PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 12, December 1995

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

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

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 α be a nonzero algebraic number with the defining polynomial

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

where $\sigma_1\alpha, \dots, \sigma_r\alpha$ are all the conjugates of α. 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 α. 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 $e_\mathfrak{p}$ for the ramification index of $\mathfrak{p}$, and for $\alpha \in K\backslash\{0\}$, we denote by $\operatorname{ord}_\mathfrak{p} \alpha$ the order to which $\mathfrak{p}$ 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.

Lemma 1 ([1, Theorem 4.1 and Corollary 1.1]). *Let* $\alpha_1, \alpha_2 \in K\backslash\{0\}$. *If* $\mathrm{ord}_{\mathfrak{p}}(\alpha_j - 1) > e_{\mathfrak{p}}/(p-1)$ $(j = 1, 2)$ *and* $\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2} \neq 0$ *for some* $b_1, b_2 \in \mathbb{Z}$, *then we have*

$$\log|\Lambda| > \begin{cases} -37390 D^4 A_1 A_2 (\log B)^2, & \text{if } p = 2, \\ -\frac{2500}{(\log p)^3}\left(\left(\frac{p}{p-1} + \frac{1}{p^2}\right)p^2 + 0.17159\right) D^4 A_1 A_2 (\log B)^2, & \text{if } p > 2, \end{cases}$$

and

$$\mathrm{ord}_{\mathfrak{p}} \Lambda \leq \frac{(51p + 67)^2}{(\log p)^4} e_{\mathfrak{p}} D^4 A_1 A_2 (\log B)^2,$$

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

Lemma 2 ([2]). *Let* $a, b, x, y, m, n \in \mathbb{Z}\backslash\{0\}$ *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* $P(ax^m + by^n) > C(a, b, m, n)((\log\log X)(\log\log\log X))^{1/2}$, *where* $C(a, b, m, n)$ *is an effectively computable constant depending only on* a, b, m *and* n, *and* $X = \max(e^{e^e}, |x|, |y|)$.

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

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

whence we get

$$2^{m/2+1} = y_1^n - y_2^n. \tag{2}$$

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 $\alpha \in O_K\backslash\{0\}$, let $[\alpha]$ denote the principal ideal of K which is generated by α. If $2 \nmid m$, then from (1) we get

$$[x + 2^{(m-1)/2}\sqrt{2}][x - 2^{(m-1)/2}\sqrt{2}] = [y]^n. \tag{3}$$

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

$$x + 2^{(m-1)/2}\sqrt{2} = (X_1 + Y_1\sqrt{2})^n (u + v\sqrt{2}), \tag{4}$$

where X_1, Y_1 and u, v satisfy

$$X_1^2 - 2Y_1^2 = y, \qquad X_1, Y_1 \in \mathbb{Z}, \ \gcd(X_1, Y_1) = 1, \tag{5}$$

and

$$u^2 - 2v^2 = 1, \qquad u, v \in \mathbb{Z}, \tag{6}$$

respectively. Let

$$\rho = 3 + 2\sqrt{2}, \qquad \overline{\rho} = 3 - 2\sqrt{2}. \tag{7}$$

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

$$x + 2^{(m-1)/2}\sqrt{2} = (X_2 + Y_2\sqrt{2})^n \overline{\rho}^t, \qquad t \in \mathbb{Z}, \ 0 \leq t < n, \tag{8}$$

where X_2, Y_2 satisfy

$$X_2^2 - 2Y_2^2 = y, \qquad X_2, Y_2 \in \mathbb{Z}, \; X_2 > 0, \; \gcd(X_2, Y_2) = 1. \tag{9}$$

Let

$$\varepsilon = X_2 + Y_2\sqrt{2}, \qquad \bar{\varepsilon} = X_2 - Y_2\sqrt{2}. \tag{10}$$

We see from (8) that

$$x - 2^{(m-1)}\sqrt{2} = \bar{\varepsilon}^n \rho^t. \tag{11}$$

By (8) and (11), we get

$$2^{(m+1)/2}\sqrt{2} = \varepsilon^n \bar{\rho}^t - \bar{\varepsilon}^n \rho^t. \tag{12}$$

Let $\alpha_1 = \bar{\rho}^2$, $\alpha_2 = \bar{\varepsilon}/\varepsilon$ and $\Lambda = \alpha_1^t - \alpha_2^n$. Since $\varepsilon > \bar{\varepsilon} > 0$ by (8) and (11), we find from (7), (9) and (10) that

$$h(\alpha_1) = \log \rho, \qquad h(\alpha_2) = \log \varepsilon. \tag{13}$$

Notice that $[2] = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime ideal of K. We have $\alpha_1, \alpha_2 \in K \backslash \{0\}$, and $\operatorname{ord}_{\mathfrak{p}}(\alpha_j - 1) \geq 3$ for $j = 1, 2$. Recall that $0 \leq t < n$. By Lemma 1, we have

$$\log|\Lambda| > -1054500(\log \varepsilon)(\log n)^2 \tag{14}$$

and

$$\operatorname{ord}_{\mathfrak{p}} \Lambda < 7054500(\log \varepsilon)(\log n)^2. \tag{15}$$

Since $2^{(m+1)/2}\sqrt{2} = \varepsilon^n \rho^t \Lambda$ by (12), we get

$$\frac{m+2}{2} \log 2 = \log \varepsilon^n \rho^t + \log|\Lambda| \geq n \log \varepsilon + \log|\Lambda| \tag{16}$$

and

$$\operatorname{ord}_{\mathfrak{p}} \Lambda = m + 2. \tag{17}$$

The combination of (14), (15), (16) and (17) yields

$$7054500(\log \varepsilon)(\log n)^2 > \frac{2n}{\log 2} \log \varepsilon - 3056600(\log \varepsilon)(\log n)^2;$$

whence we deduce that

$$n < 2 \cdot 10^9. \tag{18}$$

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

1. P.-P. Dong, *Minoration de combinaisons linéaires de deux logarithmes p-adiques*, Ann. Fac. Sci. Toulouse **12** (1991), 195–250.

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.

3. S. Rabinowitz, *The solution of* $y^2 \pm 2^n = x^3$, Proc. Amer. Math. Soc. **62** (1976), 1–6.

Department of Mathematics, Zhanjiang Teachers College, P.O. Box 524048, Zhanjiang, Guangdong, People's Republic of China