ACTA ARITHMETICA
LXXI.3 (1995)

A note on the diophantine equation $x^2 + b^y = c^z$

by

Maohua Le (Zhanjiang)

1. Introduction. Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$ be the sets of integers, positive integers and rational numbers respectively. Let (a, b, c) be a primitive Pythagorean triple such that

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

Then we have

$$(2)\qquad a = 2st, \quad b = s^2 - t^2, \quad c = s^2 + t^2,$$

where $s, t \in \mathbb{N}$ satisfy $\gcd(s, t) = 1$, $s > t$ and $2 \mid st$. Recently, Terai [5] conjectured that the equation

$$(3)\qquad x^2 + b^y = c^z, \quad x, y, z \in \mathbb{N},$$

has only the solution $(x, y, z) = (a, 2, 2)$. Simultaneously, he proved that if $b \equiv 1 \pmod 4$, $b^2 + 1 = 2c$, b, c are odd primes, c splits in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-b})$ and the order d of a prime ideal divisor of $[c]$ in K satisfies either $d = 1$ or $2 \mid d$, then (3) has only the solution $(x, y, z) = (a, 2, 2)$. In this note we prove the following general result.

Theorem. *If* $b > 8 \cdot 10^6$, $b \equiv \pm 5 \pmod 8$ *and* c *is a prime power*, *then* (3) *has only the solution* $(x, y, z) = (a, 2, 2)$.

2. Preliminaries. For any $k \in \mathbb{N}$ with $k > 1$ and $4 \nmid k$, let

$$V(k) = \prod_{q \mid k} (1 + \chi(q)),$$

where q runs over distinct prime factor of k,

$$\chi(q) = \begin{cases} 0 & \text{if } q = 2, \\ (-1)^{(q-1)/2} & \text{if } q \neq 2. \end{cases}$$

Supported by the National Natural Science Foundation of China.

Lemma 1 ([1, Theorems 6·7·1 and 6·7·4]). *The equation*

$$X_1^2 + Y_1^2 = k, \quad X_1, Y_1 \in \mathbb{Z},\ \gcd(X_1, Y_1) = 1, \tag{4}$$

has exactly $4V(k)$ *solutions* (X_1, Y_1).

Lemma 2 ([4, Chapter 15]). *If* $2 \nmid k$, *then all solutions* (X, Y, Z) *of the equation*

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

are given by

$$Z \in \mathbb{N}, \quad X + Y\sqrt{-1} = (X_1 + Y_1\sqrt{-1})^Z \quad \text{or} \quad Y + X\sqrt{-1} = (X_1 + Y_1\sqrt{-1})^Z,$$

where (X_1, Y_1) *runs over all solutions of* (4).

Let α be a non-zero algebraic number with the defining polynomial $a_0 z^r + a_1 z^{r-1} + \ldots + a_r = a_0(z - \sigma_1\alpha)\ldots(z - \sigma_r\alpha) \in \mathbb{Z}[z]$, where $a_0 > 0$, $\sigma_1\alpha, \ldots, \sigma_r\alpha$ are all the conjugates of α. Then

$$h(\alpha) = \frac{1}{r}\Big(\operatorname{Log} a_0 + \sum_{i=1}^{r} \operatorname{Log} \max(1, |\sigma_i\alpha|)\Big)$$

is called *Weil's height* of α.

Lemma 3 ([3, Section 10]). *Let* $\log\alpha$ *be any non-zero determination of the logarithm of* α. *If* $r = 2$ *and* $\Lambda = b_1\pi\sqrt{-1}/b_2 - \log\alpha \neq 0$ *for some* $b_1, b_2 \in \mathbb{Z}$ *with* $b_1 b_2 \neq 0$, *then*

$$|\Lambda| > \exp(-20600A(1.35 + \operatorname{Log} B + \operatorname{Log}\operatorname{Log} 2B)^2),$$

where $A = \max(1/2, h(\alpha))$, $B = \max(4, |b_1|, |b_2|)$.

