A new conjecture concerning the Diophantine equation $x^2 + b^y = c^z$

By Zhenfu CAO,*) Xiaolei DONG,**) and Zhong LI***)

(Communicated by Shigefumi MORI, M. J. A., Dec. 12, 2002)

Abstract: In this paper, using a recent result of Bilu, Hanrot and Voutier on primitive divisors, we prove that if $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$, and $b \equiv 3 \pmod 4$ is a prime power, then the Diophantine equation $x^2 + b^y = c^z$ has only the positive integer solution $(x, y, z) = (a, 2, r)$, where $r > 1$ is an odd integer, $m \in \mathbf{N}$ with $2 \mid m$ and the integers U_r, V_r satisfy $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$.

Key words: Exponential Diophantine equation; Lucas sequence; primitive divisor; Gauss integer.

1. Introduction. Let $\mathbf{Z}$, $\mathbf{N}$, $\mathbf{P}$ and $\mathbf{Q}$ be the sets of integers, positive integers, odd primes and rational numbers respectively, and $\mathbf{P}^{\mathbf{N}} = \{p^n \mid p \in \mathbf{P}$ and $n \in \mathbf{N}\}$. In 1993, N. Terai [13] conjectured that if (a, b, c) be a primitive Pythagorean triple such that

$$a^2 + b^2 = c^2, \quad a, b, c \in \mathbf{N}, \quad \gcd(a, b, c) = 1, \ 2 \mid a,$$

then the Diophantine equation

$$x^2 + b^y = c^z, \quad x, y, z \in \mathbf{N}$$

has the only solution $(x, y, z) = (a, 2, 2)$. He proved that if $b, c \in \mathbf{P}$ such that (i) $b^2+1 = 2c$, (ii) $d = 1$ or even if $b \equiv 1 \pmod 4$, where d is the order of a prime divisor of $[c]$ in the ideal class group of $\mathbf{Q}(\sqrt{-b})$, then his conjecture holds. Later, some further results on Terai's conjecture were published in [8], [2, 3], [15], [5] and [6].

As an analogue of Terai's conjecture, the following new conjecture is considered in [4]:

Conjecture. *If $a, b, c, p, q, r \in \mathbf{N}$ are fixed, and*

$$(1) \qquad a^p + b^q = c^r, \quad \min(a, b, c, p, q, r) \geq 2, \quad \gcd(a, b) = 1, \ 2 \mid a,$$

then the Diophantine equation

$$(2) \qquad x^p + b^y = c^z, \quad x, y, z \in \mathbf{N}$$

has only the solution $(x, y, z) = (a, q, r)$ with $y, z > 1$.

However, the condition $y, z > 1$ of the conjecture is neglected in [4]. We point out that there are some counterexamples if no condition $y, z > 1$ in the conjecture. For example, let $\varepsilon = 7 + 4\sqrt{3}$ and $\overline{\varepsilon} = 7 - 4\sqrt{3}$. For any positive integer n, let $u_n = (\varepsilon^n + \overline{\varepsilon}^n)/2$, $v_n = (\varepsilon^n - \overline{\varepsilon}^n)/(2\sqrt{3})$. Clearly, u_n and v_n are positive integers satisfying

$$(3) \qquad u_n^2 - 3v_n^2 = 1, \quad 2 \mid v_n.$$

Let

$$(4) \qquad a = 8u_n^3 + 3v_n, \quad b = u_n, \quad c = u_n^2 + v_n^2, \quad p = 2, \quad q = 2, \quad r = 3.$$

By (3) and (4), we get

$$\begin{aligned} c^3 &= (u_n^2 + v_n^2)^3 = (4v_n^2 + 1)^3 \\ &= 64v_n^6 + 48v_n^4 + 12v_n^2 + 1 \\ &= (8v_n^3 + 3v_n)^2 + 3v_n^2 + 1 \\ &= (8v_n^3 + 3v_n)^2 + u_n^2 = a^2 + b^2. \end{aligned}$$

Therefore, the positive integers a, b, c, p, q, r in (4) satisfy (1), but equation (2) has two solutions $(x, y, z) = (v_n, 2, 1)$ and $(a, 2, 3)$.

