A NOTE ON THE EXPONENTIAL DIOPHANTINE EQUATION $x^2 - 2^m = y^n$

YONGDONG GUO AND MAOHUA LE

(Communicated by William W. Adams)

Abstract. In this note we prove that the equation $x^2 - 2^m = y^n$, $x, y, m, n \in \mathbb{N}$, $\gcd(x, y) = 1$, $y > 1$, $n > 2$, has only finitely many solutions $(x, y, m, n)$. Moreover, all solutions of the equation satisfy $2 \nmid mn$, $n < 2 \cdot 10^9$ and $\max(x, y, m) < C$, where $C$ is an effectively computable absolute constant.

Let $\mathbb{Z}$, $\mathbb{N}$, and $\mathbb{Q}$ be the sets of integers, positive integers, and rational numbers respectively. In [3], Rabinowitz proved that the equation

$$(1) \quad x^2 - 2^m = y^n, \quad x, y, m, n \in \mathbb{N}, \gcd(x, y) = 1, y > 1, n > 2,$$

has only the solution $(x, y, m, n) = (71, 17, 7, 3)$ with $n = 3$. In this note we give a general result as follows.

Theorem. Equation (1) has only finitely many solutions $(x, y, m, n)$. Moreover, all solutions of (1) satisfy $2 \nmid mn$, $n < 2 \cdot 10^9$ and $\max(x, y, m) < C$, where $C$ is an effectively computable absolute constant.

In order to prove the theorem, we now introduce a result concerned with the linear forms in logarithms, which was derived by Dong [1]. Let $\alpha$ be a nonzero algebraic number with the defining polynomial

$$a_0 z^r + a_1 z^{r-1} + \cdots + a_r = a_0(z - \sigma_1 \alpha) \cdots (z - \sigma_r \alpha), \quad a_0 \in \mathbb{N},$$

where $\sigma_1 \alpha, \ldots, \sigma_r \alpha$ are all the conjugates of $\alpha$. Then

$$h(\alpha) = \frac{1}{r} \left( \log a_0 + \sum_{i=1}^{r} \log \max(1, |\sigma_i \alpha|) \right)$$

is called Weil's height of $\alpha$. Let $K$ be an algebraic number field of degree $D$ over $\mathbb{Q}$, and let $\mathfrak{p}$ be a prime ideal of $K$ with $\mathfrak{p} | p$, where $p$ is a prime. We write $e_p$ for the ramification index of $\mathfrak{p}$, and for $\alpha \in K \setminus \{0\}$, we denote by $\text{ord}_p \alpha$ the order to which $p$ divides the principal ideal $[\alpha]$ of $K$.

Received by the editors March 7, 1994 and, in revised form, June 18, 1994.

1991 Mathematics Subject Classification. Primary 11D61, 11J86.

Supported by the National Natural Science Foundation of China.

©1995 American Mathematical Society

3627
Lemma 1 ([1, Theorem 4.1 and Corollary 1.1]). Let \( \alpha_1, \alpha_2 \in K \setminus \{0\} \). If \( \text{ord}_p (\alpha_j - 1) > \epsilon_p / (p-1) \) (\( j = 1, 2 \)) and \( \Lambda = \alpha_1^{b_1} - \alpha_2^{b_2} \neq 0 \) for some \( b_1, b_2 \in \mathbb{Z} \), then we have

\[
\log |\Lambda| > \begin{cases} 
-37390D^4 A_1 A_2 (\log B)^2, & \text{if } p = 2, \\
-2500 \left( \frac{p}{p-1} + \frac{1}{p^2} \right) p^2 + 0.17159 \right) D^4 A_1 A_2 (\log B)^2, & \text{if } p > 2,
\end{cases}
\]

and

\[
\text{ord}_p \Lambda \leq \frac{(51p + 67)^2}{(\log p)^4} \epsilon_p D^4 A_1 A_2 (\log B)^2,
\]

where \( A_j = \max(h(\alpha_j), 2\log p) \) (\( j = 1, 2 \)), \( B = \max(3, |b_1|, |b_2|) \).

Lemma 2 ([2]). Let \( a, b, x, y, m, n \in \mathbb{Z} \setminus \{0\} \) be such that \( \gcd(x, y) = 1 \), \( m \geq 2 \), \( n \geq 2 \) and \( mn \geq 6 \). Then the greatest prime factor \( P(ax^m + by^n) \) of \( ax^m + by^n \) satisfies \( P(ax^m + by^n) > C(a, b, m, n)(\log \log X)(\log \log \log X) \right)^{1/2} \), where \( C(a, b, m, n) \) is an effectively computable constant depending only on \( a, b, m \) and \( n \), and \( X = \max(\epsilon x, |x|, |y|) \).

Proof of Theorem. Let \( (x, y, m, n) \) be a solution of equation (1). If \( 2 \mid m \), then we have

\[
x + 2^{m/2} = y_1^n, \quad x - 2^{m/2} = y_2^n, \quad y = y_1 y_2, \quad y_1, y_2 \in \mathbb{N};
\]

whence we get

\[
2^{m/2+1} = y_1^n - y_2^n.
\]

Since \( (y_1^n - y_2^n)/(y_1 - y_2) \) is an odd integer with \( (y_1^n - y_2^n)/(y_1 - y_2) > 1 \), (2) is impossible. Hence \( 2 \nmid m \).

