7. *The Diophantine Equation* $a^x + b^y = c^z$

By Nobuhiro TERAI

Division of General Education, Ashikaga Institute of Technology

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1994)

§1. Introduction. In 1956, Sierpiński [7] showed that the equation $3^x + 4^y = 5^z$ has the only positive integral solution $(x, y, z) = (2, 2, 2)$. And it is conjectured that if a, b, c are a Pythagorean triplet, i.e. positive integers satisfying $a^2 + b^2 = c^2$, then the Diophantine equation $a^x + b^y = c^z$ has the only positive integral solution $(x, y, z) = (2, 2, 2)$. It has been verified that this conjecture holds for many other Pythagorean triplets (cf. Sierpiński[8], Jeśmanowicz [3], Lu[4], Takakuwa and Asaeda [9], [10], Takakuwa [11]. See also Terai [12]).

As an analogy of this conjecture, we consider the following:

Conjecture. *If* a, b, c, p, q, r *are fixed positive integers satisfying* $a^p + b^q = c^r$ *with* $p, q, r \geq 2$, *then the Diophantine equation*

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

has the only positive integral solution $(x, y, z) = (p, q, r)$.

We note that Scott [6] proved that if a and b are relatively prime integers greater than one, and if c is prime, then the equation $a^x + b^y = c^z$ has at most two solutions in positive integers (x, y, z) when $c \neq 2$, and at most one solution (x, y, z) when $c = 2$, except for two cases (taking $a < b$): $(a, b, c) = (3, 5, 2)$, which has exactly three solutions $(x, y, z) = (1, 1, 3)$, $(3, 1, 5)$, $(1, 3, 7)$ and $(a, b, c) = (3, 13, 2)$, which has exactly two solutions $(x, y, z) = (1, 1, 4)$, $(5, 1, 8)$ (cf. Guy [2], section D9, p. 87).

In this paper, we consider the above Conjecture when $(p, q, r) = (2, 2, 3)$. We shall prove that the above Conjecture holds for certain a, b, c satisfying $a^2 + b^2 = c^3$ as specified in Theorem in §2. We shall also give some examples of a, b, c satisfying the conditions of Theorem.

§2. Theorem. We first prepare some lemmas.

Lemma 1. *The integral solutions of the equation* $a^2 + b^2 = c^3$ *with* $(a, b) = 1$ *are given by*

$$a = \pm u(u^2 - 3v^2),\ b = \pm v(v^2 - 3u^2),\ c = u^2 + v^2,$$

where u, v *are integers such that* $(u, v) = 1$ *and* $u \not\equiv v \pmod 2$.

Proof. If $a \equiv b \equiv 1 \pmod 2$, then $1 + 1 \equiv a^2 + b^2 = c^3 \equiv 0 \pmod 4$, which is impossible. So $a \not\equiv b \pmod 2$ since $(a, b) = 1$. It follows from $a^2 + b^2 = c^3$ that

$$a + ib = i^r(u + iv)^3$$

for some integers u, v such that $(u, v) = 1$ and $u \not\equiv v \pmod 2$. Since $i = (-i)^3$, the i^r can be absorbed in $(u + iv)^3$. Therefore we have $a = \pm u(u^2 - 3v^2)$, $b = \pm v(v^2 - 3u^2)$ and $c = u^2 + v^2$.

Conversely the above a, b, c satisfy $a^2 + b^2 = c^3$ and $(a, b) = 1$.

In the following, we consider the case $u = m$, $v = 1$; i.e.

(2) $$a = m(m^2 - 3),\ b = 3m^2 - 1,\ c = m^2 + 1,$$

and

$$m \text{ is even.}$$

Lemma 2. *Let a, b, c be positive integers satisfying* (2). *If the Diophantine equation* (1) *has positive integral solutions (x, y, z), then x and y are even.*

Proof. We first show that $\left(\frac{a}{b}\right) = -1$ and $\left(\frac{c}{b}\right) = 1$, where $\left(\frac{*}{*}\right)$ denotes the Jacobi symbol.

Using the quadratic reciprocity law, we have $\left(\frac{a}{b}\right) = \left(\frac{m(m^2-3)}{3m^2-1}\right) = \left(\frac{m}{3m^2-1}\right)\cdot\left(\frac{m^2-3}{3m^2-1}\right) = \left(\frac{m}{3m^2-1}\right)\cdot\left(\frac{2}{m^2-3}\right)$. Note that if $m \equiv 0 \pmod{t}$ and t is odd (> 1), then $\left(\frac{t}{3m^2-1}\right) = 1$. In fact, $3m^2 - 1 \equiv -1 \pmod 4$, and $\left(\frac{t}{3m^2-1}\right) = \left(\frac{3m^2-1}{t}\right) = \left(\frac{-1}{t}\right) = 1$ if $t \equiv 1 \pmod 4$, and $\left(\frac{t}{3m^2-1}\right) = -\left(\frac{3m^2-1}{t}\right) = -\left(\frac{-1}{t}\right) = 1$ if $t \equiv -1 \pmod 4$.