It seems that the proof of this conjecture is very difficult. For the case $p = q = 2$, $2 \nmid r > 1$, it is proved [4] that if $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$, $b \in \mathbf{P}$ and $b > 8 \cdot 10^6$, $b \equiv 3 \pmod 4$, then the Diophantine equation

$$(5) \qquad x^2 + b^y = c^z, \quad x, y, z \in \mathbf{N}$$

has only the solution $(x, y, z) = (a, 2, r)$, where $m \in \mathbf{N}$ with $2 \mid m$ and the integers U_r, V_r satisfy $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$.

1991 Mathematics Subject Classification. 11D61.

*) Department of Computer Science, Shanghai Jiao Tong University, Shanghai 200030, P. R. China.
**) Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200030, P. R. China.
***) Department of Mathematics, Maoming College, Maoming, Guangdong, P. R. China.

In this paper, using a recent result of Bilu, Hanrot and Voutier [1] on primitive divisors, we prove the following result.

Theorem. *Let $r, m \in \mathbf{N}$ with $2 \nmid r > 1$, $2 \mid m$. Define the integers U_r, V_r by $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$. If $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$, $b \equiv 3 \pmod 4$, and $b \in \mathbf{P}^{\mathbf{N}}$, then equation* (5) *has only the solution $(x, y, z) = (a, 2, r)$.*

From the theorem, we have

Corollary. *If $m \in \mathbf{N}$ such that $m > 1$ and $3m^2 - 1 \in \mathbf{P}^{\mathbf{N}}$, then the Diophantine equation*

$$x^2 + (3m^2 - 1)^y = (m^2 + 1)^z, \quad x, y, z \in \mathbf{N}$$

has only the solution $(x, y, z) = (m^3 - 3m, 2, 3)$.

2. Preliminaries. A Lucas pair (resp. a Lehmer pair) is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ (resp. $(\alpha + \beta)^2$ and $\alpha\beta$) are non-zero coprime rational integers and α/β is not a root of unity. For a given Lucas pair (α, β), one defines the corresponding sequence of Lucas numbers by

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (n = 0, 1, 2, \ldots).$$

For a given Lehmer pair (α, β), one defines the corresponding sequence of Lehmer numbers by

$$\widetilde{u}_n = \widetilde{u}_n(\alpha, \beta) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd}, \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even}. \end{cases}$$

It is clear that every Lucas pair (α, β) is also a Lehmer pair, and

$$u_n = \begin{cases} \widetilde{u}_n & \text{if } n \text{ is odd}, \\ (\alpha + \beta)\widetilde{u}_n & \text{if } n \text{ is even}. \end{cases}$$

Let (α, β) be a Lucas (resp. Lehmer) pair. The prime number p is a primitive divisor of the Lucas (resp. Lehmer) number $u_n(\alpha, \beta)$ (resp. $\widetilde{u}_n(\alpha, \beta)$) if p divides u_n but does not divide $(\alpha - \beta)^2 u_1 \cdots u_{n-1}$ (resp. if p divides $\widetilde{u}_n$ but does not divide $(\alpha^2 - \beta^2)^2 \widetilde{u}_1 \cdots \widetilde{u}_{n-1}$). The following lemmas are classical.

Lemma 1. *Let (α, β) be a Lucas (resp. Lehmer) pair. If the prime number p is a primitive divisor of the Lucas (resp. Lehmer) number $u_n(\alpha, \beta)$ (resp. $\widetilde{u}_n(\alpha, \beta)$), then $n \equiv \pm 1 \pmod p$.*

Lemma 2. *If $u_m \neq 1$, then $u_m \mid u_n$ iff $m \mid n$.*

Proof. For example, see W. L. McDaniel [11]. □

Recently, Y. Bilu, G. Hanrot and P. Voutier [1] proved the following

Lemma 3. *For any integer $n > 30$, every n-th term of any Lucas or Lehmer sequence has a primitive divisor.*

A Lucas (resp. Lehmer) pair (α, β) such that $u_n(\alpha, \beta)$ (resp. $\widetilde{u}_n(\alpha, \beta)$) has no primitive divisors will be called n-defective Lucas (resp. Lehmer) pair. Two Lucas pairs (α_1, β_1) and (α_2, β_2) are equivalent if $(\alpha_1/\alpha_2) = (\beta_1/\beta_2) = \pm 1$. Two Lehmer pairs (α_1, β_1) and (α_2, β_2) are equivalent if

$$\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2} \in \{\pm 1, \pm\sqrt{-1}\}.$$

In 1995, P. Voutier [14] proved the following

Lemma 4. *Let n satisfy $4 < n \leq 30$ and $n \neq 6$. Then, up to equivalence, all n-defective Lucas pairs are of form $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$, where (a, b) are given in Table* 1 *of* [1].

