PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 2, February 1995

ON THE DIOPHANTINE EQUATION $2^n + px^2 = y^p$

LE MAOHUA

(Communicated by William Adams)

ABSTRACT. Let p be a prime with $p > 3$. In this paper we prove that: (i) the equation $2^n + px^2 = y^p$ has no positive integer solution (x, y, n) with $\gcd(x, y) = 1$; (ii) if $p \not\equiv 7 \pmod 8$, then the equation has no positive integer solution (x, y, n).

1. INTRODUCTION

Let $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ be the sets of integers, positive integers, and rational numbers, respectively. Let p be an odd prime. In [7], Rabinowitz found all solutions (x, y, n) of the equation

$$2^n + px^2 = y^p, \qquad x, y, n \in \mathbb{N}, \tag{1}$$

for $p = 3$. In this paper we prove the following results.

Theorem 1. *If $p > 3$, then (1) has no solution (x, y, n) with $\gcd(x, y) = 1$.*

Theorem 2. *If $p > 3$ and $p \not\equiv 7 \pmod 8$, then (1) has no solution (x, y, n).*

2. LEMMAS

Lemma 1 [2, Formula 1.76]. *For any $m \in \mathbb{N}$ and any complex numbers α, β, we have*

$$\alpha^m + \beta^m = \sum_{j=0}^{[m/2]} (-1)^j \begin{bmatrix} m \\ j \end{bmatrix} (\alpha + \beta)^{m-2j} (\alpha\beta)^j,$$

where

$$\begin{bmatrix} m \\ j \end{bmatrix} = \frac{(m-j-1)!m}{(m-2j)!j!} \in \mathbb{N}, \qquad j = 0, \dots, [m/2]. \quad \square$$

Let $D \in \mathbb{N}$ be squarefree, and let $h(-D)$ denote the class number of $\mathbb{Q}(\sqrt{-D})$.

Lemma 2 [5]. *If $D > 2$, then the equation*

$$1 + DX^2 = Y^n, \qquad X, Y, n \in \mathbb{N},\ Y > 1,\ n > 2,$$

has no solution (X, Y, n) with $n \nmid h(-D)$. $\square$

Received by the editors October 26, 1992 and, in revised form, April 26, 1993.
1991 *Mathematics Subject Classification.* Primary 11D61, 11J86.
Supported by the National Natural Science Foundation of China.

Lemma 3 [3]. *The equations*

$$1+DX^2=2Y^n, \qquad D\equiv 1 \pmod 4),\ X,\ Y,\ n\in\mathbb{N},\ Y>1,\ n>2,\ 2\nmid nY,$$

and

$$1+DX^2=4Y^n, \qquad D\equiv 3 \pmod 4),\ X,\ Y,\ n\in\mathbb{N},\ Y>1,\ n>2,\ 2\nmid nY,$$

have no solution (X, Y, n) *with* $n\nmid h(-D)$. □

Lemma 4 [6]. *If* $2\nmid D$ *and* $D\geq 3$, *then the equation*

$$2+DX^2=Y^n, \qquad X,\ Y,\ n\in\mathbb{N},\ Y>1,\ n>2,$$

has no solution (X, Y, n) *with* $n\nmid h(-2D)$. □

Lemma 5. *If* $p>3$ *and* $p\equiv 3 \pmod 8$, *then the equation*

$$\frac{X^p-2^p}{X-2}=pY^2, \qquad X,\ Y\in\mathbb{N},\ X\equiv 3 \pmod 8), \tag{2}$$

has no solution (X, Y).