Let \( K = \mathbb{Q}(\sqrt{2}) \), and let \( h_K, O_K \) be the class number and the algebraic integer ring of \( K \), respectively. Then we have \( h_K = 1 \) and \( O_K = \mathbb{Z}[\sqrt{2}] \). For any \( \alpha \in O_K \setminus \{0\} \), let \( [\alpha] \) denote the principal ideal of \( K \) which is generated by \( \alpha \). If \( 2 \nmid m \), then from (1) we get

\[
[x + 2^{(m-1)/2}\sqrt{2}] [x - 2^{(m-1)/2}\sqrt{2}] = [y]^n.
\]

Since \( \gcd(x, y) = 1 \) and \( 2 \nmid xy \), \( \gcd([x + 2^{(m-1)/2}\sqrt{2}], [x - 2^{(m-1)/2}\sqrt{2}]) = [1] \), and by (3), we get \( [x + 2^{(m-1)/2}\sqrt{2}] = [\alpha]^n \), where \( \alpha \in O_K \) with the norm \( N(\alpha) = y \). It implies that

\[
x + 2^{(m-1)/2}\sqrt{2} = (X_1 + Y_1 \sqrt{2})^n(u + v\sqrt{2}),
\]

where \( X_1 \), \( Y_1 \) and \( u \), \( v \) satisfy

\[
X_1^2 - 2Y_1^2 = y, \quad X_1, Y_1 \in \mathbb{Z}, \quad \gcd(X_1, Y_1) = 1,
\]

and

\[
u^2 - 2v^2 = 1, \quad u, v \in \mathbb{Z},
\]

respectively. Let

\[
\rho = 3 + 2\sqrt{2}, \quad \overline{\rho} = 3 - 2\sqrt{2}.
\]

Since \( \rho \) is the fundamental solution of (6), by (4) and (5),

\[
x + 2^{(m-1)/2}\sqrt{2} = (X_2 + Y_2 \sqrt{2})^n\overline{\rho}^t, \quad t \in \mathbb{Z}, \quad 0 \leq t < n,
\]
where $X_2$, $Y_2$ satisfy
\begin{equation}
X_2^2 - 2Y_2^2 = y, \quad X_2, Y_2 \in \mathbb{Z}, \quad X_2 > 0, \quad \gcd(X_2, Y_2) = 1.
\end{equation}

Let
\begin{equation}
\varepsilon = X_2 + Y_2\sqrt{2}, \quad \overline{\varepsilon} = X_2 - Y_2\sqrt{2}.
\end{equation}

We see from (8) that
\begin{equation}
x - 2^{(m-1)}\sqrt{2} = \varepsilon^n\rho'.
\end{equation}

By (8) and (11), we get
\begin{equation}
2^{(m+1)/2}\sqrt{2} = \varepsilon^n\rho' - \overline{\varepsilon^n}\rho'.
\end{equation}

Let $\alpha_1 = \overline{\rho}^2$, $\alpha_2 = \varepsilon/\varepsilon$ and $\Lambda = \alpha_1^j - \alpha_2^j$. Since $\varepsilon > \overline{\varepsilon} > 0$ by (8) and (11), we find from (7), (9) and (10) that
\begin{equation}
h(\alpha_1) = \log \rho, \quad h(\alpha_2) = \log \varepsilon.
\end{equation}

Notice that $[2] = p^2$, where $p$ is a prime ideal of $K$. We have $\alpha_1, \alpha_2 \in K\setminus\{0\}$, and $\ord_p(\alpha_j - 1) \geq 3$ for $j = 1, 2$. Recall that $0 < t < n$. By Lemma 1, we have
\begin{equation}
\log |\Lambda| > -1054500(\log \varepsilon)(\log n)^2
\end{equation}
and
\begin{equation}
\ord_p \Lambda < 7054500(\log \varepsilon)(\log n)^2.
\end{equation}

Since $2^{(m+1)/2}\sqrt{2} = \varepsilon^n\rho'\Lambda$ by (12), we get
\begin{equation}
\frac{m + 2}{2} \log 2 = \log \varepsilon^n\rho' + \log |\Lambda| \geq n \log \varepsilon + \log |\Lambda|
\end{equation}
and
\begin{equation}
\ord_p \Lambda = m + 2.
\end{equation}

The combination of (14), (15), (16) and (17) yields
\begin{equation}
7054500(\log \varepsilon)(\log n)^2 > \frac{2n}{\log 2} \log \varepsilon - 3056600(\log \varepsilon)(\log n)^2;
\end{equation}
whence we deduce that
\begin{equation}
n < 2 \cdot 10^9.
\end{equation}
Thus, by Lemma 2, we get from (1) and (18) that $\max(x, y, m) < C$, where $C$ is an effectively computable absolute constant. The theorem is proved.

REFERENCES

2. S. V. Kotov, Über die maximale norm der idealteiler des polynoms $\alpha x^m + \beta y^n$ mit algebraischen Koeffizienten, Acta Arith. 31 (1976), 219–230.

DEPARTMENT OF MATHEMATICS, ZHANJIANG TEACHERS COLLEGE, P.O. BOX 524048, ZHANJIANG, GUANGDONG, PEOPLE’S REPUBLIC OF CHINA