Let n satisfy $6 < n \leq 30$ and $n \notin \{8, 10, 12\}$. Then, up to equivalence, all n-defective Lehmer pairs are of form $((\sqrt{a} - \sqrt{b})/2, (\sqrt{a} + \sqrt{b})/2)$, where (a, b) are given in Table 2 *of* [1].

In [1], for any positive integer $n \leq 30$, all Lucas sequences and all Lehmer sequences whose n-th term has no primitive divisor are explicitely determined. i.e., Y. Bilu, G. Hanrot and P. Voutier [1] proved also the following

Lemma 5. *Any Lucas pair is* 1*-defective, and any Lehmer pair is* 1*-and* 2*-defective.*

For $n \in \{2, 3, 4, 6\}$, all (up to equivalence) n-defective Lucas pairs are of form $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$, where (a, b) are given in Table 3 *of* [1].

For $n \in \{3, 4, 5, 6, 8, 10, 12\}$, all (up to equivalence) n-defective Lehmer pairs are of form $((\sqrt{a} - \sqrt{b})/2, (\sqrt{a} + \sqrt{b})/2)$, where (a, b) are given in Table 4 *of* [1].

We will use the following Lemmas to prove the theorem.

Lemma 6. *Let $r, m \in \mathbf{N}$ with $2 \nmid r > 1$, $2 \mid m$. Define the integers U_r, V_r by $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$. If $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$, $b \equiv 3 \pmod 4$, and $b \in \mathbf{P}^{\mathbf{N}}$, then equation* (5) *has no solution (x, y, z) with $2 \mid z$.*

Proof. See the proof of Theorem in [4]. □

Lemma 7. *If $2 \nmid r$ and $r > 1$, then all solutions (X, Y, Z) of the equation*

$$X^2 + Y^2 = Z^r, \quad X, Y, Z \in \mathbf{Z}, \quad \gcd(X, Y) = 1$$

are given by

$$X+Y\sqrt{-1}=\lambda_1(X_1+\lambda_2 Y_1\sqrt{-1})^r,\quad Z=X_1^2+Y_1^2,$$

where

$$\lambda_1,\lambda_2\in\{-1,1\},\ X_1,Y_1\in\mathbf{N}\ \text{and}\ \gcd(X_1,Y_1)=1.$$

Lemma 7 follows directly from a theorem in the book of Mordell [12] pp. 122–123.

Lemma 8. *The Diophantine equation*

$$x^2-\lambda=y^n,\quad n>1,\quad \lambda=\pm1$$

has only solution in positive integers $x=3$, $y=2$, $n=3$, $\lambda=1$.

It follows from [7, 9] that the only solution of the equation $x^2-1=y^n$ $(n>1)$ in positive integers is $(x,y,n)=(3,2,3)$, the equation $x^2+1=y^n$ $(n>1)$ has no solutions in positive integers, respectively. Hence Lemma 8 holds.

3. Proof of Theorem. Since $b\equiv 3 \pmod 4$ and $c\equiv 1 \pmod 4$, we have from (5) that $2\mid x$ and so $3^y\equiv 1 \pmod 4$, that is, $2\mid y$. Hence, we can assume that $y=2y_1$, $y_1\in\mathbf{N}$ and $2\nmid z$ by Lemma 6. Furthermore, since $b\in\mathbf{P^N}$, we have

$$\binom{r}{1}m^{r-3}-\binom{r}{3}m^{r-5}+\cdots+(-1)^{(r-3/2)}\binom{r}{r-2}\neq 0$$

