ACTA ARITHMETICA
LXXXIV.2 (1998)

On the diophantine equation $x^2 + b^y = c^z$

by

Pingzhi Yuan and Jiabao Wang (Hunan)

In 1993, Terai [3] conjectured that if $a^2 + b^2 = c^2$ with $(a, b, c) = 1$ and a even, then the equation

$$x^2 + b^y = c^z \tag{1}$$

has the only positive integral solution $(x, y, z) = (a, 2, 2)$. In 1995, using Baker's efficient method, Maohua Le proved that Terai's conjecture holds if $b > 8 \cdot 10^6$, $b \equiv \pm 5 \pmod 8$ and c is a prime power.

In this paper, by a completely different method, we prove the following

Theorem. *If $a^2 + b^2 = c^2$, $(a, b, c) = 1$, $b \equiv \pm 5 \pmod 8$ and c a prime, then Terai's Conjecture holds.*

It is clear that the results in this paper cover that in [2].

Lemma. *If $2 \nmid k$, then all integral solutions (X, Y, Z) of the equation*

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

can be given as follows:

(a) *when Z is odd*,

$$X + Y\sqrt{-1} = 2^{(1-Z)/2}(X_1 + Y_1\sqrt{-1})^Z$$

or

$$Y + X\sqrt{-1} = 2^{(1-Z)/2}(X_1 + Y_1\sqrt{-1})^Z;$$

(b) *when Z is even*,

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

or

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

where $\lambda_1, \lambda_2 \in \{1, -1\}$, and (X_1, Y_1) runs over all integral solutions of the equation $X_1^2 + Y_1^2 = 2k$, $(X_1, Y_1) = 1$.

1991 *Mathematics Subject Classification*: Primary 11D61.

Proof. From Theorems 6.7.1 and 6.7.4 of [1], we need only prove that X, Y in (a) and (b) are integers, and $(X,Y)=1$, and also that the solutions $X+Y\sqrt{-1}$ are all different for the different $X_1+Y_1\sqrt{-1}$. This is clear.

Proof of Theorem. Suppose that (x,y,z) is a solution of (1). Since $a^2+b^2=c^2$, $(a,b,c)=1$, $2\,|\,a$, we may assume that

$$a=2st,\qquad b=s^2-t^2,\qquad c=s^2+t^2,\qquad s>t>0,\qquad (s,t)=1.$$

From the proof of the Theorem of [2] we have $2\,|\,y$ and $2\,|\,z$, so $(x,m,n)=(x,y/2,z/2)$ is a positive integral solution of the equation

$$x^2+b^{2m}=c^{2n}. \tag{3}$$

By (3) and since b is odd, there exist integers b_1, b_2 satisfying

$$b_1^{2m}+b_2^{2m}=2c^n,\qquad b_1b_2=b,\qquad (b_1,b_2)=1; \tag{4}$$

here we may assume, without loss of generality, that $b_1>0$, $b_2>0$. Since c is a prime power, for any given positive integer n, the equation

$$X^2+Y^2=2c^n,\qquad (X,Y)=1, \tag{5}$$

has exactly eight integral solutions (X,Y). Note that the equation $X_1^2+Y_1^2=2c$, $(X_1,Y_1)=1$, has exactly eight integral solutions

$$(X_1,Y_1)=(\lambda_1(s+t),\lambda_2(s-t)),\ (\lambda_1(s-t),\lambda_2(s+t)),$$

where $\lambda_1,\lambda_2\in\{1,-1\}$; then, by (4), $(X,Y)=(b_1^m,b_2^m)$ is a solution of (5).

It follows from the Lemma that if n is odd, then

$$\lambda_1b_1^m+\lambda_2b_2^m\sqrt{-1}=2^{(1-n)/2}(X_1+Y_1\sqrt{-1})^n \tag{6}$$

or

$$\lambda_1b_2^m+\lambda_2b_1^m\sqrt{-1}=2^{(1-n)/2}(X_1+Y_1\sqrt{-1})^n,\qquad \lambda_1,\lambda_2\in\{1,-1\}. \tag{7}$$

Owing to the symmetry of (6) and (7), it is sufficient for the proof only to consider the case of (6) with $X_1=s+t$, $Y_1=s-t$. By (6),

$$\lambda_1b_1^m2^{(n-1)/2}=(s+t)\sum_{i=0}^{(n-1)/2}\binom{n}{2i+1}(s+t)^{2i}(-(s-t)^2)^{(n-1-2i)/2}, \tag{8}$$

$$\lambda_2b_2^m2^{(n-1)/2}=(s-t)\sum_{i=0}^{(n-1)/2}\binom{n}{2i+1}(s-t)^{2i}(-1)^i(s+t)^{n-1-2i}. \tag{9}$$

From (8), (9) and $b_1b_2=b=s^2-t^2$, $b_1>0$, $b_2>0$, we have

$$b_1=s+t,\qquad b_2=s-t. \tag{10}$$

Let p be a prime factor of $s+t$, $p^\alpha\,\|\,s+t$, $p^\beta\,\|\,n$, $\alpha\ge1$, $\beta\ge0$. Since $p\ge3$, we have

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

Hence,

$$(11)\qquad \binom{n}{2i+1}(s+t)^{2i} = n\binom{n-1}{2i}\frac{(s+t)^{2i}}{2i+1} \equiv 0 \pmod{p^{\beta+1}}, \quad i = 1, 2, \ldots, (n-1)/2.$$

From (8), (10), (11), we get

$$(12)\qquad n \equiv 0 \pmod{b_1^{m-1}}.$$

Therefore, if $b_1 = s + t > 3$, then $n \geq 5^{m-1} \geq 2m + 1$ when $m > 1$, and hence

$$2c^n > 2c^{2m+1} > 2((s+t)^2/2)^{2m} > (s+t)^{2m} + (s-t)^{2m},$$

contradicting (10) and (4). If $b_1 = s+t = 3$, then $s = 2,\ t = 1,\ b = 3,\ c = 5$, and it is easy to prove that $3^{2m} + 1 = 2 \cdot 5^n,\ 2 \nmid n$, has only the solution $(m, n) = (1, 1)$.

If n is even, then

$$(13)\qquad b_1^m + b_2^m\sqrt{-1} = (A + B(s^2 - t^2)\sqrt{-1})(1 + \lambda\sqrt{-1}),$$

where $A,\ B$ are integers, and $(A, B(s^2 - t^2)) = 1$, $\lambda \in \{1, -1\}$, whence

$$(14)\qquad b_1^m = A - \lambda B(s^2 - t^2), \qquad b_2^m = \lambda A + B(s^2 - t^2).$$

From (5) and $(A, B(s^2 - t^2)) = 1$, we get $(b_1 b_2, s^2 - t^2) = 1$, but this is impossible. This completes the proof of the Theorem.

Acknowledgements. The authors wish to thank the Editor for his valuable suggestions.

References

[1] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.
[2] M. Le, *A note on the diophantine equation* $x^2 + b^y = c^z$, Acta Arith. 71 (1995), 253–257.
[3] N. Terai, *The Diophantine equation* $x^2 + q^m = p^n$, ibid. 63 (1993), 351–358.

Department of Mathematics and Mechanics
Changsha Railway University
Hunan 410075
P.R. China
E-mail: slx@csru.edu.cn

Received on 4.3.1997
and in revised form on 25.11.1997 (3144)