The Diophantine Equation $x^2 + D^m = 2^{n+2}$

by

Maohua Le

(Received May 10, 1993)

Abstract. Let $D$ be a positive integer with $2 \nmid D$. In this paper we prove that if $D \geq e^{e^{447}}$, then the equation $x^2 + D^m = 2^{n+2}$ has at most one positive integer solution $(x, m, n)$ with $m > 1$. Moreover, if $D \geq C$, then the equation has no solution $(x, m, n)$ with $m > 1$, where $C$ is an effectively computable absolute constant.

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$ denote the sets of integers, positive integers and rational numbers, respectively. Let $D \in \mathbb{N}$ be odd, and let $N(D)$ denote the number of solutions of the equation

$$(1) \quad x^2 + D^m = 2^{n+2}, \quad x, m, n \in \mathbb{N}, \quad m > 1.$$ 

Tanahashi [8] proved that $N(7) = 1$. Toyoizumi [9] proved that if $D > 7$, $D = 2^r - a^2$, $a, r \in \mathbb{N}$, $r \geq 3$ and $D$ is square free, then $N(D) = 0$. In this paper we prove the following result:

Theorem. If $D \geq e^{e^{447}}$, then $N(D) \leq 1$. Moreover, if $D \geq C$, then $N(D) = 0$, where $C$ is an effectively computable absolute constant.

2. Lemmas

Lemma 1 ([1, Proof of Lemma 8]). If the equation

$$(2) \quad X^2 + DY^2 = 2^{z+2}, \quad X, Y, Z \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Z > 0,$$

has solutions $(X, Y, Z)$, then it has a unique solution $(X_1, Y_1, Z_1)$ such that $X_1 > 0$, $Y_1 > 0$ and $Z_1 \leq Z$, where $Z$ runs over all solutions of (2). $(X_1, Y_1, Z_1)$ is called the least solution of (2). Moreover, all solutions $(X, Y, Z)$ of (2) are given by
\[ Z = Z_1 t, \quad \frac{X + Y \sqrt{-D}}{2} = \lambda_1 \left( \frac{X_1 + \lambda_2 Y_1 \sqrt{-D}}{2} \right)^t, \quad \lambda_1, \lambda_2 \in \{-1, 1\}, \]

where \( t \) is an arbitrary positive integer.

**Lemma 2 ([5, page 117]).** For any \( k \in \mathbb{N} \) and any complex numbers \( \alpha, \beta \), we have

\[
\alpha^k + \beta^k = \sum_{i=0}^{\lfloor k/2 \rfloor} (-1)^i \binom{k}{i} (\alpha + \beta)^{k-2i} (\alpha \beta)^i,
\]

where

\[
\binom{k}{i} = \frac{(k-i-1)!k}{(k-2i)!i!} \in \mathbb{N}, \quad i = 0, \ldots, \left\lfloor \frac{k}{2} \right\rfloor.
\]

**Lemma 3.** Let \((X, Y, Z)\) be a solution of (2), and let

\[ \varepsilon = \frac{X + Y \sqrt{-D}}{2}, \quad \tilde{\varepsilon} = \frac{X - Y \sqrt{-D}}{2}. \]

Let \( p_1, \ldots, p_s \) be distinct odd primes which satisfy \( p_j \geq 7 \) and \( p_j \mid D \) for \( j = 1, \ldots, s \). If

\[ \left| \frac{\varepsilon^k - \tilde{\varepsilon}^k}{\varepsilon - \tilde{\varepsilon}} \right| = p_1^{a_1} \cdots p_s^{a_s} \]

for some \( k, a_1, \ldots, a_s \in \mathbb{N} \) with \( 2 \nmid k \), then \( k = p_1^{a_1} \cdots p_s^{a_s} k_1 \), where \( k_1 \in \mathbb{N} \) with \( \gcd(k_1, p_1 \cdots p_s) = 1 \).

**Proof.** By (3), we have

\[ \varepsilon + \tilde{\varepsilon} = X, \quad \varepsilon - \tilde{\varepsilon} = Y \sqrt{-D}, \quad \varepsilon \tilde{\varepsilon} = 2^Z. \]

Since \( p_j \mid D \) for \( j = 1, \ldots, s \), by Lemma 2, we see from

\[ \frac{\varepsilon^k - \tilde{\varepsilon}^k}{\varepsilon - \tilde{\varepsilon}} = \left( \sum_{i=0}^{(k-1)/2} \binom{k}{i} (\varepsilon - \tilde{\varepsilon})^{k-2i} (\varepsilon \tilde{\varepsilon})^i \right) = \left( \sum_{i=0}^{(k-1)/2} \binom{k}{i} (-D Y^2)^{(k-1)/2 - i} 2^{2i} \right) \]

that \( p_j \mid k \). Let \( p_j^{\beta_j} \mid D Y^2, p_j^{\gamma_j} \parallel k \) and \( p_j^{\beta_j + 1} \parallel 2l + 1 \) for any \( l \in \mathbb{N} \). Since \( p_j \geq 7 \), then we have

\[ \delta_{l, j} \leq \frac{\log(2l + 1)}{\log p_j} < l, \quad j = 1, \ldots, s. \]

