ACTA ARITHMETICA
LII (1989)

The diophantine equation $x^2+D^m=p^n$

by

MAOHUA LE (Hunan, China)

1. Introduction. Let p be an odd prime, and let D be a non-power integer with $D>1$ and $p\nmid D$. Toyoizumi [12] considered the integer solutions of the equation

$$x^2+D^m=p^n,\qquad m>0,\ n>0,\ x>0 \tag{1}$$

for some fixed D and p. In this paper, we prove the following

THEOREM. *Let a, r be positive integers. If* $\max(D,p)>M=\exp\exp\exp 1000$, *then we have:*

(i) *When $D=3a^2+1$, $p=4a^2+1$, (1) has at most three integer solutions*

$$(m,n,x)=(1,1,a),\ (1,3,8a^3+3a),\ (m_3,n_3,x_3)$$

where $2|m_3$.

(ii) *When $D=2$, $p=2^{2^r}+1$, (1) has exactly two integer solutions*

$$(m,n,x)=(2^r,1,1),\ (2^r+2,2,2^{2^r}-1). \tag{2}$$

(iii) *Excepting the above cases, (1) has at most two integer solutions. Further, if these are*

$$(m_1,n_1,x_1),\ (m_2,n_2,x_2),$$

then $m_1\not\equiv m_2 \pmod 2$.

From the Theorem, we immediately deduce the following

COROLLARY. *If $\max(D,p)>M$ and $p\equiv 3 \pmod 4$, then (1) has at most one integer solution (m,n,x).*

Clearly, these results are good upper bounds for the numbet of solutions of (1) except for a finite number of D and p.

2. Preliminaries.

LEMMA 1 (van der Poorten and Loxton [10]). *Let $\alpha_1,\ldots,\alpha_s$ be algebraic numbers, and let H_i $(i=1,\ldots,s)$ denote the height of α_i, $A_i=\max(4,H_i)$. If*

$A_1 \leqslant \ldots \leqslant A_{s-1} \leqslant A_s$ *and*

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_s \log \alpha_s \neq 0$$

for some integers $b_1, \ldots, b_s$, *then*

$$|\Lambda| > \exp\left(-2^{61s+47} s^{10s} d^{10s+10} (\log B)(\log\log A_{s-1}) \prod_{i=1}^{s} \log A_i\right),$$

where d *is the degree of the field* $Q(\alpha_1, \ldots, \alpha_s)$, $B = \max(4, |b_1|, \ldots, |b_s|)$. ∎

LEMMA 2 (Baker [1]). *Let* k *be a positive integer, and let* $f(x, y)$ *be a homogeneous irreducible polynomial of degree* $r \geqslant 3$ *and with integer coefficients. The integer solutions* (x, y) *of the equation*

$$f(x, y) = k$$

satisfy

$$\max(|x|, |y|) < \exp\left((rH)^{(10r)^5} + (\log k)^{2r+2}\right),$$

where H *is the height of* $f(x, y)$. ∎

LEMMA 3 (Cohn [6]). *The equation*

$$4x^4 - 5y^2 = \pm 1, \quad x > 0,\ y > 0$$

has the only integer solution $(x, y) = (1, 1)$. ∎

LEMMA 4 (Nagell [9]). *Let* d *be a square free positive integer. If the equation*

$$1 + dx^2 = y^n, \quad n > 0,\ x > 0,\ y > 0$$

has an integer solution (n, x, y) *with* $2 \nmid y$, *then* $n \mid h(-d)$, *where* $h(-d)$ *is the class number of the field* $Q(\sqrt{-d})$. ∎

LEMMA 5 (Le [7]). *Let* D' *be a positive integer with* $D' > 1$ *and* $p \nmid D'$. *If the equation*

$$X^2 + D' Y^2 = p^Z, \quad \gcd(X, Y) = 1,\ Z > 0 \tag{3}$$

has an integer solution (X, Y, Z), *then there exists a unique integer solution* $(X, Y, Z) = (X_1, Y_1, Z_1)$ *which satisfies* $X_1 > 0$, $Y_1 > 0$ *and* $Z_1 \leqslant Z$, *where* Z *runs over all integer solutions of* (3). *Such* (X_1, Y_1, Z_1) *is called the least solution of* (3). *Further, every integer solution* (X, Y, Z) *of* (3) *can be expressed as*

$$Z = Z_1 t,$$

$$X + Y\sqrt{-D'} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-D'})^t, \quad \lambda_1 = \pm 1,\ \lambda_2 = \pm 1,$$

where t *is a positive integer.* ∎

LEMMA 6 (Bender and Herzberg [2]). *If* $\max(D', p) > 7$, *then* (3) *has at most one integer solution* (X, Y, Z) *with* $X = 1$ *and* $Y > 0$. ∎