Put $m = 2^s t$ ($s \geq 1$ and t is odd). If $s = 1$, then $\left(\frac{a}{b}\right) = \left(\frac{2t}{3m^2-1}\right)\cdot\left(\frac{2}{m^2-3}\right) = \left(\frac{2}{3m^2-1}\right)\cdot\left(\frac{2}{m^2-3}\right) = (-1)\cdot 1 = -1$ since $m^2 \equiv 4 \pmod 8$. If $s \geq 2$, then $\left(\frac{a}{b}\right) = \left(\frac{2^s}{3m^2-1}\right)\cdot\left(\frac{2}{m^2-3}\right) = 1 \cdot (-1) = -1$ since $m^2 \equiv 0 \pmod 8$. We also have $\left(\frac{c}{b}\right) = \left(\frac{m^2+1}{3m^2-1}\right) = \left(\frac{3m^2-1}{m^2+1}\right) = \left(\frac{-4}{m^2+1}\right) = 1.$

Hence $a^x + b^y = c^z$ implies that $(-1)^x = 1$, so x is even. Then we have $(-1)^y \equiv 1 \pmod 4$ since $x \geq 2$. Thus y is even.

Lemma 3. *Let a, b, c be positive integers satisfying* (2). *Suppose that there is a prime l such that $m^2 - 3 \equiv 0 \pmod{l}$ and $e \equiv 0 \pmod 3$, where e is the order of* 2 *modulo l. If the Diophantine equation* (1) *has positive integral solutions (x, y, z), then $z \equiv 0 \pmod 3$.*

Proof. It follows from (1) and (2) that $8^y \equiv 4^z \pmod{l}$ since $m^2 \equiv 3 \pmod{l}$.

Hence we have $2^{3y-2z} \equiv 1 \pmod{l}$, so $3y - 2z \equiv 0 \pmod{e}$. Therefore $z \equiv 0 \pmod 3$.

Remark. If $m^2 - 3 \equiv 0 \pmod{l}$, then $l \equiv 1, 11 \pmod{12}$. If $e \equiv 0 \pmod 3$, then $l \equiv 1 \pmod 3$. Hence we must have $l \equiv 1 \pmod{12}$.

Lemma 4. (a) (Nagell) *Let n be an odd integer ≥ 3, and let A be a square-free integer ≥ 1. If the class number in the field $\boldsymbol{Q}(\sqrt{-A})$ is not divisi-*

ble by n, then the Diophantine equation $Ax^2 + 1 = y^n$ *has no solutions in integers* x *and* y *for* y *odd* ≥ 1, *apart from* $x = \pm 11$, $y = 3$ *for* $A = 2$ *and* $n = 5$ (cf. Nagell [5], Theorem 25).

(b) (Mahler) *Let* D *be a positive integer* > 1 *which is not a perfect square, and let* C *be a square-free divisior of* $2D$ *and* $|C| \neq 1, D$.

Let U *and* V *be positive integers satisfying the equation*

$$U^2 - DV^2 = C. \tag{3}$$

If all prime factors of V *divide* D, *then we have* (i) $U = U_1$, $V = V_1$ *or* (ii) $U = \dfrac{U_1^3 + 3U_1V_1^2D}{|C|}$, $V = \dfrac{3U_1^2V_1 + DV_1^3}{|C|}$, *where* U_1 *and* V_1 *denote the least positive integral solution of* (3). *The numbers* U *and* V *in* (ii) *are determined by the formula* $\dfrac{U + V\sqrt{D}}{|\sqrt{C}|} = \left[\dfrac{U_1 + V_1\sqrt{D}}{|\sqrt{C}|}\right]^3$ (cf. Nagell [5], Theorem 16).

We use Lemma 4 to show the following:

Lemma 5. *Let* a, b, c *be positive integers satisfying* (2) *and let* b *be prime. Then the Diophantine equation*

$$a^{2X} + b^{2Y} = c^{3Z}$$

has the only positive integral solution $(X, Y, Z) = (1, 1, 1)$.

Proof. It follows from Lemma 1 that we have

$$a^X = \pm u(u^2 - 3v^2),\ b^Y = \pm v(v^2 - 3u^2),\ c^Z = u^2 + v^2,$$

where $(u, v) = 1$, u is even and v is odd, since b is odd.