Therefore,

\[ \left[ \frac{k-1}{2} - l \right] (-D Y^2)^l = \frac{k(-D Y^2)^l}{2l + 1} \left( \frac{k-1}{2l + 1} + l \right) \equiv 0 \pmod{p_j^{\gamma_j + 1}}, \quad j = 1, \ldots, s, \]

for \( l \geq 1 \). It implies that
The Diophantine Equation $x^2 + D^n = 2^{n+2}$

$$p_j^N \parallel \frac{\epsilon^k - \bar{\epsilon}^k}{\epsilon - \bar{\epsilon}}, \quad j = 1, \ldots, s,$$

by (6). Thus, if (4) holds, then $k = p_1^{a_1} \cdots p_s^{a_s} k_1$ with $\gcd(k_1, p_1 \cdots p_s) = 1$. The lemma is proved.

Lemma 4 ([6, Section 10]). Let $x$ be an algebraic number of degree 2 with the minimal polynomial

$$a_0 z^2 + a_1 z + a_2 = a_0(z - \sigma_1 x)(z - \sigma_2 x) \in \mathbb{Z}[z], \quad a_0 > 0,$$

where $\sigma_1 x, \sigma_2 x$ are conjugates of $x$. Further let $\log x$ be any nonzero determination of the logarithm of $x$. If $A = b_1 \pi \sqrt{-1}/b_2 - \log x \neq 0$ for some coprime $b_1, b_2 \in \mathbb{N}$, then

$$|A| \geq \exp(-20600A(1.35 + \log B + \log \log 2B)^2),$$

where

$$A = \max \left( \frac{1}{2}, \frac{1}{2} \left( \log a_0 + \sum_{j=1}^{2} \log \max(1, |\sigma_j x|) \right) \right), \quad B = \max(b_1, b_2).$$

Lemma 5. Let $(X, Y, Z)$ be a solution of (2), and let $\epsilon, \bar{\epsilon}$ be defined as in (3). If

$$\left| \frac{\epsilon^k - \bar{\epsilon}^k}{\epsilon - \bar{\epsilon}} \right| \leq k$$

for some $k \in \mathbb{N}$, then $k < 8 \cdot 10^6$.

Proof. For any complex number $z$, we have either $|e^z - 1| > 1/2$ or $|e^z - 1| \geq |z - t \pi \sqrt{-1}|/2$ for $t \in \mathbb{Z}$ with $2 | t$. Hence, if (7) holds, then

$$\log k + \log |\epsilon - \bar{\epsilon}| \geq \log |\epsilon^k - \bar{\epsilon}^k| = k \log |\epsilon| + \log \left( \frac{\bar{\epsilon}}{\epsilon} \right)^k - 1$$

(8)

$$\geq k \log |\epsilon| + \log \left| k \log \frac{\bar{\epsilon}}{\epsilon} - t \pi \sqrt{-1} \right| - \log 2,$$

where $t \in \mathbb{Z}$ with $|t| \leq k$. By (2) and (3), $\bar{\epsilon}/\epsilon$ satisfies

$$2^2 \left( \frac{\bar{\epsilon}}{\epsilon} \right)^2 - \left( \frac{X^2 - DY^2}{2} \right) \frac{\bar{\epsilon}}{\epsilon} + 2^2 = 0.$$

Since $Z > 0$, $\bar{\epsilon}/\epsilon$ is not a root of unity. Therefore $k \log(\bar{\epsilon}/\epsilon) - t \pi \sqrt{-1} \neq 0$. By Lemma 4, we get from (9) that

(9)

$$k \log \frac{\bar{\epsilon}}{\epsilon} - t \pi \sqrt{-1} \geq k \exp \left( -20600 \left( \frac{\log 2^2}{2} \right)(1.35 + \log k + \log \log 2k)^2 \right).$$

Since $|\epsilon - \bar{\epsilon}| = |Y| \sqrt{D} < 2^{2Z/2 + 1}$ and $|\epsilon| = 2^{Z/2}$, substituting (10) into (8),
\[
\log 2^{z/2 + 2} + 10300(\log 2^z)(1.35 + \log k + \log \log 2k)^2 \geq k \log 2^{z/2},
\]
whence we conclude that \(k \leq 8 \times 10^6\). The lemma is proved.