LEMMA 7 (Le [8]). *If* $\max(D', p) > M$, *then* (3) *has at most one integer solution* (X, Y, Z) *with* $X > 0$ *and* $Y = 1$ *except when*

$$D' = 3a^2 + 1, \quad p = 4a^2 + 1, \tag{4}$$

where a *is a positive integer; in this case* (3) *exactly has two integer solutions*

$$(X, Y, Z) = (a, 1, 1),\ (8a^3 + 3a, 1, 3)$$

with $X > 0$ *and* $Y = 1$. ∎

LEMMA 8 (Cao [4]). *The equation*

$$x^2 + 2^m = y^n, \quad m > 0,\ n > 0,\ x > 0,\ y > 0,$$

has only integer solutions

$$(m, n, x, y) = (2^r + 2, 2, 2^{2^r} - 1, 2^{2^r} + 1)$$

with $n > 1$, $y > 5$ *and* $2 \nmid y$, *where* r *is a positive integer.* ∎

LEMMA 9 (Brown [3]). *The equation*

$$x^2 + 3^m = y^n, \quad m > 0,\ n > 0,\ x > 0,\ y > 0,$$

has no integer solution (m, n, x, y) *with* $2 \nmid m$, $n > 1$, $2 \nmid n$ *and* $y > 7$. ∎

3. Further preliminary lemmas.

LEMMA 10. *Let* (X, Y, Z) *be an integer solution of* (3) *and let*

$$\varepsilon = X + Y\sqrt{-D'}, \quad \bar{\varepsilon} = X - Y\sqrt{-D'}. \tag{5}$$

If

$$t|\varepsilon - \bar{\varepsilon}| \geqslant |\varepsilon^t - \bar{\varepsilon}^t| \tag{6}$$

for some positive integer t, *then* $t < 2^{227}$.

Proof. From the proof of Lemma 3 in [11],

$$\log|\varepsilon^t - \bar{\varepsilon}^t| > t \log|\varepsilon| + \log\left|t \log\frac{\bar{\varepsilon}}{\varepsilon} - k\log(-1)\right|, \tag{7}$$

where k is an integer with $|k| \leqslant 2t$. From (3) and (5), $\bar{\varepsilon}/\varepsilon$ is a root of the equation

$$p^Z z^2 - 2(X^2 - D' Y^2) z + p^Z = 0.$$

Hence, $\bar{\varepsilon}/\varepsilon$ is not a root of unity and its degree $d = 2$ and the height

$$H = \max(p^Z, 2|X^2 - D' Y^2|) < 2p^Z.$$

It follows that

$$\Lambda = t\log\frac{\bar{\varepsilon}}{\varepsilon} - k\log(-1) \neq 0.$$

Further, by Lemma 1, we have

$$|\Lambda| > \exp(-2^{189} d^{30}(\log 2t)(\log 2p^Z)(\log 4)(\log\log 4))$$
$$> \exp(-2^{218}(\log 2t)(\log 2p^Z)).$$

Substituting it into (7), we obtain

$$\log|\varepsilon^t - \bar{\varepsilon}^t| > t\log|\varepsilon| - 2^{218}(\log 2t)(\log 2p^Z). \tag{8}$$

Note that $p \geqslant 3$. From (3) and (5),

$$|\varepsilon| = p^{Z/2}, \quad |\varepsilon - \bar{\varepsilon}| = 2|Y|\sqrt{D'} < 2p^{Z/2} < p^{3Z/2}.$$

