ACTA ARITHMETICA
LXIII.4 (1993)

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

by

NOBUHIRO TERAI (Tokyo)

1. Introduction. In 1956, Sierpiński [4] showed that the equation

$$3^x + 4^y = 5^z$$

has the only positive integral solution $(x, y, z) = (2, 2, 2)$. Jeśmanowicz [2] proved that the only positive integral solution of each of the equations

$$5^x + 12^y = 13^z, \quad 7^x + 24^y = 25^z, \quad 9^x + 40^y = 41^z, \quad 11^x + 60^y = 61^z$$

is given by $(x, y, z) = (2, 2, 2)$, and conjectured that if a, b, c are Pythagorean triples, i.e. positive integers satisfying $a^2 + b^2 = c^2$, then the equation

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

has the only solution $(x, y, z) = (2, 2, 2)$ (cf. [5]).

As an analogue of his conjecture, we consider the following:

CONJECTURE. *If $a^2 + b^2 = c^2$ with $(a, b, c) = 1$ and a even, then the equation*

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

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

In this paper, under the assumption that b and c in the above conjecture are odd primes p, q which satisfy $q^2 + 1 = 2p$, we 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. Then we prove the following:

THEOREM. *Let p and q be primes such that*

(i) $q^2 + 1 = 2p$,
(ii) $d = 1$ *or even if* $q \equiv 1 \pmod 4$,

where d is the order of a prime divisor of (p) in the ideal class group of $\mathbb{Q}(\sqrt{-q})$. Then the equation

$$x^2 + q^m = p^n \tag{1}$$

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

The proof of the Theorem is divided into three cases: (a) n is even, (b) m is even and n is odd, (c) m and n are odd. In case (a), from the results of Störmer and Ljunggren, it follows that (1) has the only positive integral solution $(x, m, n)=(p - 1, 2, 2)$. In cases (b) and (c), we show that (1) has no positive integral solutions (x, m, n), by decomposing (1) in the imaginary quadratic field $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-q})$, and using the well known method which reduces the problem of a Diophantine equation of second degree to that of a linear recurrence of second order.

Finally, we give the examples where b and c in the Conjecture are such that $b^2 + 1 = 2c$, $b < 20$, $c < 200$. In these cases, the Conjecture certainly holds.

2. The equation $x^2 + q^m = p^n$ (n even). In this section we treat the equation $x^2 + q^m = p^n$ when n is even. We use the following two lemmas to prove Proposition 1.

LEMMA 1 (Störmer [6]). *The Diophantine equation*

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

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

LEMMA 2 (Ljunggren [3]). *The Diophantine equation*

$$x^2 + 1 = 2y^4$$

has the only positive integral solutions $(x, y) = (1, 1)$, $(239, 13)$.

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

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

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

Proof. Put $n = 2k$. By the equation $x^2 + q^m = p^n$, we have

$$q^m = (p^k + x)(p^k - x).$$

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

$$q^m = p^k + x, \quad 1 = p^k - x\,,$$

so

$$q^m + 1 = 2p^k\,. \tag{2}$$

Now we show that m is even. It follows from $q^2 + 1 = 2p$ that $q^2 \equiv -1 \pmod{p}$, so q has order 4 $\pmod{p}$. From (2) we have $q^m \equiv -1 \pmod{p}$, hence $q^{2m} \equiv 1 \pmod{p}$. Thus we find that $2m \equiv 0 \pmod{4}$, i.e. m is even.

If $k = 1$ or 2, then we easily see that (2) has the only solution $(m, k) = (2, 1)$ since $q^2 + 1 = 2p$. If $k \geq 3$, then it follows from Lemmas 1 and 2 that (2) has no solutions. ∎

3. The equation $x^2 + D^m = p^n$ (m even and n odd). In this section we consider the equation (1) when m is even and n is odd. More generally, we show the following:

PROPOSITION 2. *Suppose that $D = a^2 - b^2$ and $p = a^2 + b^2$, where a and b are positive integers with $(a, b) = 1$, $a > b$ and opposite parity. If m is even and n is odd, then the equation*

$$x^2 + D^m = p^n \tag{3}$$

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

Proof. Put $m = 2r$. By (3), we have

$$(x + D^r i)(x - D^r i) = (a + bi)^n (a - bi)^n .$$

Since $x + D^r i$, $x - D^r i$ are relatively prime and $a + bi$, $a - bi$ are prime in $\mathbb{Q}(i)$, we obtain

$$\varepsilon(x \pm D^r i) = (a + bi)^n , \tag{4}$$

where $\varepsilon = \pm 1, \pm i$.