**Lemma 6 ([3]).** Let \(a \in \mathbb{Z}\) with \(a \neq 0\), and let \(f(X, Y) \in \mathbb{Z}[X, Y]\) be a binary form of degree \(r\) such that among the linear factors in the factorization of \(f(X, Y)\) at least three are distinct. Then all solutions \((X, Y)\) of the equation

\[
f(X, Y) = a, \quad X, Y \in \mathbb{Z}
\]

satisfy \(\max(|X|, |Y|) \leq \exp(10^{150} \cdot 6 \log(a |H))\), where \(H\) is the maximum absolute value of coefficients of \(f(X, Y)\).

**Lemma 7.** If (7) holds for some \(k \in \mathbb{N}\) with \(2 \nmid k\) and \(k \geq 7\), then \(D < e^{e^{47}}\).

**Proof.** For any \(k \in \mathbb{N}\) with \(2 \nmid k\) and \(k \geq 7\), let

\[
f(X, Y) = \sum_{i=0}^{(k-1)/2} \binom{k}{i} X^{(k-1)/2 - i} Y^i.
\]

By Lemma 2, \(f(X, Y) \in \mathbb{Z}[X, Y]\) is a binary form of degree \((k-1)/2\) such that among the linear factors in the factorization of \(f(X, Y)\) at least three are distinct. If (7) holds, then we have

(11) \[
f(-DY^2, 2^z) = a,
\]

where \(a \in \mathbb{Z}\) with \(0 < |a| \leq k\). Notice that

\[
\max_{i=0, \ldots, (k-1)/2} \binom{k}{i} = \max_{i=0, \ldots, (k-1)/2} \frac{k}{k-i} \binom{k-i}{i} \leq 2^{k-1}.
\]

On applying Lemma 6 with (11), we get

(12) \[
D \leq \max(DY^2, 2^z) \leq \exp \left(10^{150} \left(\frac{k-1}{2}\right)^6 \log(2^{k-1}k)\right).
\]

Further, on applying Lemma 5 with (12), we conclude that \(D < e^{e^{47}}\). The lemma is proved.

**Lemma 8 ([2]).** The equation

\[
X^2 - 5Y^4 = 1, \quad X, Y \in \mathbb{N}
\]

has only the solution \((X, Y) = (9, 2)\).

**Lemma 9 ([7, Theorem 2]).** Let \(S\) be the set of all nonzero integers composed of primes from a fixed finite set \(P\). Let \(f(X, Y) \in \mathbb{Z}[X, Y]\) be a binary form with \(f(1, 0) \neq 0\) such that among the linear factors in the factorization of \(f(X, Y)\) at least two are distinct, and let \(H\) denote the maximum absolute value of coefficients of \(f(X, Y)\). Then all solutions \((X, Y, Z, m)\) of the equation
The Diophantine Equation $x^2 + D^m = 2^n + 2$

$f(X, Y) = Z^m, \quad X, Y, Z, m \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Y \in S, \quad |Z| > 1, \quad m > 0$
satisfy $m < C_1$, where $C_1$ is an effectively computable constant depending only on $H$ and $S$.

**Lemma 10 ([4]).** Let $a, b, X, Y, r, s \in \mathbb{Z}$ be nonzero with $r \geq 2, s \geq 2, rs \geq 6$ and $
\gcd(X, Y) = 1$, and let $P[aX' + bY']$ denote the great prime factor of $aX' + bY'$. Then

$$P[aX' + bY'] > C_2 \sqrt{(\log \log X')(\log \log \log X')},$$

where $X' = \max(|X|, |Y|), \quad C_2$ is an effectively computable constant depending only on $a, b, r$ and $s$.

3. **Proof of Theorem**

First we assume that $D \geq e^{*47}$. Let $(x, m, n)$ be a solution of (1). Then $2 \nmid m$ and $m \geq 2$. If $2 \nmid n$, then we get from (1) that $2^{n/2 + 1} + x = D_1^m, 2^{n/2 + 1} - x = D_2^m$ and

$$D_1^m + D_2^m = 2^{n/2 + 2},$$

where $D_1, D_2 \in \mathbb{N}$ with $D_1D_2 = D$. Since $m \geq 3$ and $2 \nmid D$, (13) is impossible. Hence, $2 \nmid n$ and $(x, D^{2(m-1)/2}, n)$ is a solution of (2). By Lemma 1,

$$n = Z_1 t,$$

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

where $t \in \mathbb{N}$ with $2 \nmid t, (X_1, Y_1, Z_1)$ is the least solution of (2).