Hence, if (6) holds, then from (8) we deduce

$$3 + 2\log t + 2^{220}\log 2t > t,$$

whence we conclude that $t < 2^{227}$. ∎

LEMMA 11. *Under the assumption of Lemma 10, let $q_1, q_2, \ldots, q_s$ be odd primes which satisfy $q_1 < q_2 < \ldots < q_s$ and $q_i | D'$ $(i = 1, 2, \ldots, s)$. If*

$$\left|\frac{\varepsilon^t - \bar{\varepsilon}^t}{\varepsilon - \bar{\varepsilon}}\right| = q_1^{r_1} q_2^{r_2} \ldots q_s^{r_s} \tag{9}$$

for some positive integers t and $r_1, r_2, \ldots, r_s$ with $2 \nmid t$, then

$$t = q_1^{r'_1} q_2^{r'_2} \ldots q_s^{r'_s} t' \tag{10}$$

where $r'_1, r'_2, \ldots, r'_s$ and t' are positive integers satisfying

$$r'_1 \begin{cases} \leqslant r_1, & q_1 = 3 \text{ and } 3 \| D' Y^2, \\ = r_1, & \text{otherwise}; \end{cases} \qquad r'_j = r_j,\ j = 2, \ldots, s. \tag{11}$$

Proof. If (9) holds, then $t > 1$, and from (5) we have

$$\left|tX^{t-1} + \sum_{l=1}^{(t-1)/2} \binom{t}{2l+1} X^{t-2l-1}(-D'Y^2)^l\right| = q_1^{r_1} q_2^{r_2} \ldots q_s^{r_s}.$$

Since $q_i | D'$ $(i = 1, 2, \ldots, s)$ and $q_i \nmid X$ from (3), we see that $q_i | t$. If $q_i^{\alpha_i} \| D' Y^2$, $q_i^{\beta_i} \| t$, $q_i^{\lambda_{l,i}} \| (2l+1)$ $(l = 1, \ldots, (t-1)/2)$, then

$$\lambda_{l,i} \leqslant \frac{\log(2l+1)}{\log q_i} \leqslant l \leqslant \alpha_i l, \quad i = 1, 2, \ldots, s,\ l = 1, \ldots, (t-1)/2,$$

where all "$\leqslant$" can be replaced by "$=$" if and only if $q_i = 3$, $\alpha_i = 1$ and $l = 1$.

Hence

$$\binom{t}{2l+1} X^{t-2l-1}(-D'Y^2)^l$$
$$= t\binom{t-1}{2l}\frac{(-D'Y^2)^l}{2l+1} X^{t-2l-1} \equiv 0 \pmod{q_i^{\beta_i+1}},$$
$$i = 1, 2, \ldots, s,\ l = 1, \ldots, (t-1)/2$$

except when $q_i = 3$, $\alpha_i = 1$ and $l = 1$. This proves the lemma. ∎

LEMMA 12. *When $\max(D', p) > M$, if (9) holds, then $s = 1$ and $q_s = 3$.*

Proof. By Lemma 11, if (9) holds, then t satisfies (10) and (11). Let

$$\varepsilon_1 = \varepsilon^{t'}, \quad \bar{\varepsilon}_1 = \bar{\varepsilon}^{t'}, \quad \varepsilon_j = \varepsilon^{q_1^{r'_1} \ldots q_{j-1}^{r'_{j-1}} t'}, \quad \bar{\varepsilon}_j = \bar{\varepsilon}^{q_1^{r'_1} \ldots q_{j-1}^{r'_{j-1}} t'},\ j = 2, \ldots, s.$$

By Lemma 5, we have

$$\varepsilon_i = X'_i + Y'_i\sqrt{-D'}, \quad \bar{\varepsilon}_i = X'_i - Y'_i\sqrt{-D'}, \quad i = 1, 2, \ldots, s,$$

where X'_i, Y'_i $(i = 1, 2, \ldots, s)$ are integers satisfying

$$X_1'^2 + D' Y_1'^2 = p^{zt'}, \quad \gcd(X'_1, Y'_1) = 1,$$

$$X_j'^2 + D' Y_j'^2 = p^{zq_1^{r'_1} \ldots q_{j-1}^{r'_{j-1}} t'}, \quad \gcd(X'_j, Y'_j) = 1, \quad j = 2, \ldots, s.$$