and so

$$\begin{aligned}b&=\left|m^2\left(\binom{r}{1}m^{r-3}-\binom{r}{3}m^{r-5}+\cdots\right.\right.\\&\qquad\left.\left.+(-1)^{(r-3/2)}\binom{r}{r-2}\right)+(-1)^{(r-1/2)}\right|\\&\geq m^2\left|\binom{r}{1}m^{r-3}-\binom{r}{3}m^{r-5}+\cdots\right.\\&\qquad\left.+(-1)^{(r-3/2)}\binom{r}{r-2}\right|-1\\&\geq m^2-1=c-2,\end{aligned}$$

that is, $b\geq c-2$. It follows that $z>1$ by equation (5). So, we also can assume that $p\mid z$, $p\in\mathbf{P}$. Hence, (5) gives that

$$x^2+b^{2y_1}=(c^{z/p})^p,\quad x,y_1\in\mathbf{N},\quad p\in\mathbf{P}. \tag{6}$$

Clearly, $\gcd(b,c)=\gcd(x,b)=1$. By Lemma 7, we have from (6) that

$$\begin{aligned}x+b^{y_1}\sqrt{-1}&=\lambda_1(X+\lambda_2Y\sqrt{-1})^p,\\ c^{z/p}&=X^2+Y^2,\end{aligned}\tag{7}$$

where $\lambda_1,\lambda_2\in\{-1,1\}$, $X,Y\in\mathbf{N}$ and $\gcd(X,Y)=1$. It follows from (7) that

$$\begin{aligned}b^{y_1}&=\lambda_1\lambda_2Y\frac{\alpha^p-\beta^p}{\alpha-\beta}\\&=\lambda_1\lambda_2Y\left(\binom{p}{1}X^{p-1}-\binom{p}{3}X^{p-3}Y^2+\cdots\right.\\&\qquad\left.+(-1)^{(p-1/2)}\binom{p}{p}Y^{p-1}\right),\end{aligned}\tag{8}$$

where $\alpha=X+\lambda_2Y\sqrt{-1}$, $\beta=X-\lambda_2Y\sqrt{-1}$. Clearly, (8) gives

$$\left(Y,\frac{\alpha^p-\beta^p}{\alpha-\beta}\right)=1\ \text{ or }\ p \tag{9}$$

since $\gcd(X,Y)=1$.

If $Y=1$, then from the last equality of (7) and Lemma 8, we obtain $z=p$, $X=m$ and so $|U_r|^{y_1}=|U_p|$ by (8). By Lemma 2, we have $r=p$ and so $y_1=1$, $z=r$, that is, the theorem holds.

If $Y>1$, since $b\in\mathbf{P^N}$ and

$$p\,\Big\|\,\frac{\alpha^p-\beta^p}{\alpha-\beta}\ \text{ if }\ p\mid\frac{\alpha^p-\beta^p}{\alpha-\beta},$$

we see from (8) and (9) that

$$\left|\frac{\alpha^p-\beta^p}{\alpha-\beta}\right|=1\ \text{ or }\ p. \tag{10}$$

Clearly, $(\alpha^p-\beta^p)/(\alpha-\beta)$ is p-th term of Lucas sequence. And from (10) and Lemma 1, we have that $(\alpha^p-\beta^p)/(\alpha-\beta)$ has no primitive divisor. Hence, using Lemmas 3–5 and Tables 1 and 3 in [1], and note that $p\in\mathbf{P}$, we get the following 4 cases:

Case I: $p=5$ and

$$\begin{aligned}(2X,-4Y^2)\in\{&(1,5),(1,-7),(2,-40),(1,-11),\\&(1,-15),(12,-76),(12,-1364)\}.\end{aligned}$$

But this is impossible since $Y\in\mathbf{N}$.

Case II: $p=7$ and

$$(2X,-4Y^2)\in\{(1,-7),(1,-19)\}.$$

Clearly, this also is impossible.

Case III: $p=13$ and $(2X,-4Y^2)=(1,-7)$ which is impossible.

Case IV: $p=3$, $(2X,-4Y^2)=(u,-3u^2+4\lambda)$, $u>1$ or $(u,-3u^2+4\lambda\cdot 3^l)$, $3\nmid u$, $(l,u)\neq(1,2)$, where $\lambda\in\{-1,1\}$, $l,u\in\mathbf{N}$.

