] presented the following conjecture that 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 the only positive integral solution $(x, m, n) = (a, 2, 2)$.

---

1inag.s@hotmail.com
In his paper, he proved under the assumption that $b$ and $c$ in the above conjecture were odd primes $p,q$ which satisfy $q^2 + 1 = 2p$, he consider whether the equation

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

has other positive integral solutions $(x, m, n)$ than $(p - 1, 2, 2)$ or not.

Later some further results on Terai's conjecture we published [5], [7], [12], [13] and [14]. Under the assumption that we can give our conjecture.

**Conjecture 1.** If $a^2 + b^2 = c^4$ with $(a, b, c) = 1$, $2 | a$, and $(a, b, c^2)$ is a Pythagorean Triple then the Diophantine equation

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

has the only positive integral solution $(x, m, n) = (a, 2, 4)$.

In this paper, under the assumption that $b$ and $c$ in the above conjecture are odd primes $p,q$ which satisfy $q^2 + 1 = 2p^2$, we consider whether the equation

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

has other positive integral solutions $(x, m, n)$ than $((p^2 - 1), 2, 4)$ or not.

**Theorem 1.** Let $p$ and $q$ be primes such that

1. $q^2 + 1 = 2p^2$
2. $d = 1$ or even if $q \equiv 1$ or $3 \pmod{4}$ where $d$ is the order of prime divisor of $(p)$ in ideal class group of $Q(\sqrt{-q})$.

Then the equation

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

has the only positive integral solution $(x, m, n) = ((p^2 - 1), 2, 4)$.

For the proof of theorem we think three cases:

(a) We consider the first, the equation $x^2 + q^m = p^n$ when $n$ is even

Under this condition, we will use the following lemma and remark to prove our theorem.

**Lemma 1.** The diophantine equation

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

has no solutions in integers $x > 1$, $y \geq 1$ and odd $n \geq 3$ [2].

**Lemma 2.** The diophantine equation


The Diophantine equation $x^2 + B^m = y^n$

\[ x^2 + 1 = 2y^n \]  
\[ (2) \]

for $x > 1$, $y > 1$ and $n > 2$ has the only $(x, m, n)$ positive integral solution is $(x, y, n) = (239, 13, 4)$.

**Proposition 1.** Let $p$ and $q$ be primes with $q^2 + 1 = 2p^2$. If $n$ is even, then the equation

\[ x^2 + q^m = p^n \]

has the only positive integral solution $(x, m, n) = ((p^2 - 1), 2, 4)$.

**Proof.** If we write $n = 2k$ in the equation

\[ x^2 + q^m = p^n \]

then we have

\[ q^m = p^{2k} - x \]

\[ q^m = (p^k - x)(p^k + x) \]

Since $q$ is prime and $((p^k - x), (p^k + x)) = 1$, we have

\[ q^m = p^k + x \]

\[ 1 = p^k - x \]

so

\[ q^m + 1 = 2p^k \]  
\[ (3) \]

Now we show that $m$ is even. From $q^2 + 1 = 2p^2$, we have $q^2 \equiv -1 \pmod{p}$, so $q$ has order 4 ($\text{Mod } p$). From (3) we can say $q^m \equiv -1 \pmod{p}$. Hence $q^{2m} \equiv 1 \pmod{p}$. Thus we find that $2m \equiv 0 \pmod{4}$ i.e. $m$ is even.

If $k = 2$ or 1 , then from (3) and $q^2 + 1 = 2p^2$ we have $q^m + 1 = 2p^2 = q^2 + 1 \Rightarrow m = 2$ i.e. we can say that (3) has the only solution $(m, k) = (2, 2)$.

If odd $k \geq 2$, then it follows from lemma 1, that (3) has no solutions. And this proves the proposition 1.

**(b)** We consider the equation $x^2 + q^m = p^n$ when $m$ and $n$ are odd

We first investigate the equation when $q \equiv 1 \pmod{4}$, and then $q \equiv 3 \pmod{4}$.
Proposition 2. Let $p$ and $q$ be primes with $q \equiv 1 \pmod{4}$ and $m = 1$. Then the equation

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

has positive integral solutions $(x, n)$ if and only if $p^d - q$ is a square, where $d$ is the order of a prime divisor of $(p)$ in the ideal class group of $\mathbb{Q}(\sqrt{-q})$ [6].

We give a corollary about our conjecture, from the proof of proposition 2.

Corollary 1. Let $p$ and $q$ be primes such that

(i) $q^2 + 1 = 2p^2$

(ii) $q \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{4}$

(iii) $d = 1$ or even

where $d$ is as in proposition 2. Then the equation $x^2 + q = p^n$ has no positive integral solutions $(x, n)$.