By Waring's formula that for any positive integer t and complex numbers α, β

$$\alpha^t + \beta^t = \sum_{l=0}^{[t/2]} (-1)^l \binom{t}{l}(\alpha+\beta)^{t-2l}(\alpha\beta)^l,$$

where

$$\binom{t}{l} = \frac{(t-l-1)!\,t}{(t-2l)!\,l!}, \quad l = 0, \ldots, [t/2]$$

are positive integers, we see that

$$\left|\frac{\varepsilon_1 - \bar{\varepsilon}_1}{\varepsilon - \bar{\varepsilon}}\right| \quad \text{and} \quad \left|\frac{\varepsilon_i^{q_i^{k_i}} - \bar{\varepsilon}_i^{q_i^{k_i}}}{\varepsilon_i^{q_i^{k_i-1}} - \bar{\varepsilon}_i^{q_i^{k_i-1}}}\right|, \quad k_i = 1, \ldots, r'_i,\ i = 1, 2, \ldots, s,$$

are positive integers satisfying

$$\left|\frac{\varepsilon_i^{q_i^{k_i}} - \bar{\varepsilon}_i^{q_i^{k_i}}}{\varepsilon_i^{q_i^{k_i-1}} - \bar{\varepsilon}_i^{q_i^{k_i-1}}}\right| \equiv 0 \pmod{q_i}.$$

Since we know from (10) that

$$\left|\frac{\varepsilon^t-\bar{\varepsilon}^t}{\varepsilon-\bar{\varepsilon}}\right| = \left|\frac{\varepsilon_1-\bar{\varepsilon}_1}{\varepsilon-\bar{\varepsilon}}\right| \prod_{i=1}^{s} \prod_{k_i=1}^{r_i'} \left|\frac{\varepsilon_i^{q_i^{k_i}}-\bar{\varepsilon}_i^{q_i^{k_i}}}{\varepsilon_i^{q_i^{k_i-1}}-\bar{\varepsilon}_i^{q_i^{k_i-1}}}\right|.$$

Substitute it into (9): from (11) we deduce that if $q_s > 3$ then

$$q_s = \left|\frac{\varepsilon_s^{q_s}-\bar{\varepsilon}_s^{q_s}}{\varepsilon_s-\bar{\varepsilon}_s}\right| = \pm \sum_{l=0}^{(q_s-1)/2} \binom{q_s}{2l} (X_s'^2)^l (-D' Y_s'^2)^{(q_s-1)/2-l} \tag{12}$$

Note that q_s is an odd prime and

$$\binom{q_s}{0} = 1, \quad \binom{q_s}{q_s-1} = q_s, \quad q_s \left| \binom{q_s}{2l}\right., \quad l = 1, \ldots, (q_s-1)/2.$$

By Eisenstein's theorem

$$f(x, y) = \pm \sum_{l=0}^{(q_s-1)/2} \binom{q_s}{2l} x^l y^{(q_s-1)/2-l}$$

is a homogeneous irreducible polynomial of degree $(q_s-1)/2$ and with integer coefficients. From (12) we have

$$f(X_s'^2, -D' Y_s'^2) = q_s. \tag{13}$$

Since

$$\max_{l=0,\ldots,(q_s-1)/2} \binom{q_s}{2l} < 2^{q_s-1},$$

by Lemma 2, we see from (13) that if $q_s \geqslant 7$ then

$$\begin{aligned} \tfrac{1}{2}\max(D', p) &< \max(X_s'^2, D' Y_s'^2) \\ &< \exp\left(2^{q_s-2}(q_s-1)^{(5(q_s-1))^5} + (\log q_s)^{q_s+1}\right). \end{aligned} \tag{14}$$

On the other hand, by Lemma 10, if (12) holds then $q_s < 2^{227}$. Substituting it into (14), we conclude that $\max(D', p) < M$. Thus $q_s < 7$.

If $q_s = 5$, then from (12) we have

$$4X_s'^4 - 5\left(X_s'^2 - \frac{D' Y_s'^2}{5}\right)^2 = \pm 1.$$

Since $5 | D'$, by Lemma 3, we get $X_s'^2 = Y_s'^2 = 1$ and $D' = 10 < M$, whence $p = 11 < M$. This completes the proof. ■.