Now we show that (4) is impossible for odd n. Let π be a rational prime divisor of D. Then either $a \equiv b \pmod{\pi}$ or $a \equiv -b \pmod{\pi}$. Assume the first possibility, the second being similar. It follows from (4) that

$$\varepsilon x \equiv a^n (1 + i)^n \pmod{\pi} .$$

Note that $(1 + i)^n = (2i)^{(n-1)/2}(1 + i)$ for odd n. Since π does not divide $2a$, the right hand side of the above congruence can never be purely real or imaginary modulo π, whereas the left hand side is. Thus (4) is impossible for odd n. This completes the proof of Proposition 2. ∎

4. The equation $x^2 + q^m = p^n$ (m and n odd). In this section we treat the equation (1) when m and n are odd.

We first consider (1) when $m = 1$. We show the following:

PROPOSITION 3. *Let p and q be odd primes with $q \equiv 1 \pmod{4}$. Then the equation*

$$x^2 + q = p^n \tag{5}$$

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 $\mathbb{Q}(\sqrt{-q})$.

Proof. Since $\left(\frac{-q}{p}\right) = 1$ by (5), it follows from the theory of quadratic fields that $(p) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct conjugate prime ideals in $\mathbb{Q}(\sqrt{-q})$. Therefore (5) yields the ideal equation

$$(x+\sqrt{-q})(x-\sqrt{-q}) = \mathfrak{p}^n\mathfrak{p}'^n .$$

Since the factors on the left are relatively prime, we have either $(x+\sqrt{-q}) = \mathfrak{p}^n$ or $\mathfrak{p}'^n$. We may assume that

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

Then $\mathfrak{p}^n$ is a principal ideal and so $n = dt$ for some positive integer t. By definition, $\mathfrak{p}^d$ is principal, say

$$\mathfrak{p}^d = (a+b\sqrt{-q}) . \tag{6}$$

Thus we have

$$(x+\sqrt{-q}) = \mathfrak{p}^{dt} = (a+b\sqrt{-q})^t ,$$

so

$$x+\sqrt{-q} = \pm(a+b\sqrt{-q})^t ,$$

which implies

$$1 = \pm b \sum_{j=0}^{(t-1)/2} \binom{t}{2j+1} a^{t-(2j+1)} b^{2j} (-q)^j .$$

Hence $b = \pm 1$. Then it follows from (6) that

$$\mathfrak{p}^d = (a \pm \sqrt{-q}) .$$

Taking the norm from $\mathbb{Q}(\sqrt{-q})$ to $\mathbb{Q}$ of the above equation gives $p^d = a^2+q$. Therefore $p^d - q$ is a square.

The converse is clear. This completes the proof of Proposition 3. ∎

Corollary. *Let p and q be primes such that*

(i) $q^2+1 = 2p$,
(ii) $q \equiv 1 \pmod 4$,
(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).

Remark. If $(\frac{-q}{p}) = -1$, then (p) would be inert in $\mathbb{Q}(\sqrt{-q})$, so $d = 1$. Thus we may assume $(\frac{-q}{p}) = 1$. There are altogether 10 pairs of (p, q) satisfying $q^2+1 = 2p$, $q \equiv 1 \pmod 4$ and $(\frac{-q}{p})$=1, in the range $q < 2000$. In all these cases, we verified that $d = 1$ or even. (It is conjectured that $d = 1$ or even for all such primes p, q.)

P r o o f o f C o r o l l a r y. By Proposition 3, it suffices to show that $p^d - q$ is not a square. On the contrary, suppose that $p^d - q$ were a square, say $p^d - q = a^2$ for some a.

If $d = 1$, then we have

$$2a^2 + 2q = 2p = q^2 + 1\,,$$

so

$$2a^2 = (q-1)^2\,,$$

which is impossible.

If d is even, then $a^2 + q = p^d$ has no positive integral solutions by Proposition 1. Therefore $p^d - q$ is not a square. ■

We next consider the equation (1) when m and n are odd. First we prepare the following:

LEMMA 3. *Let p and q be primes as in the Corollary. Suppose that r is a fixed positive integer. If the equation*

$$x^2 + q^{2r+1} = p^n \tag{7}$$

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

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

P r o o f. We note that if (7) has positive integral solutions (x, n), then n is odd ≥ 3 from Proposition 1 and $q^2 + 1 = 2p$. In view of the proof of Proposition 3, the equation (7) leads to

$$x + q^r\sqrt{-q} = \pm(a + b\sqrt{-q})^t\,.$$

Thus we have

$$q^r = \pm b \sum_{j=0}^{(t-1)/2} \binom{t}{2j+1} a^{t-(2j+1)} b^{2j} (-q)^j = \pm bB\,,$$

$a \not\equiv 0 \pmod q$ and a is even since $p^d = a^2 + bq^2$.

If $B = \pm 1$, then $b = \pm q^r$. Thus

$$x + q^r\sqrt{-q} = \pm(a + q^r\sqrt{-q})^t\,. \tag{8}$$

(If necessary, replace a with $-a$.) We show $t = 1$.