Proof. Let (X, Y) be a solution of (2), and let $A=(X^p-2^p)/(X-2)$, $B=(X^{(p-1)/2}-2^{(p-1)/2})/(X-2)$. Since $p>3$, $X\equiv 3 \pmod 8$, and $X-2\equiv 0 \pmod p$ by (2), we have $B\in\mathbb{N}$ such that $B\equiv 3 \pmod 8$, $B\equiv 2^{(p-3)/2}(p-1)/2 \pmod p$, and $A\equiv 2^{p-1} \pmod B$. Let $(*/*)$ denote the Kronecker symbol. Then we have

$$\left(\frac{A}{B}\right)=\left(\frac{2^{p-1}}{B}\right)=1, \tag{3}$$

and by (2),

$$\left(\frac{A}{B}\right)=\left(\frac{pY^2}{B}\right)=\left(\frac{p}{B}\right)=-\left(\frac{B}{p}\right)=-\left(\frac{2^{(p-3)/2}(p-1)/2}{p}\right)=\left(\frac{2}{p}\right)=-1,$$

which contradicts (3). Thus (2) has no solution (X, Y). □

Lemma 6 [1]. *If* $p\notin\{1093, 3511\}$ *and* $2^{p-1}\equiv 1 \pmod{p^2}$, *then* $p>3\cdot 10^9$. □

Let α be an algebraic number with the minimal polynomial

$$a_0z^d+\cdots+a_d=a_0\prod_{i=1}^{d}(z-\sigma_i\alpha), \qquad a_0>0,$$

where $\sigma_1\alpha, \dots, \sigma_d\alpha$ are conjugates of α. Then

$$H(\alpha)=\frac{1}{d}\left(\operatorname{Log} a_0+\sum_{i=1}^{d}\operatorname{Log}\max(1, |\sigma_i\alpha|)\right)$$

is called Weil's height of α. Let α_1, α_2 be nonzero algebraic numbers which are multiplicatively dependent, and let r denote the degree of $\mathbb{Q}(\alpha_1, \alpha_2)$. For $j=1, 2$, let $\log\alpha_j$ be any nonzero determination of the logarithm of α_j, and let $A_j=\max(1, H(\alpha_j)+\operatorname{Log}2, e^2|\log\alpha_j|/r)$. Then we have:

Lemma 7. *If* $r = 2$ *and* $\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2 \neq 0$ *for some* $b_1, b_2 \in \mathbb{N}$ *with* $\max(b_1, b_2) \geq 10^6$, *then* $|\Lambda| \geq \exp(-704 A_1 A_2 (1 + \operatorname{Log} B + \operatorname{Log}\operatorname{Log} 2B)^2)$ *where* $B = \max(b_1, b_2)$.

Proof. Under the above hypotheses, by the definitions in [4], we may choose $\theta = 12$, $Z = 3$, $G = 1 + \operatorname{Log} B + \operatorname{Log}\operatorname{Log} 2B$, $c = 9.15$, $c_0 = 136.89$, $c_1 = 2.84$, and $C/Z^3 = 44$ by [4, Figure 4]. The lemma follows immediately from [4, Theorem 5.11]. □

3. Proofs

Proof of Theorem 1. Let (x, y, n) be a solution of (1) with $\gcd(x, y) = 1$. Then $2 \nmid xy$. By Lemma 4, it suffices to prove the case that $n \geq 2$.

If $2 \mid n$, then $n = 2m$, where $m \in \mathbb{N}$ with $m \geq 1$. Since the class number of $\mathbb{Q}(\sqrt{-p})$ is less than p, we get from (1) that

$$2^m + x\sqrt{-p} = (x_1 + y_1\sqrt{-p})^p, \tag{4}$$

where $x_1, y_1 \in \mathbb{Z}$ satisfying

$$x_1^2 + py_1^2 = y, \qquad \gcd(x_1, y_1) = 1. \tag{5}$$

By Lemma 1, we get from (4) that

$$\begin{aligned} 2^{m+1} &= (x_1 + y_1\sqrt{-p})^p + (x_1 - y_1\sqrt{-p})^p \\ &= 2x_1 \sum_{k=0}^{(p-1)/2} (-1)^k \begin{bmatrix} p \\ k \end{bmatrix} (2x_1)^{p-2k-1} y^k, \end{aligned}$$

whence we obtain $x_1 = \pm 2^m$ and

$$\pm 1 = \sum_{k=0}^{(p-1)/2} (-1)^k \begin{bmatrix} p \\ k \end{bmatrix} 2^{(m+1)(p-2k-1)} y^k. \tag{6}$$