4. The proof of the Theorem. By Lemma 8, we see that the theorem holds for $D = 2$. We proceed now to prove that the theorem holds for $D = 3$. By Lemma 9, if $p > 7$, then the equation

$$x^2 + 3^m = p^n, \quad m > 0,\ n > 0,\ x > 0 \tag{15}$$

has no integer solution (m, n, x) with $2 \nmid m$, $n > 1$ and $2 \nmid n$. If (15) has an integer solution (m, n, x) with $2 \nmid m$ and $2 | n$, then

$$p^{n/2} - x = 1, \quad p^{n/2} + x = 3^m$$

whence

$$2 \equiv 2p^{n/2} = 1 + 3^m \equiv 0 \pmod 4,$$

which is a contradiction. Hence, (15) has at most one integer solution (m, n, x) with $2 \nmid m$.

If (15) has an integer solution (m, n, x) with $2 | m$, then $(X, Y, Z) = (x, 3^{m/2-1}, n)$ is an integer solution of

$$X^2 + 9Y^2 = p^Z, \quad \gcd(X, Y) = 1, \quad Z > 0. \tag{16}$$

Let $(X, Y, Z) = (X_1, Y_1, Z_1)$ be the least solution of (16). By Lemma 5, we have

$$n = Z_1 t, \tag{17}$$

$$x + 3^{m/2-1}\sqrt{-9} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-9})^t, \quad \lambda_1 = \pm 1,\ \lambda_2 = \pm 1, \tag{18}$$

where t is a positive integer. We see from (18) that $2 \nmid t$ and

$$3^{m/2-1} = \lambda_1 \lambda_2 Y_1 \sum_{l=0}^{(t-1)/2} \binom{t}{2l+1} X_1^{t-2l-1} (-9Y_1^2)^l. \tag{19}$$

Hence

$$Y_1 | 3^{m/2-1}, \quad Y_1 = 3^r \quad (0 \leqslant r \leqslant m/2-1).$$

If $r < m/2-1$, then from (19) we obtain $3 | t$. Let

$$X' + Y'\sqrt{-9} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-9})^{t/3}.$$

By Lemma 5, we see from (15), (17) and (18) that X', Y' are integers satisfying

$$X'^2 + 9Y'^2 = p^{Z_1 t/3} = p^{n/3}, \quad \gcd(X', Y') = 1$$

and

$$3^{m/2-1} = 3Y'(X'^2 - 3Y'^2). \tag{20}$$

From (20) we get $|Y'| = 3^{m/2-2}$ and

$$X'^2 - 3Y'^2 = X'^2 - 3^{m-3} = \pm 1.$$

It implies from [5] that $m = 4$, $X' = \pm 2$ and $p = 13$. Hence, if $p > M$, then $r = m/2-1$ and $Y_1 = 3^{m/2-1}$. Recalling that the least solution of (16) is unique, it follows that m is fixed for every integer solution (m, n, x) of (15) with $2 | m$. Therefore, by Lemma 7, if $p > M$ then (15) has at most one integer solution (m, n, x) with $2 | m$. Thus the theorem holds for $D = 3$. We obtain the following:

CONCLUSION 1. *The theorem holds for $D = 2$ and 3.*

For the general D, if (1) has an integer solution (m, n, x) with $2 \nmid m$, then $(X, Y, Z) = (x, D^{(m-1)/2}, n)$ is an integer solution of (3). Let $(X, Y, Z) = (X_1, Y_1, Z_1)$ be the least solution of (3). By Lemma 5,

$$n = Z_1 t,$$

(21) $$x + D^{(m-1)/2}\sqrt{-D} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-D})^t, \quad \lambda_1 = \pm 1,\ \lambda_2 = \pm 1,$$

where t is a positive integer

If $4|t$, let

(22) $$X' + Y'\sqrt{-D} = (X_1 + \lambda_2 Y_1 \sqrt{-D})^{t/4}, \qquad X'' + Y''\sqrt{-D} = (X_1 + \lambda_2 Y_1 \sqrt{-D})^{t/2}.$$

Then, by Lemma 5, X', Y', X'', Y'' are integers satisfying

(23) $$X'^2 + DY'^2 = p^{Z_1 t/4} = p^{n/4}, \quad \gcd(X', Y') = 1, \qquad X''^2 + DY''^2 = p^{Z_1 t/2} = p^{n/2}, \quad \gcd(X'', Y'') = 1$$

and

(24) $$X'' = X'^2 - DY'^2, \quad Y'' = 2X'Y'.$$

From (21) and (22), we have

(25) $$D^{(m-1)/2} = 2\lambda_1 X'' Y''.$$

Since $p \nmid D$ and $\gcd(D, X'') = 1$, from (25) we get

(26) $$|X''| = 1, \quad |Y''| = \frac{D^{(m-1)/2}}{2}.$$

Further, from (24) and (26) we obtain $|X'| = 1$, $|Y'| = D^{(m-1)/2}/4$ and

$$1 = |X''| = \left|1 - \frac{D^m}{16}\right|,$$

whence we deduce that $D = 2$, $m = 5$ and $p = 3$. Hence, if $\max(D, p) > M$, then $4 \nmid t$.