Lemma 4. *Let* $X, Y \in \mathbb{Z}$ *be such that* $XY \neq 0$, $\gcd(X, Y) = 1$ *and* $2 \mid XY$. *Further, let* $\varepsilon = X + Y\sqrt{-1}$ *and* $\overline{\varepsilon} = X - Y\sqrt{-1}$. *If*

$$\left|\frac{\varepsilon^n - \overline{\varepsilon}^n}{\varepsilon - \overline{\varepsilon}}\right| \le n \tag{5}$$

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

Proof. By much the same argument as in the proof of [2, Lemma 10], if (5) holds, then we have

$$\operatorname{Log} n + \operatorname{Log}|\varepsilon - \overline{\varepsilon}| \ge \operatorname{Log}|\varepsilon^n - \overline{\varepsilon}^n| \ge n \operatorname{Log}|\varepsilon| + \operatorname{Log}\left|n \log\frac{\overline{\varepsilon}}{\varepsilon} - t\pi\sqrt{-1}\right|, \tag{6}$$

where $t \in \mathbb{Z}$ with $|t| \le n$. Let $k = X^2 + Y^2$ and $\Lambda = n\log(\overline{\varepsilon}/\varepsilon) - t\pi\sqrt{-1}$. Then $k \ge 5$ and $\overline{\varepsilon}/\varepsilon$ satisfies

$$k\left(\frac{\overline{\varepsilon}}{\varepsilon}\right)^2 - 2(X^2 - Y^2)\frac{\overline{\varepsilon}}{\varepsilon} + k = 0, \quad \gcd(k, 2(X^2 - Y^2)) = 1.$$

This implies that $\overline{\varepsilon}/\varepsilon$ is not a root of unity and $h(\overline{\varepsilon}/\varepsilon) = \operatorname{Log}\sqrt{k}$. Therefore, we have $\Lambda \neq 0$. Notice that $|\varepsilon| = \sqrt{k}$, $|\varepsilon - \overline{\varepsilon}| < 2\sqrt{k}$, and the degree of $\overline{\varepsilon}/\varepsilon$ is equal to 2. On applying Lemma 3 to (6), we get

$$\operatorname{Log} 2\sqrt{k} + 20600(\operatorname{Log}\sqrt{k})(1.35 + \operatorname{Log} n + \operatorname{Log}\operatorname{Log} 2n)^2 > n \operatorname{Log}\sqrt{k},$$

whence we deduce that $n < 8 \cdot 10^6$. The lemma is proved.

3. Proof of Theorem. Let (x, y, z) be a solution of (3). If $2 \nmid y$, then from (3) we get $(-b/c) = 1$, where $(\cdot/\cdot)$ is Jacobi's symbol. Since $c \equiv 1 \pmod 4$ and $c \equiv 2s^2 \pmod b$ by (2), if $b \equiv \pm 5 \pmod 8$, then

$$1 = \left(\frac{-b}{c}\right) = \left(\frac{b}{c}\right) = \left(\frac{c}{b}\right) = \left(\frac{2s^2}{b}\right) = \left(\frac{2}{b}\right) = -1,$$

a contradiction. Similarly, we see from $(c/b) = -1$ that (3) has no solution (x, y, z) with $2 \mid y$ and $2 \nmid z$.

If $2 \mid y$ and $2 \mid z$, then $(X, Y, Z) = (x, b^{y/2}, z/2)$ is a solution of the equation

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

Since c is a prime power and $c^2 = a^2 + b^2$, by Lemmas 1 and 2, we obtain the following four cases:

$$\begin{aligned} &x + b^{y/2}\sqrt{-1} = \lambda_1(a + \lambda_2 b\sqrt{-1})^{z/2} \quad \text{or} \quad \lambda_1(b + \lambda_2 a\sqrt{-1})^{z/2},\\ &b^{y/2} + x\sqrt{-1} = \lambda_1(a + \lambda_2 b\sqrt{-1})^{z/2} \quad \text{or} \quad \lambda_1(b + \lambda_2 a\sqrt{-1})^{z/2}, \end{aligned} \tag{7}$$

where $\lambda_1, \lambda_2 \in \{-1, 1\}$.

When $z = 2$, we see from (7) that $x = a$ and $y = 2$.

When $z > 2$ and $2 \mid z/2$, (7) is impossible, since $a > 1$, $b > 1$ and $\gcd(a, b) = 1$.