Since $2^{p-1} \equiv 1 \pmod p$, we have

$$\begin{aligned} 1 &= \sum_{k=0}^{(p-1)/2} (-1)^k \begin{bmatrix} p \\ k \end{bmatrix} 2^{(m+1)(p-2k-1)} y^k \\ &= (-1)^{(p-1)/2} p y^{(p-1)/2} \\ &\quad + \sum_{k=1}^{(p-1)/2} (-1)^{(p-1)/2-k} \times \begin{bmatrix} p \\ (p-1)/2-k \end{bmatrix} 2^{(m+1)k} y^{(p-1)/2-k}, \end{aligned} \tag{7}$$

by (6). Recall that $x_1 = \pm 2^m$ and $m \geq 1$. We see from (5) that $p \equiv y \pmod 4$ and $py \equiv 1 \pmod 4$. Let $2^\alpha \| p - 1$. Then we have

$$2^\alpha \| (-1)^{(p-1)/2} p y^{(p-1)/2} - 1. \tag{8}$$

It is a well-known fact that $\operatorname{ord}_2 (2k+1)! < 2k$ for any $k \in \mathbb{N}$. By Lemma 1, we have

$$\begin{aligned} \begin{bmatrix} p \\ (p-1)/2-k \end{bmatrix} 2^{2(m+1)k} &= p \frac{2^{2(m+1)k}}{(2k+1)!} \prod_{i=1}^{2k} \left(\frac{p-1}{2} - k + i \right) \\ &\equiv 0 \pmod{2^{2mk+\alpha}}, \qquad k \geq 1. \end{aligned} \tag{9}$$

On combining (9) with (8), (7) is impossible. Thus (1) has no solution (x, y, n) with $\gcd(x, y) = 1$ and $2 \mid n$.

If $2 \nmid n$, then $n = 2m+1$, where $m \in \mathbb{N}$. Notice that the class number of $\mathbb{Q}(\sqrt{-2p})$ is less than p. We get from (1) that

$$2^m\sqrt{2} + x\sqrt{-p} = (x_1'\sqrt{2} + y_1'\sqrt{-p})^p, \tag{10}$$

where $x_1', y_1' \in \mathbb{Z}$ satisfying

$$2x_1'^2 + py_1'^2 = y, \qquad \gcd(x_1', y_1') = 1. \tag{11}$$

By Lemma 1, we obtain from (10) that

$$2^{m+1} = 2x_1' \sum_{k=0}^{(p-1)/2} (-1)^k \begin{bmatrix} p \\ k \end{bmatrix} (2x_1'^2)^{(p-1)/2-k} y^k,$$

whence we get $x_1' = \pm 2^m$ and

$$\pm 1 = \sum_{k=0}^{(p-1)/2} (-1)^k \begin{bmatrix} p \\ k \end{bmatrix} 2^{(2m+1)((p-1)/2-k)} y^k. \tag{12}$$

Since $2^{(p-1)/2} \equiv \delta \pmod{p}$ with $\delta \in \{-1, 1\}$, we have

$$\delta = (-1)^{(p-1)/2} p y^{(p-1)/2} + \sum_{k=1}^{(p-1)/2} (-1)^{(p-1)/2-k} \begin{bmatrix} p \\ (p-1)/2-k \end{bmatrix} 2^{(2m+1)k} y^{(p-1)/2-k} \tag{13}$$

by (12). Recall that $x_1' = \pm 2^m$ and $m \geq 1$. We see from (11) that $p \equiv y \pmod 8$ and $py \equiv 1 \pmod 8$. By much the same argument as in the proof for the case that $2 \mid n$, (13) is impossible for $\delta = 1$ and for $\delta = -1$, $p \equiv 1 \pmod 4$. Further, if $\delta = -1$ and $p \equiv 3 \pmod 4$, then $p \equiv 3 \pmod 8$, since $2^{(p-1)/2} + 1 \equiv 0 \pmod{p}$ and -2 is a quadratic residue modulo p.