If $t = 2t_1$, $2 \nmid t_1$, let X'', Y'' satisfy (22). Then from (22) and (26) we have

(27) $$\lambda_3 + \lambda_4 \frac{D^{(m-1)/2}}{2}\sqrt{-D} = (X_1 + \lambda_2 Y_1 \sqrt{-D})^{t_1}, \quad \lambda_3 = \pm 1,\ \lambda_4 = \pm 1.$$

If $t_1 > 1$, then

$$\pm 1 = X_1 \sum_{l=0}^{(t_1-1)/2} \binom{t_1}{2l} X_1^{t_1-2l-1}(-DY_1^2)^l,$$

whence $X_1 = 1$. Hence, we see from (23) that (3) has two integer solutions

$$(X, Y, Z) = (1, Y_1, Z_1),\ (1, D^{(m-1)/2}/2, n/2)$$

with $X = 1$ and $Y > 0$. By Lemma 6, it is impossible when $\max(D, p) > 7$. Therefore, if $2|t$ then $t = 2$ and the least solution of (3) is

$$(X_1, Y_1, Z_1) = (1, D^{(m-1)/2}/2, n/2).$$

In this case, we see from the above analysis that if (1) has another integer solution $(m, n, x) = (m', n', x')$ with $2 \nmid m'$, then from Lemma 5 we have

$$n' = \frac{n}{2}t',$$

$$x' + D^{(m'-1)/2}\sqrt{-D} = \lambda_1 \left(1 + \lambda_2 (D^{(m-1)/2}/2)\sqrt{-D}\right)^{t'}, \quad \lambda_1 = \pm 1,\ \lambda_2 = \pm 1,$$

where t' is an integer with $t' > 1$ and $2 \nmid t'$. It follows that

(28) $$D^{(m'-1)/2} = \lambda_1 \lambda_2 \frac{D^{(m-1)/2}}{2} \sum_{l=0}^{(t'-1)/2} \binom{t'}{2l+1}\left(\frac{D^m}{4}\right)^l.$$

Since $2 \nmid p$, $8 | D^m$ and

$$2 \nmid \sum_{l=0}^{(t'-1)/2} \binom{t'}{2l+1}\left(\frac{D^m}{4}\right)^l,$$

from (28) we deduce that $m' = m - 2$, $2 \| D$ and D has no odd prime factor. Hence $D = 2$ and

$$1 + 2^{m-2} = p^{n/2}.$$

Note that $2 \nmid m$. We have $m = 3$ and $p = 3$. Thus we obtain the following:

CONCLUSION 2. *When $\max(D, p) > 7$, if (1) has an integer solution (m, n, x) with $2 \nmid m$ and $2|t$ in (21), then (1) has only one solution with $2 \nmid m$.*

If $2 \nmid t$, let

$$\varepsilon = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-D}), \quad \bar{\varepsilon} = \lambda_1 (X_1 - \lambda_2 Y_1 \sqrt{-D}).$$

From (21), we get

$$Y_1 \left|\frac{\varepsilon^t - \bar{\varepsilon}^t}{\varepsilon - \bar{\varepsilon}}\right| = D^{(m-1)/2}.$$

Since $2 \nmid p$ and $X_1^2 + DY_1^2 = p^{Z_1}$, one and only one of X_1^2 and DY_1^2 is even. Hence $(\varepsilon^t - \bar{\varepsilon}^t)/(\varepsilon - \bar{\varepsilon})$ is odd since

$$\frac{\varepsilon^t - \bar{\varepsilon}^t}{\varepsilon - \bar{\varepsilon}} = \sum_{l=0}^{(t-1)/2} \binom{t}{2l+1}(X_1^2)^{(t-1)/2-l}(-DY_1^2)^l.$$