Proof. From the proof of the proposition 2, we first show that $p^d - q$ is not a square. Now on the contrary suppose that $p^d - q$ is a square and $p^d - q = c^2$ for some $c$.

If $d = 1$, then we have,

\[
\begin{align*}
p &= c^2 + q \
p^2 &= (c^2 + q)^2 \\
p^2 &= c^4 + 2c^2q + q^2 \\
2p^2 &= 2c^4 + 4c^2q + 2q^2
\end{align*}
\]

Since $q^2 + 1 = 2p^2$, we can write

\[
\begin{align*}
2p^2 &= 2c^4 + 4c^2q + 2q^2 = q^2 + 1 \\
2c^4 + 4c^2q + q^2 &= 1
\end{align*}
\]

is impossible.

If $d = 2$, then we have

\[
p^2 = c^2 + q \Rightarrow 2c^2 + 2q = 2p^2
\]

and since $q^2 + 1 = 2p^2$, we obtain from the above equation,

\[
\begin{align*}
2c^2 + 2q &= 2p^2 = q^2 + 1 \\
2c^2 + 2q &= q^2 + 1 \\
2c^2 &= q^2 - 2q + 1 \\
2c^2 &= (q - 1)^2
\end{align*}
\]
The Diophantine equation \( x^2 + B^m = y^n \)

**Proof.** which is clearly impossible. Therefore \( p^d - q \) is not a square and \( c^2 + q = p^d \) and so \( x^2 + q = p^n \) has no positive integral solutions. The converse is clear.

And now we must think \( m \neq 1 \) is odd. And for this we give a Theorem and lemma.

**Theorem 2.** The equation

\[
x^2 + q^{2k+1} = y^n
\]

when \( q \) is an odd prime, \( q \not\equiv 7 \pmod{8} \), \( n \) is an odd integer \( \geq 5 \), \( n \) is not a multiple of 3 and \( (n,h) = 1 \), where \( h \) is the class number of the field \( \mathbb{Q}(\sqrt{-q}) \) has exactly two families of solutions by \( (q,n,k,x,y) = (19,5,0,22434,55), (341,5,0,2759646,377) \) [9].

**Lemma 3.** Let \( p \) and \( q \) be primes as in the corollary 1. Suppose that \( k \) is a fixed positive integer and \( n \geq 3 \) and odd. If the equation

\[
x^2 + q^{2k+1} = p^n
\]

has positive integral solutions \( (x, n) \), then so does the equation

\[
x^2 + q^{2k-1} = p^n
\]

[6].

**Proof.** This Lemma’s proof can do by using [6].

We investigated that when \( q \equiv 1 \pmod{4} \). Now we consider the case \( q \equiv 3 \pmod{4} \) with \( m \) and \( n \) are odd. Alter and Kubato gave under these conditions the following proposition for \( m = 1 \).

**Proposition 3.** Let \( D = 3 \pmod{4} \) be a positive square free integer \( \neq 3 \), \( p \) be an odd prime which does not divide \( D \) and \( d \) be the order of a prime ideal divisor of \( (p) \) in the class group of the quadratic field \( \mathbb{Q}(\sqrt{-q}) \). In order for the equation

\[
x^2 + D = p^n \quad x \geq 0, \, n \geq 0
\]

to have a solution in integers. It is necessary and sufficient that \( \left( \frac{-D}{p} \right) = 1 \) and that one of the following mutually exclusive conditions hold:

(i) \( 4p^d - D \) is a square and \( 3p^d - D = \pm 2 \)

(ii) \( p^d - D \) is a square

[8].

With this, we give a corollary about our conjecture for \( m = 1 \).
Corollary 2. Let $p$ and $q$ be primes such that

(i) $q^2 + 1 = 2p^2$
(ii) $q \equiv 3 \pmod{4}$ \hspace{1em} $p \equiv 1 \pmod{4}$
(iii) $d = 1$ or even

where $d$ is as in Proposition 3. Then the equation $x^2 + q = p^n$ has no positive integral solutions $(x, n)$.

Proof. We first think condition $(i)$ in proposition 3; and suppose that $4p^d - q = a^2$ for some $a$.

If $d = 1$, then we have $4p^d = a^2 + q \Rightarrow p = \frac{a^2 + q}{4}$.

$2 \left( \frac{a^2 + q}{4} \right)^2 = q^2 + 1 = 2p^2$

$\frac{a^4 + q^2 + 2a^2q}{8} = q^2 + 1$

$a^4 + q^2 + 2a^2q = 8a^2 + 8$

$a^4 - 8 = 7a^2 + 2a^2q$

which is impossible.