On the other hand, we find from (10) and (13) that

$$-1 = 2^{(2m+1)((p-1)/2)} + \sum_{k=1}^{(p-1)/2} (-1)^k \binom{p}{2k} 2^{(2m+1)((p-1)/2-k)} (py_1'^2)^k \tag{14}$$

for $\delta = -1$, whence we get

$$2^{(2m+1)(p-1)/2} \equiv -1 \pmod{p^2}.$$

This implies that either

$$2m+1 \equiv 0 \pmod{p} \tag{15}$$

or

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{16}$$

If (15) holds, then $2m+1 = lp$ and

$$y^p - 2^{lp} = px^2 \tag{17}$$

by (1), where $l \in \mathbb{N}$. We see from equality (17) that $y \equiv 2^l \pmod{p}$,

$\gcd(y - 2^l, (y^p - 2^{lp})/(y - 2^l)) = p$, and $p^2 \nmid (y^p - 2^{lp})/(y - 2^l)$. Therefore,

$$y - 2^l = x'^2, \tag{18}$$

$$\frac{y^p - 2^{lp}}{y - 2^l} = px''^2, \tag{19}$$

where $x', x'' \in \mathbb{N}$ with $x'x'' = x$. Recall that $p \equiv y \pmod 8$ and $p \equiv 3 \pmod 8$. We have $y \equiv 3 \pmod 8$ and $l = 1$ by (18) and, hence,

$$\frac{y^p - 2^p}{y - 2} = px''^2$$

by (19). Since $p > 3$ and $p \equiv y \equiv 3 \pmod 8$, it is impossible by Lemma 5. Therefore, by Lemma 6, we get from (16) that

$$p > 3 \cdot 10^9. \tag{20}$$

Let $\varepsilon = 2^m\sqrt{2} + y_1'\sqrt{-p}$, $\bar{\varepsilon} = 2^m\sqrt{2} - y_1'\sqrt{-p}$. Then $\varepsilon + \bar{\varepsilon} = 2^{m+1}\sqrt{2}$, $\varepsilon\bar{\varepsilon} = y$, $|\varepsilon| = |\bar{\varepsilon}| = \sqrt{y}$, and

$$|\varepsilon + \bar{\varepsilon}| = |\varepsilon^p + \bar{\varepsilon}^p|$$

by (13). This implies that

$$\operatorname{Log}|\varepsilon + \bar{\varepsilon}| = p\operatorname{Log}|\varepsilon| + \operatorname{Log}|(-\bar{\varepsilon}/\varepsilon)^p - 1|. \tag{21}$$

For any complex number z, we have either $|e^z - 1| > 1/2$ or $|e^z - 1| \geq |z - k\pi\sqrt{-1}|/2$ for some $k \in \mathbb{Z}$. Put $e^z = (-\bar{\varepsilon}/\varepsilon)^p$. If $|e^z - 1| > 1/2$, then from (1), (11), and (21) we get

$$8y > 8(y - py_1'^2) = 2^{n+3} = 2^{2m+4} > y^p,$$

a contradiction. If $|e^z - 1| \geq |z - k\pi\sqrt{-1}|/2$ for some $k \in \mathbb{Z}$, then from (21) we get

$$\operatorname{Log}|\varepsilon + \bar{\varepsilon}| = p\operatorname{Log}|\varepsilon| + \operatorname{Log}|p\log(-\bar{\varepsilon}/\varepsilon) - k\log(-1)| - \operatorname{Log} 2, \tag{22}$$

where $k \in \mathbb{Z}$ with $|k| \leq p$. By (11), $-\bar{\varepsilon}/\varepsilon$ satisfies

$$y(-\bar{\varepsilon}/\varepsilon)^2 + 2(2^{2m+1} - py_1'^2)(-\bar{\varepsilon}/\varepsilon) + y = 0.$$