When $z > 2$ and $2 \nmid z/2$, we see from (7) that

$$x + b^{y/2}\sqrt{-1} = \lambda_1(a + \lambda_2 b\sqrt{-1})^{z/2}. \tag{8}$$

So we have

$$\begin{aligned} b^{y/2-1} &= \lambda_1\lambda_2\left(\binom{z/2}{1}a^{z/2-1} - \binom{z/2}{3}a^{z/2-3}(-b^2)\right.\\ &\qquad \left. + \ldots + (-1)^{(z-2)/4}\binom{z/2}{z/2}(-b^2)^{(z-2)/4}\right)\\ &= (-1)^{(z-2)/4}\lambda_1\lambda_2 \sum_{i=0}^{(z-2)/4} (-1)^i \binom{z/2}{2i} a^{2i} b^{z/2-2i-1}. \end{aligned} \tag{9}$$

If $y=2$, then from (9) we get

$$1=\sum_{i=0}^{(z-2)/4}(-1)^i\binom{z/2}{2i}a^{2i}b^{z/2-2i-1}, \tag{10}$$

since $a^2\equiv 0 \pmod 4$ and $b^2\equiv 1 \pmod 4$. Let $2^\alpha \parallel a$, $2^\beta \parallel b^2-1$, $2^\gamma \parallel (z-2)/4$ and $2^{\delta_i}\parallel 2i$ for any $i\in\mathbb{N}$. Notice that $2\parallel st$ if $b\equiv \pm 5 \pmod 8$ by (2). We have $\alpha=2$ and $\beta=3$. Hence,

$$2^{3+\gamma}\parallel b^{z/2-1}-1. \tag{11}$$

On the other hand, since

$$\delta_i\le \frac{\log 2i}{\log 2}\le 2i-1<2(2i-1),\qquad i\in\mathbb{N},$$

we have

$$\binom{z/2}{2i}a^{2i}=\frac{az}{2}\left(\frac{z-2}{2}\right)\binom{z/2-2}{2i-2}\frac{a^{2i-1}}{2i(2i-1)}\equiv 0 \pmod{2^{4+\gamma}}, \tag{12}$$
$$i=1,\ldots,(z-2)/4.$$

Therefore, we see from (11) and (12) that (10) is impossible.

If $y>2$, then $z/2\equiv 0 \pmod b$ by (9). Let p be a prime factor of b. Further, let $p^\alpha\parallel b$, $p^\beta\parallel z/2$ and $p^{\gamma_i}\parallel 2i+1$ for any $i\in\mathbb{N}$. Notice that $2\nmid b$, $p\ge 3$ and

$$\gamma_i\le\frac{\log(2i+1)}{\log p}<2i,\qquad i\in\mathbb{N}.$$

We have

$$\binom{z/2}{2i+1}b^{2i}=\frac{z}{2}\binom{z/2-1}{2i}\frac{b^{2i}}{2i+1}\equiv 0 \pmod{p^{\beta+1}}, \tag{13}$$
$$i=1,\ldots,(z-2)/4.$$

On applying (13) together with (9), we get

$$\beta=\alpha\left(\frac{y}{2}-1\right). \tag{14}$$

Let p run over distinct prime factors of b. We see from (14) that

$$z/2\equiv 0 \pmod{b^{y/2-1}}. \tag{15}$$

Recalling that $y>2$, we deduce from (15) that

$$z/2\ge b^{y/2-1}\ge b. \tag{16}$$

Let $\varepsilon=a+b\sqrt{-1}$ and $\overline{\varepsilon}=a-b\sqrt{-1}$. From (8) and (9), we get

$$\left|\frac{\varepsilon^{z/2}-\overline{\varepsilon}^{z/2}}{\varepsilon-\overline{\varepsilon}}\right|=b^{y/2-1}. \tag{17}$$

By (16), on applying Lemma 4 to (17), we obtain $z/2 < 8 \cdot 10^6$. Thus, by (16), we deduce $b < 8 \cdot 10^6$. The Theorem is proved.

References

[1] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.
[2] M.-H. Le, *The diophantine equation* $x^2 + D^m = p^n$, Acta Arith. 52 (1989), 255–265.
[3] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method, III*, Ann. Fac. Sci. Toulouse Math. 97 (1989), 43–75.
[4] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.
[5] N. Terai, *The Diophantine equation* $x^2 + q^m = p^n$, Acta Arith. 63 (1993), 351–358.

DEPARTMENT OF MATHEMATICS
ZHANJIANG TEACHER'S COLLEGE
P.O. BOX 524048
ZHANJIANG, GUANDONG
P.R. CHINA

Received on 21.6.1994 (2632)