Since b is prime, we see that

$$v = \pm b^Y,\ v^2 - 3u^2 = \pm 1, \tag{4}$$

or

$$v = \pm 1,\ v^2 - 3u^2 = \pm b^Y. \tag{5}$$

We first consider (4). Then we have

$$3u^2 \pm 1 = b^{2Y}. \tag{6}$$

The $-$ sign must be rejected since $-1 \equiv (b^Y)^2 \pmod 3$ is impossible. If Y is even, then $3u^2 + 1 = B^4$ (with $B = b^{\frac{Y}{2}}$) has no solutions. In fact, $3u^2 = (B^2 + 1)(B^2 - 1)$ implies that $\dfrac{B^2 + 1}{2} = h^2$ and $\dfrac{B^2 - 1}{2} = 3k^2$, where $u = 2hk$. Hence $B^2 = h^2 + 3k^2$ and $1 = h^2 - 3k^2$, so $B^2 = h^4 - 9k^4$, which has no non-trivial solutions by the method of infinite descent (cf. Dickson [1], p. 634). Therefore Y is odd. So it follows from Lemma 4.(a) that if (6) has positive integral solutions, then $Y = 1$. If $Y = 1$, then we have $3u^2 = (b + 1)(b - 1) = 3m^2(3m^2 - 2)$, so $u^2 = 8m_1^2(6m_1^2 - 1)$ (with $m = 2m_1$), which is impossible.

We next consider (5). Then we have

$$3u^2 - 1 = b^Y. \tag{7}$$

If Y is even, then $-1 \equiv (b^{\frac{Y}{2}})^2 \pmod 3$, which is impossible. Hence Y is odd. If $Y = 1$, then we have $b = 3u^2 - 1 = 3m^2 - 1$, so $u = \pm m$, $Z = 1$ and $X = 1$. If $Y > 1$, then put $Y = 2n + 1$ $(n \geq 1)$. Then from (7) we have

$$(3u)^2 - 3b(b^n)^2 = 3.$$

Since $b = 3m^2 - 1$, the least integral solution of $U^2 - 3bV^2 = 3$ is given by $U_1 = 3m$, $V_1 = 1$. Hence it follows from Lemma 4.(b) that we have (i) $3u = 3m$, $b^n = 1$ or (ii) $b^n = 9m^2 + b = 4b + 3$, which are impossible.

Combining Lemmas 2, 3 with Lemma 5, we obtain the following theorem:

Theorem. *Let $a = m(m^2 - 3)$, $b = 3m^2 - 1$, $c = m^2 + 1$ with m even and let b be prime. Suppose that there is a prime l such that $m^2 - 3 \equiv 0 \pmod{l}$ and $e \equiv 0 \pmod{3}$, where e is the order of 2 modulo l. Then the Diophantine equation $a^x + b^y = c^z$ has the only positive integral solution $(x, y, z) = (2, 2, 3)$.*

Finally we give some examples satisfying the conditions of Theorem.

Table. $m(< 100)$, a, b, c, l, e satisfying the conditions of Theorem

m	a	b	c	l	e
4	52	47	17	13	12
8	488	191	65	61	60
14	2702	587	197	193	96
22	10582	1451	485	13	12
26	17498	2027	677	673	48
30	8970	2699	901	13	12
34	39202	3467	1157	1153	288
48	36816	6911	2305	13	12
52	140452	8111	2705	37	36
58	194938	10091	3365	3361	168
60	6540	10799	3601	109	36
74	405002	16427	5477	13	12
92	778412	25391	8465	8461	1692
96	294816	27647	9217	37	36

It seems that there are infinitely many m satisfying the conditions of Theorem. But it is difficult to show this.

Acknowledgement. The author would like to thank H. Taya for his valuable suggestions.

References

[1] L. E. Dickson: History of the Theory of Numbers. vol. II, Chelsea, New York (1971).

[2] R. Guy: Unsolved Problems in Number Theory. Springer-Verlag (1981).

[3] L. Jeśmanowicz: Kilka uwag o liczbach pitagorejskich [Some remarks on Pythagorean numbers]. Wiadom. Mat., **1**, 196–202 (1956).

[4] Lu Wen-Twan: On Pythagorean numbers $4n^2 - 1$, $4n$, $4n^2 + 1$. Acta Sc. Nat. Univ. Szechuan., pp. 39–42 (1959) (Chinese).

[5] T. Nagell: Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. Nova Acta Soc. Sci. Upsal., ser. 4 (2), **16**, 1–38 (1955).

[6] R. Scott: On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$. J. Number Theory, **44**, 153–165 (1993).

[7] W. Sierpiński: O równaniu $3^x + 4^y = 5^z$ [On the equation $3^x + 4^y = 5^z$]. Wiadom. Mat., **1**, 194–195 (1956).

[8] W. Sierpiński: Elementary Theory of Numbers. PWN-Polish Scientific Publishers, Warszawa (1988).
[9] K. Takakuwa and Y. Asaeda: On a conjecture on Pythagorean numbers. Proc. Japan Acad., **69**A, 252–255 (1993).
[10] ——: ditto. II. ibid., **69**A, 287–290 (1993).
[11] K. Takakuwa: ditto. III. ibid., **69**A, 345–349 (1993).
[12] N. Terai: The Diophantine equation $x^2 + q^m = p^n$. Acta Arith., **63.4**, 351–358 (1993).