It implies that $-\bar{\varepsilon}/\varepsilon$ is not a root of unity, its degree is 2, and its Weil's height $H(-\bar{\varepsilon}/\varepsilon) = \operatorname{Log}\sqrt{y}$. Therefore, we have $|p\log(-\bar{\varepsilon}/\varepsilon) - k\log(-1)| \neq 0$, and by Lemma 7,

$$\begin{aligned} &\left|p\log\left(-\frac{\bar{\varepsilon}}{\varepsilon}\right) - k\log(-1)\right| \\ &\geq \exp\left(-704\left(\frac{e^2\pi}{2}\right)(\operatorname{Log} 2\sqrt{y})(1 + \operatorname{Log} p + \operatorname{Log}\operatorname{Log} 2p)^2\right) \\ &> \exp(-8200(\operatorname{Log} 2\sqrt{y})(1 + \operatorname{Log} p + \operatorname{Log}\operatorname{Log} 2p)^2) \end{aligned} \tag{23}$$

with (20). Substituting (23) into (22),

$$\operatorname{Log} 2 + \operatorname{Log} 2\sqrt{y} + 8200(\operatorname{Log} 2\sqrt{y})(1 + \operatorname{Log} p + \operatorname{Log}\operatorname{Log} 2p)^2 > p\operatorname{Log}\sqrt{y}. \tag{24}$$

Since $y \geq 8 + p$, if (20) holds, then (24) is impossible. The theorem is proved. □

Proof of Theorem 2. By Theorem 1, it suffices to prove the case that $\gcd(x, y) > 1$. Then we have one of the following three cases:

$$2^{n'} + pX_1^2 = Y_1^p, \qquad X_1, Y_1, n' \in \mathbb{N}, \gcd(X_1, Y_1) = 1; \tag{25}$$

$$1 + 2^r pX_2^2 = Y_2^p, \qquad X_2, Y_2 \in \mathbb{N}, 2 \nmid Y_2, r \in \{1, 2\}; \tag{26}$$

$$1 + pX_3^2 = 2^r Y_3^p, \qquad X_3, Y_3, r \in \mathbb{N}, 2 \nmid X_3Y_3. \tag{27}$$

The case (25) is trivial. By Lemma 2, (26) is impossible, since $p > \max(h(-p), h(-2p))$. Finally, if $p \not\equiv 7 \pmod 8$, then $r \in \{1, 2\}$ in (27). It follows that $p \equiv 1 \pmod 4$, y odd if $r = 1$, and that $p \equiv 3 \pmod 8$, y odd if $r = 2$. This is impossible by Lemma 3. The theorem is proved. □

Acknowledgment

The author thanks the referee for his valuable suggestions.

References

1. J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory, Academic Press, New York, 1971, pp. 213–222.
2. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
3. W. Ljunggren, *Über die Gleichungen* $1 + Dx^2 = 2y^n$ *und* $1 + Dx^2 = 4y^n$, Norske Vid. Selsk. Forh., Trondhjem **15** (1942), 115–118.
4. M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method.* III, Ann. Fac. Sci. Toulouse Math. (5) Special Issue **97** (1989), 43–75.
5. T. Nagell, *Sur l'impossibilité de quelques équations a deux indéterminées*, Norsk Mat. Forenings Skrifter (1) **13** (1921), 65–82.
6. ——, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Nova Acta Soc. Sci. Upsal. **16** (1955).
7. S. Rabinowitz, *The solutions of* $3y^2 \pm 2^n = x^3$, Proc. Amer. Math. Soc. **69** (1978), 213–218.

Research Department, Changsha Railway Institute, Changsha, Hunan, People's Republic of China

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