If $d = 2$, then we have $4p^2 - q = a^2 \Rightarrow 2p^2 = \frac{a^2 + q}{2}$

$\frac{a^2 + q}{2} = q^2 + 1 = 2p^2$

$a^2 = 2q^2 - q + 2$

which is impossible.

We suppose that in condition $(i)$, $3p^d - q = \pm 2$. If $d = 1 \Rightarrow 3p - q = \pm 2 \Rightarrow p = \frac{\pm 2 + q}{3}$

$2 \left( \frac{\pm 2 + q}{3} \right)^2 = q^2 + 1 = 2p^2$

$8 + 2q^2 \pm 8q = 9q^2 + 9$

$0 = 7q^2 \pm 8q + 1$

is impossible. And If $d = 2 \Rightarrow 3p^2 - q = \pm 2$, then we have $p^2 = \frac{\pm 2 + q}{3}$

$2 \left( \frac{\pm 2 + q}{3} \right) = q^2 + 1 = 2p^2$

$\pm 4 + 2q = 3q^2 + 1$

$-1 \pm 4 = 3q^2 - 2q$

which is impossible too. The converse is clear.
The Diophantine equation $x^2 + B^n = y^n$

In proposition 3, condition (ii)'s proof did in corollary 1.

**Lemma 4.** Let $p$ and $q$ be primes such that Corollary 2. Suppose that $r$ is a fixed positive integer and $n \geq 3$ is odd. If the equation

$$x^2 + q^{2r+1} = p^n$$

has positive integral solutions $(x, n)$, then done the equation

$$x^2 + q^{2r-1} = p^n$$

**Proof.** The equation (4) can be factored as

$$(x + q^r\sqrt{-q})(x - q^r\sqrt{-q}) = p^n$$

in the ring of integers $R_k$ of the quadratic field $\mathbb{Q}(\sqrt{-q})$. From the theory of quadratic fields that $(\frac{-q}{p}) = 1$ and $(\rho) = pp^\prime$ where $p$ and $p^\prime$ are distinct conjugate prime ideals. So we get

$$(x + q^r\sqrt{-q})(x - q^r\sqrt{-q}) = p^n p^\prime n$$

Since the factors on the left are relatively prime i.e. $((x + q^r\sqrt{-q}), (x - q^r\sqrt{-q})) = 1$. We have either $(x + q^r\sqrt{-q}) = p^n$ or $p^\prime n$. It follows that $p^n$ is a principal ideal and so $n = dt$ for some $t$, where $d$ is the order of $(\rho)$ in the class group of $R_k$. By the definition, $p^d$ is

$$p^d = \left(\frac{a + b\sqrt{-q}}{2}\right)$$

where $a$ and $b$ are integers with $b \geq 0$. Thus

$$x + q^r\sqrt{-q} = \pm \left(\frac{a + b\sqrt{-q}}{2}\right)$$

(6)

Thus we have

$$q^r = \pm b \frac{a^t - 1}{2^j j!} \left(2j + 1\right) a^t - 2j - 1 (-b^2 q)^j$$

(7)

where $p^d = \frac{a^2 + b^2 q}{4}$. 

$a \neq 0 \pmod{q}$ and $a$ is even, then $b$ is even too, since $p^d = \frac{a^2 + b^2 q}{4}$. Put $a = 2A$ and $b = 2B$ then $p^d = A^2 + B^2 q$. In this case we get from (7)
\[
q^r = \pm \frac{2B}{2^t} \sum_{j=0}^{t-1} \binom{t}{2j+1} 2A^{t-2j-1} (-q4B^2)^j
\]
\[
q^r = \pm \sum_{j=0}^{t-1} \binom{t}{2j+1} A^{t-2j-1} (-qB^2)^j
\]
\[
q^r = \pm BK
\]

If \( K = \pm 1 \), then \( B = \pm q^r \). Thus we get from (6)
\[
(x + q^r \sqrt{-q}) = \pm (A + q^r \sqrt{-q})^t
\]

**Proof.** Now we show \( t = 1 \). For this we define the sequences of rational integers \( \langle u_n \rangle \) and \( \langle v_n \rangle \) \((n \geq 1)\) by setting
\[
(A + q^r \sqrt{-q}) = u_n + v_n \sqrt{-q}
\]

The sequence \( \langle v_n \rangle \) has the following properties
\[
v_1 = q^r, \quad v_2 = 2Aq^r, \quad v_{n+2} = 2Av_{n+1} - p^d v_n \quad \text{for} \quad n \geq 1.
\]