Now we suppose that $t > 1$. Let

$$\varepsilon = \frac{X_1 + Y_1 \sqrt{-D}}{2}, \quad \bar{\varepsilon} = \frac{X_1 - Y_1 \sqrt{-D}}{2}.$$

Then

$$\varepsilon + \bar{\varepsilon} = X_1, \quad \varepsilon - \bar{\varepsilon} = Y_1 \sqrt{-D}, \quad \varepsilon \bar{\varepsilon} = 2Z_1.$$

We get from (15) that

$$D^{(m-1)/2} = \lambda_1 \lambda_2 \frac{\varepsilon^t - \bar{\varepsilon}^t}{\sqrt{-D}} = \lambda_1 \lambda_2 Y_1 \frac{\varepsilon^t - \bar{\varepsilon}^t}{\varepsilon - \bar{\varepsilon}}.$$

Using Lemma 2, we have

$$\frac{\varepsilon^t - \bar{\varepsilon}^t}{\varepsilon - \bar{\varepsilon}} = \sum_{i=0}^{t-1} \left( \begin{array}{c} t-1 \cr i \end{array} \right) (-D Y_i^2)^{(t-1)/2} z_i, \quad z_i \in \mathbb{Z}$$

by (17).

Write $D = q_1^\beta_1 \cdots q_r^\beta_r$, where $q_1, \cdots, q_r$ are distinct odd primes, $\beta_1, \cdots, \beta_r \in \mathbb{N}$. 
Since \( 2 \nmid n \), we see from (1) that \( (2/q_j) = 1 \) for \( j = 1, \ldots, r \), where \( (2/q_j) \) is the Legendre symbol. It implies that \( q_j \equiv \pm 1 \pmod{8} \) and \( q_j \geq 7 \) for \( j = 1, \ldots, r \).

By (18) and (19), if \( Y_1 = D^{(m-1)/2} \), then

\[
\frac{e^t - \bar{e}^t}{e - \bar{e}} = 1.
\]

Under our assumption, on applying Lemma 7 with (20), we obtain either \( t = 3 \) or \( t = 5 \). When \( t = 3 \), we get from (20) that

\[ 1 + D^m = 3 \cdot 2^{Z_1}.
\]

Since \( m \geq 3 \), it is impossible. When \( t = 5 \), since \( 2 \nmid n \) and \( 2 \nmid Z_1 \) by (14), we get

\[
(D^{2m} - 5 \cdot 2^{Z_1 - 1})^2 - 5 \cdot 2^{4((Z_1 - 1)/2)} = 1.
\]

By Lemma 8, it is impossible.

If \( Y_1 \neq D^{(m-1)/2} \), the from (18) and (19) we get

\[
\frac{e^t - \bar{e}^t}{e - \bar{e}} = p_1^{s_1} \cdots p_s^{s_s},
\]

where \( \{p_1, \ldots, p_s\} \subseteq \{q_1, \ldots, q_r\} \). Recalling that \( q_j \geq 7 \) for \( j = 1, \ldots, r \). On applying Lemma 3 with (21), we obtain \( t \geq p_1^{s_1} \cdots p_s^{s_s} \). Further, by Lemma 7, (21) is false for \( D < e^{e^{e^e}} \). Thus \( t = 1 \) and \( (x, n) = (X_1, Z_1) \) by (15). It implies that \( N(D) \leq 1 \) for \( D \geq e^{e^{e^{e^e}}} \).

On the other hand, since \( 2 \nmid n \), we find from (1) that \( (x, 2^{(n+1)/2}, -D, m) \) is a solution of the equation

\[
X^2 - 2Y^2 = Z^m, \quad X, Y, Z, m \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Y \in S, \quad |Z| > 1, \quad m > 0,
\]

where \( S = \{ \pm 2^r \mid r \in \mathbb{Z}, r \geq 0 \} \). Hence, by Lemma 9, we get

\[
m < C_3,
\]

where \( C_3 \) is an effectively computable absolute constant. Clearly, we see from (1) that \( P[x^2 + D^m] = 2 \). Since \( m \geq 3 \), by Lemma 10, we get

\[
D \leq \max(x, D) < C_4,
\]

where \( C_4 \) is an effectively computable constant depending only on \( m \). Thus, by (22), we deduce that \( D < C \), when \( C \) is an effectively computable absolute constant. This implies that if \( D \geq C \), then \( N(D) = 0 \). The proof is complete.

References


Hunan Normal University
Department of Mathematics
P.O. Box 410081 Changsha,
P. R. China

Current address:
Zhanjiang Teachers College
Department of Mathematics
P.O. Box 524048
Zhanjiang, Guangdong
P. R. China