If $(2X,-4Y^2)=(u,-3u^2+4\lambda)$, $u>1$, then $Y^2=3X^2-\lambda$ and from the last equality of (7), we obtain $4X^2-\lambda=c^{z/3}$. It follows by Lemma 8 that $z=3$. Notice that $c=m^2+1$. We have $\lambda=-1$, $m=2X$ and

$$Y^2-3X^2=1. \tag{11}$$

By $p = 3$ and (11), we obtain $(\alpha^p - \beta^p)/(\alpha - \beta) = -1$. So, we get from (8) that $Y = b^{y_1}$. However, from $b \geq c - 2$ and the last equality of (7), we can obtain $c = X^2 + Y^2 \geq 1 + b^2 \geq 1 + (c-2)^2 > c$, a contradiction.

If $(2X, -4Y^2) = (u, -3u^2 + 4\lambda \cdot 3^l)$, $3 \nmid u$, $(l, u) \neq (1, 2)$, then

$$Y^2 = 3X^2 - \lambda \cdot 3^l \tag{12}$$

and so

$$(\alpha^p - \beta^p)/(\alpha - \beta) = \lambda \cdot 3^l \text{ (note that } p = 3). \tag{13}$$

From (8) and (13), we get $Y = 3^t$, $t \in \mathbf{N}$ and $l = 1$ since $3 \| (\alpha^3 - \beta^3)/(\alpha - \beta)$. Substituting $l = 1$ and $Y = 3^t$ into (12), we have $3^{2t-1} = X^2 - \lambda$ and so $X = 2$, $Y = 3$. Substituting these into the last equality of (7), we have $13 = c^{z/3}$ which is impossible since $c = m^2 + 1$.

This proves Theorem.

Acknowledgement. This project was supported by China Postdoctoral Science Foundation and the National Natural Science Foundation of China.

References

[1] Bilu, Y., Hanrot, G., and Voutier, P. (with an appendix by Mignotte, M.): Existence of primitive divisors of Lucas and Lehmer numbers. J. Reine Angew. Math., **539**, 75–122 (2001).

[2] Cao, Z., and Dong, X.: On Terai's conjecture. Proc. Japan Acad., **74A**, 127–129 (1998).

[3] Cao, Z., and Dong, X.: Some new results on Terai's conjecture. J. Harbin Inst. Tech. New Ser., 5, pp. 1–3 (1998).

[4] Cao, Z., and Dong, X.: The Diophantine equation $x^2+b^y = c^z$. Proc. Japan Acad., **77A**, 1–4 (2001).

[5] Chen, X., and Le, M.: A note on Terai's conjecture concerning Pythagorean numbers. Proc. Japan Acad., **74A**, 80–81 (1998).

[6] Dong, X.: Diophantine equations and class numbers of quadratic fields. Ph. D. Thesis, Harbin Institute of Technology, Ch. 4 (2001).

[7] Ko, C.: On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$. Sci. Sin., **14**, 457–460 (1964).

[8] Le, M.: A note on the Diophantine equation $x^2 + b^y = c^z$. Acta Arith., **71**, 253–257 (1995).

[9] Lebesgue, V. A.: Sur l'impossibilitéon nombres entiers de l'équation $x^m = y^2 + 1$. Nouv. Ann. Math., **9** (1), 178–181 (1850).

[10] Ljunggren, W.: Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. Norske Vid. Akad. Oslo, **5**, 1–27 (1942).

[11] McDaniel, W. L.: The g.c.d. in Lucas sequences and Lehmer number sequences. Fibonacci Quart., **29**, 24–29 (1991).

[12] Mordell, L. J.: Diophantine Equations. Academic Press, New York-London (1969).

[13] Terai, N.: The Diophantine equation $x^2 + q^m = p^n$. Acta Arith., **63** (4), 351–358 (1993).

[14] Voutier, P.: Primitive divisors of Lucas and Lehmer sequences. Math. Comp., **64**, 869–888 (1995).

[15] Yuan, P., and Wang, J.: On the Diophantine equation $x^2 + b^y = c^z$. Acta Arith., **84**, 145–147 (1998).