Here we put \( V_n = v_n \cdot v_1 \). Then
\[
V_1 = 1, \quad V_2 = V = 2A = a \equiv 0 \pmod{4}, \quad V_{n+2} = VV_{n+1} - p^d V_n
\]

For this \( V_n \), we use the following result \( \blacksquare \)

**Lemma 5.** If \( n \geq 3 \) is odd, \( 2^s \| V, \ 2^k \| n - 1, \ p \equiv 2^l - 1 \pmod{2^{l+1}} \) and \( 2s - 2 \geq l \), then \( V_n \equiv 1 + 2^{k+l-1} \pmod{2^{k+l}} \). In particular \( V_n \neq \pm 1 \) for \( n \geq 1 \).

In our case, since \( V \equiv 0 \pmod{4} \) and \( p \equiv 1 \pmod{4} \), we have \( n \geq 2 \) and \( l = 1 \), so \( 2 (s - 1) \geq l \). Hence it follows from Lemma 4 that
\[
V_n \neq \pm 1 \quad \text{for} \quad n \geq 1
\]

Therefore the only \( t \) satisfying (11) is equal to 1. From \( n = dt \), we have \( n = d \) which is impossible since \( n \) is odd \( \geq 3 \) and \( d = 1 \) or even. Hence \( K \neq \pm 1 \).

If \( K \neq \pm 1 \), then \( K \equiv 0 \pmod{q} \). Since \( K \equiv ta^{-1} \pmod{q} \) and \( a \neq 0 \pmod{q} \), we have \( t \equiv 0 \pmod{q} \) say \( t = qc \). Thus by (8) we obtain
\[
(x + q^r \sqrt{-q}) = \pm (u + v \sqrt{-q})^t
\]

so
\[
q^r = \pm qv (u^{q-1} + qw)
\]

for some integers \( u, v, w \). Since \( u \neq 0 \pmod{q} \), we have \( q^r = \pm qv \), so \( v = \pm q^{r-1} \). Hence by (4) and (9) we obtain,
\[
(u^2 + q^{2r-1})^q = x^2 + q^{2r+1} = p^n = p^{dt} = p^{gcd}
\]
Proposition 4. Suppose that \( B = \frac{b}{a} \) is a rational prime divisor of \( r^2 - s^2 \). Since \( d \) satisfies the conditions of Theorem 1, we obtain \( D = \frac{d}{B} \). So we consider the case where \( r^2 - s^2 \) has no positive integral solutions \((x, m, n)\).

Corollary 3. Let \( p \) and \( q \) be primes as in corollary 1 and Corollary 2. If \( m \) is odd then the equation \( x^2 + q^m = p^n \) has no positive integral solutions \((x, m, n)\).

(c) We consider the equation \( x^2 + B^m = c^2 + C^k \) when \( m \) is even and \( n = 2k \) is even \((k \text{ odd})\).

We know from conjecture 1, \((a, b, c^2)\) is a Pythagorean Triple. If we write \( c^2 = C \), \( n = 2k \) our equation turn \( x^2 + B^m = C^k \). So we consider the equation \( x^2 + B^m = C^k \), where \( C \) is a prime square when \( B \equiv 1, 3 \pmod{4} \). We note that \( B \) can be written as a difference of two squares because we know from Dujella; since \( d = -1 \) is the only negative integer \( d \equiv 3 \pmod{4} \) which satisfies the conditions of Theorem 1 [1]. So we can use the case \( B \equiv 3 \pmod{4} \).

Proposition 4. Suppose that \( B = r^4 + s^4 - 6r^2s^2 = (r^2 - s^2)^2 - (2rs)^2 \) and \( C = c^2 = (r^2 + s^2)^2 = r^4 + 4s^2 + 2r^2s^2 \) where \( r \) and \( s \) are positive integers with \((r, s) = 1, r > s \) and one of them is odd. If \( m \) is even and \( n \) is odd, then the equation

\[
x^2 + B^m = C^n
\]

has no positive integral solutions \((x, m, n)\).

Proof. If \( m = 2k \), then we have from the equation (10)

\[
(x + B^k_i)(x - B^k_i) = (2rs - (r^2 - s^2)i)^n(2rs + (r^2 - s^2)i)^n.
\]

Since \((x + B^k_i), (x - B^k_i)\) are relatively prime and \((2rs - (r^2 - s^2)i), (2rs + (r^2 - s^2)i)\) are prime in \( \mathbb{Q}(i) \), we obtain

\[
\epsilon(x + B^k_i) = (2rs + (r^2 - s^2)i)^n
\]

where \( \epsilon = \mp 1, \mp i \).