By Lemma 12, if $\max(D, p) > M$, then $D^{(m-1)/2}/Y_1 = 3^r$ for some $r \geqslant 0$. Suppose there are two integer solutions $(m, n, x) = (m_1, n_1, x_1), (m_2, n_2, x_2)$ with $2 \nmid m_1$ and $2 \nmid m_2$ for which $2 \nmid t$ in (21). Since Y_1 is fixed, if $m_1 \neq m_2$, then we deduce that $D = 3$ and according to Conclusion 1, the theorem holds. If $m_1 = m_2$, $D' = D^{m_1}$, then from Lemma 7 we see that D' and p satisfy (4). In this case, if $m_1 > 1$ and $2 \nmid m_1$, then $2 \nmid D$. It is impossible by Lemma 4. If $2 | m_1$, then

$$p = (2a)^2 + 1 = a^2 + (D^{m_1/2})^2,$$

which is a contradiction since p is a prime and $\max(D, p) > M$. Thus, by Lemma 7 and Conclusion 2, we obtain the following:

CONCLUSION 3. *When* $\max(D, p) > M$, (1) *has at most one integer solution* (m, n, x) *with* $2 \nmid m$ *except when* $D = 3a^2 + 1$, $p = 4a^2 + 1$; *in this case* (1) *exactly has two integer solutions*

$$(m, n, x) = (1, 1, a),\ (1, 3, 8a^3 + 3a)$$

with $2 \nmid m$.

In the same way as the proof of Conclusion 3, we have the following:

CONCLUSION 4. *When* $\max(D, p) > M$, (1) *has at most one inetger solution* (m, n, x) *with* $2 | m$ *except when* $D = 2$, $p = 2^{2^r} + 1$.

Thus, from Conclusions 3 and 4, the theorem is proved.

Acknowledgement. The author would like to thank the referee for his valuable suggestions.

References

[1] A. Baker, *Contributions to the theory of diophantine equation I: On the representation of integers by binary forms*, Phil. Trans. Roy. Soc. London, A 263 (1968), 173–208.

[2] E. A. Bender and N. P. Herzberg, *Some diophantine equations related to the quadratic form* $ax^2 + by^2$, *Studies in Algebra and Number Theory*, pp. 219–272, Advances in Mathematics Supplementary Studies, Vol. 6, Academic Press, New York 1979.

[3] E. Brown, *Diophantine equation of form* $ax^2 + b^2 D = y^p$, J. Reine Angew. Math. 291 (1977), 110–127.

[4] Z. F. Cao, *On the equation* $x^2 + 2^m = y^n$ *and Hugh Edgar's problem*, Kexue Tongbao (Chinese), 31 (1986), 555–556.

[5] J. W. S. Cassels, *On the equation* $a^x - b^y = 1$ *(II)*, Proc. Camb. Phil. Soc. 56 (1960), 97–103.

[6] J. H. E. Cohn, *Lucas and Fibonacci numbers and some diophantine equations*, Proc. Glasgow Math. Assoc. 7 (1965), 24–28.

[7] M. H. Le, *On the generalized Ramanujan–Nagell equation (I)*, Kexue Tongbao (Chinese), 29 (1984), 268–271.

[8] M. H. Le, *On the generalized Ramanujan–Nagell equation (II)*, Kexue Tongbao (Chinese), 30 (1985), 396; Acta Changchun Teachers College Natur. Sci. Ser. (Chinese), (1986), 8–18.

[9] T. Nagell, *Sur l'impossibilité de quelques équations à deux indeterminées*, Norsk. Matem. Forenings Skrifter, 13 (1921), 65–82.

[10] A. J. van der Poorten and J. H. Loxton, *Multiplicative relations in number fields*, Bull. Austral. Math. Soc. 16 (1977), 83–98.

[11] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, *Transcendence Theory: Advances and Applications*, pp. 79–92, Academic Press, London and New York 1977.

[12] M. Toyoizumi, *On the diophantine equation* $y^2 + D^m = p^n$, Acta Arith. 42 (1983), 303–309.

RESEARCH DEPARTMENT,
CHANGSHA RAILWAY INSTITUTE
Changsha, Hunan, China

Received on 16.6.1987
and in revised form on 19.1.1988 (1730)