Now, we define the sequences of rational integers $\{u_n\}$ and $\{v_n\}$ $(n \geq 1)$ by setting

$$(a + q^r\sqrt{-q})^n = u_n + v_n\sqrt{-q}\,.$$

The sequence $\{v_n\}$ has the following properties:

$$v_1 = q^r, \quad v_2 = 2aq^r, \quad v_{n+2} = 2av_{n+1} - p^d v_n, \quad v_1 \mid v_n$$

for $n \geq 1$.

Here we put $V_n = v_n/v_1$. Then

$$V_1 = 1, \quad V_2 = V = 2a \equiv 0 \pmod 4, \quad V_{n+2} = VV_{n+1} - p^d V_n .$$

For this V_n, we use the following result ([1], Corollary, p. 15):

LEMMA 4. *If* $n \ge 3$ *is odd*, $2^s \| V$, $2^k \| n-1$, $p \equiv 2^l - 1 \pmod{2^{l+1}}$, *and* $2s-2 \ge l$, *then* $V_n \equiv 1 + 2^{k+l-1} \pmod{2^{k+l}}$. *In particular*, $V_n \ne \pm 1$ *for* $n > 1$ *if* $2(s-1) \ge l$.

In our case, since $V \equiv 0 \pmod 4$ and $p \equiv 1 \pmod 4$, we have $s \ge 2$ and $l = 1$, so $2(s-1) \ge l$. Hence it follows from Lemma 4 that

$$V_n \ne \pm 1 \quad \text{for } n > 1 .$$

Therefore the only t satisfying (8) is equal to 1. From $n = dt$, we have $n = d$, which is impossible since n is odd ≥ 3 and $d = 1$ or even. Hence $B \ne \pm 1$.

If $B \ne \pm 1$, then $B \equiv 0 \pmod q$. Since $B \equiv ta^{t-1} \pmod q$ and $a \not\equiv 0 \pmod q$, we have $t \equiv 0 \pmod q$, say $t = qc$. Thus by (8) we obtain

$$x + q^r \sqrt{-q} = \pm (u + v\sqrt{-q})^q , \tag{9}$$

so

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

for some integers u, v, w. Since $u \not\equiv 0 \pmod q$, we have $q^r = \pm qv$, so $v = \pm q^{r-1}$. Hence by (7), (9) we obtain

$$(u^2 + q^{2r-1})^q = x^2 + q^{2r+1} = p^n = p^{dqc} ,$$

which implies $u^2 + q^{2r-1} = p^{dc}$. This completes the proof of Lemma 3. ∎

PROPOSITION 4. *Let* p *and* q *be primes as in the Corollary. If* m *is odd*, *then the equation* $x^2 + q^m = p^n$ *has no positive integral solutions* (x, m, n).

Proof. The proposition follows immediately from the Corollary and Lemma 3. ∎

5. Proof of Theorem and examples. Now, using Propositions 1, 2 and 4, we can prove the Theorem.

Proof of Theorem. We note that $q^2 + 1 = 2p$ implies $p \equiv 1 \pmod 4$.

Suppose that n is even. Then by Proposition 1, (1) has the only positive integral solution $(x, m, n) = (p-1, 2, 2)$.

Suppose that n is odd. When $q \equiv 3 \pmod 4$, (1) yields $(-1)^m \equiv 1 \pmod 4$, so m is even. Then by Proposition 2, (1) has no solutions. When $q \equiv 1 \pmod 4$, by Propositions 2 and 4 the equation (1) has no solutions if $d = 1$ or even. ∎

We give the examples where b and c in the Conjecture are such that $b^2 + 1 = 2c, b < 20, c < 200$. In these cases, the Conjecture certainly holds.

Examples. *The only positive integral solution of each of the equations*

(a) $x^2 + 3^m = 5^n$, (b) $x^2 + 5^m = 13^n$, (c) $x^2 + 7^m = 25^n$,

(d) $x^2 + 9^m = 41^n$, (e) $x^2 + 11^m = 61^n$, (f) $x^2 + 13^m = 85^n$,

(g) $x^2 + 15^m = 113^n$, (h) $x^2 + 17^m = 145^n$, (i) $x^2 + 19^m = 181^n$

is given by $(x, m, n) = (4, 2, 2)$, $(12, 2, 2)$, $(24, 2, 2)$, $(40, 2, 2)$, $(60, 2, 2)$, $(84, 2, 2)$, $(112, 2, 2)$, $(144, 2, 2)$, *and* $(180, 2, 2)$, *respectively.*

Proof. Cases (a), (b), (e) and (i) are covered by the Theorem. (Note that in (b), m is even by taking the equation mod 3.)

(c) Taking the equation mod 4, we see that m is even. The equation $x^2 + 7^m = 5^{2n}$ leads to $7^m + 1 = 2 \cdot 5^n$. Hence our assertion follows from Lemmas 1 and 2.