Now we show (11) and consequently (10) are impossible for odd \( n \), let \( \pi \) be a rational prime divisor of \( B \).

Since \( B = r^4 + s^4 - 6r^2s^2 = (r^2 - s^2)^2 - (2rs)^2 = (r^2 - s^2 - 2rs)(r^2 - s^2 + 2rs) = (a - b)(a + b) \),

\[
B = a^2 - b^2,
\]

then \( \pi \mid a^2 - b^2 \Rightarrow \) either \( \pi \mid a - b \) or \( \pi \mid a + b \). This implies that \( \pi \mid r^2s^2 - 2rs \) or \( \pi \mid r^2s^2 + 2rs \). i.e.either \( r^2 - s^2 \equiv 2rs \pmod{\pi} \) or \( r^2 - s^2 \equiv -2rs \pmod{\pi} \). Assume the first possibility; the second begin similar. It follows from that (11).

\[
\epsilon x = (2rs + 2rsi)^n \pmod{\pi}
\]

\[
\epsilon x = (2rs)^n(1 + i)^n \pmod{\pi}
\]

Note that \( (1 + i)^n = (2i)^{\frac{n-1}{2}}(1 + i) \) for odd \( n \). Since \( \pi \) does not divide \( 4rs \), the right hand side of the above congruence has never be purely real or
imaginary module \( \pi \), where as the left hand side is. Thus (11) and so (10) is imposible for odd \( n \). This completes the proof of proposition 4.

**Notation 1.** Let \( p \) and \( q \) be different primes, we note that \( q^2 + 1 = 2p^2 \) implies that \( p \equiv 1 \pmod{4} \).

**Remark 1.** We investigate \( b \) and \( c \) primes such that \( b^2 + 1 = 2c^2 \), \( b \not\equiv 20,000 \) and \( c \not\equiv 157,000 \). We give the following 5 examples for \( b \) and \( c \). In these cases the conjecture certainly holds.

**Example 1.** The only positive integral solution of each of examples

\[
\begin{align*}
(a) & \quad x^2 + 7m = 5^n \\
(b) & \quad x^2 + 41m = 29^n \\
(c) & \quad x^2 + 239m = 169^n \\
(d) & \quad x^2 + 1393m = 985^n \\
(e) & \quad x^2 + 8119m = 5741^n
\end{align*}
\]

are given by \((24, 2, 4), (840, 2, 4), (28560, 2, 4), (970224, 2, 4), (32959080, 2, 4)\) respectively.

**Proof.** Cases \((a)\) and \((b)\) are covered by theorem. \((c)\) taking the equation \((\text{mod } 4)\), we see that \( m \) is even. The equation \( x^2 + 239m = 13^2n \) leads to \( 239m + 1 = 2.13^n \) from Lemma 2. We have \( m = 2 \) and \( n = 4 \). The others can do similarly. \(\blacksquare\)

In Proposition 3, we see when \( n \) is odd, then the equation \( x^2 + B^m = C^n \) has no solution. So we can give the following generalize for solutions of the equation \( x^2 + q^m = p^n \), when \( n \) is even.

**Corollary 4.** We think \( x^2 + b^m = c^n \) Diophantine equation. Let \( b = q = 3 \) or \( 1 \pmod{4} \) and \( p = c = 1 \pmod{4} \). We obtain \( x^2 + q^m = p^n \) Diophantine equation. Diophantine equation’s \((x, m, n)\) positive solutions can be generalized; \( k \) is even except for \( k = 1, n \geq 1 \) and \( n = 2k \) such that;

If \( q^2 + 1 = 2p^k \) has positive integral solutions, then \( x^2 + q^m = p^n \) equation’s the only \((x, m, n)\) solution is given by \((x, m, n) = ((p^k - 1), 2, 2k)\).

We know from Lemma 2, The diophantine equation

\[ q^2 + 1 = 2p^k \]

for \( x > 1, y > 1 \) and \( n > 2 \) has the only \((x, m, n)\) positive integral solution is \((x, m, n) = (239, 13, 4)\). So for \( k > 2 \), the diophantine equation \( x^2 + q^m = p^n \) has no positive integral solution except the equation \( x^2 + q^2 = p^8 \).

**References**


[2] C.Stormer, Solution complete en nombres entiers de l’équation \( m \arctan \frac{x}{y} + n \arctan \frac{1}{y} = k \pi \), Bull. Soc. Math. France, 27, 1899, 160-170.

The Diophantine equation $x^2 + B^m = y^n$ 


Received: February, 2009