(d) Taking the equation mod 3, we see that n is even, say $n = 2k$. Thus the equation $x^2 + 3^{2m} = 41^n$ leads to $3^{2m} + 1 = 2 \cdot 41^k$. Hence our assertion follows from Lemmas 1 and 2.

(f) By $(\frac{13}{5}) = (\frac{85}{13}) = -1$, we see that m is even and n is even. Therefore our assertion follows from Lemmas 1 and 2.

(g) Taking the equation mod 3 and 4 respectively, we see that m and n are even, say $n = 2k$. Thus we have

$$15^m + 1 = 2 \cdot 113^k ,$$

or

$$3^m + 5^m = 2 \cdot 113^k .$$

The first equation has the only solution $(m, k) = (2, 1)$ by Lemmas 1 and 2.

Taking the second equation mod 7, yields $3^m + 5^m \equiv 2 \pmod 7$. Since 3 and 5 are primitive roots mod 7 respectively and 3^m, $5^m \equiv 1, 2, 4 \pmod 7$ for even m, we see that $m \equiv 0 \pmod 6$. Hence $1 \pm 1 \equiv 2 \cdot 113^k \pmod{13}$. Since the order of 113 mod 13 is equal to 3, $k \equiv 0 \pmod 3$. Put $X = 3^{m/3}$, $Y = 5^{m/3}$ and $Z = 113^{k/3}$. Therefore we have

$$X^3 + Y^3 = 2Z^3 ,$$

which has no solutions, as is well-known.

(h) Taking the equation mod 3, we see that m is even, say $m = 2k$. If n is even, then the equation has the only solution $(x, m, n) = (144, 2, 2)$ by Lemmas 1 and 2.

Suppose that n is odd. By an argument similar to the one used in Proposition 2, we obtain

$$x^2 + 17^k i = i^r (a + bi)^n, \quad r = 0, 1, 2, 3 .$$

The factor i^r can be absorbed into the nth power, so we may assume $r = 0$. Since $a^2 + b^2 = 145$ and a is even and b is odd, $(a, b) = (8, 9)$, $(12, 1)$. Now, we define the sequences of rational integers $\{a_n\}$ and $\{b_n\}$ ($n \ge 1$) by setting

$$(a+bi)^n = a_n + b_n i\,.$$

The sequence $\{b_n\}$ has the following properties:

$$b_{m+n} = a_m b_n + a_n b_m, \qquad b_1 \mid b_n$$

for $m \ge 1$, $n \ge 1$. We show that $b_n \not\equiv 0 \pmod{17}$ for odd n.

By $b_1 \mid b_n$, we have $b_1 = b = 1$, $a = 12$. Then $b_1 \equiv 1 \pmod{17}$, $b_2 \equiv 7 \pmod{17}$, $b_3 \equiv 6 \pmod{17}$, $b_4 \equiv 13 \pmod{17}$, $b_5 \equiv 3 \pmod{17}$, $b_6 \equiv 6 \pmod{17}$, $b_7 \equiv 15 \pmod{17}$ and $b_8 \equiv 0 \pmod{17}$. Since $b_{n+8} = a_8 b_n + a_n b_8$, we have $b_{n+8} \equiv a_8 b_n \pmod{17}$. Thus by $a_8 \not\equiv 0 \pmod{17}$, we obtain

$$17 \mid b_n \Leftrightarrow 8 \mid n\,,$$

which is impossible since n is odd. Hence $b_n \not\equiv 0 \pmod{17}$ for odd n. Therefore the equation has no solutions when n is odd. ∎

Acknowledgment. The author would like to thank the referee for his valuable suggestions and Y. Sato for his generous assistance.

References

[1] R. Alter and K. K. Kubota, *The diophantine equation* $x^2 + D = p^n$, Pacific J. Math. (1) 46 (1973), 11–16.

[2] L. Jeśmanowicz, *Kilka uwag o liczbach pitagorejskich* [*Some remarks on Pythagorean numbers*], Wiadom. Mat. 1 (1956), 196–202.

[3] W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo 5 (1942), 1–27.

[4] W. Sierpiński, *O równaniu* $3^x + 4^y = 5^z$ [*On the equation* $3^x + 4^y = 5^z$], Wiadom. Mat. 1 (1956), 194–195.

[5] —, *Elementary Theory of Numbers*, PWN—Polish Scientific Publishers, Warszawa 1988.

[6] C. Störmer, *L'équation* $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$, Bull. Soc. Math. France 27 (1899), 160–170.

DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCE AND ENGINEERING
WASEDA UNIVERSITY
OKUBO, SHINJUKU, TOKYO 169, JAPAN

Received on 31.3.1992
and in revised form on 20.7.1992 (2248)