A Note on the Diophantine Equation $a^x + b^y = c^z$

By Nobuhiro TERAI*) and Kei TAKAKUWA**)

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1997)

§ 1. Introduction. In our previous papers Terai [6], [7] and [8], we proposed the following conjecture and proved it under some conditions when $p = 2$, $q = 2$ and r is an odd prime.

Conjecture. *If a, b, c, p, q, r are fixed positive integers satisfying $a^p + b^q = c^r$ with $p, q, r \geq 2$ and $(a, b) = 1$, then the Diophantine equation*

$$(1) \qquad a^x + b^y = c^z$$

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

The positive integers a, b, c satisfying $a^2 + b^2 = c^r$ can be expressed as follows (cf. Lemma 1 in [8]):

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

$$a = \pm u \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j} u^{r-(2j+1)} v^{2j},$$

$$b = \pm v \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j+1} u^{r-(2j+1)} v^{2j},$$

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

From now on, let a, b, c be as in Lemma 1 with $u = m$, $v = 1$; i.e.

$$(2) \quad a = \pm m \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j} m^{r-(2j+1)},$$

$$b = \pm \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j+1} m^{r-(2j+1)}, \; c = m^2 + 1,$$

where m is a positive integer with $2|m$.

Then in [6], [7] and [8], we showed that if b is an odd prime and there is an odd prime l such that $ab \equiv 0$ (mod l) and $e \equiv 0$ (mod r), where e is the order of c modulo l, then equation (1) has only the positive integral solution $(x, y, z) = (2, 2, r)$ under some conditions. Recently, using the divisibility property concerning Lucas seqences, when $r = 3$, Le [3] has proved the following:

Theorem. (Le [3]). *Let a, b, c be positive integers satisfying* (2) *with $r = 3$. If $2 \| m$ and b is an odd prime, then equation (1) has only the positive integral solution $(x, y, z) = (2, 2, 3)$.*

In this paper, using a similar method as in [3], when r is an odd prime, we generalize Le's theorem as follows:

Theorem 1. *Let r be an odd prime. Let a, b, c be positive integers satisfying* (2). *Let m be a positive integer with $2 \| m$ and $m \geq 6$. Suppose that b is an odd prime and b satisfies at least one of the following three conditions:*

(i) $b \equiv -1$ (mod m), (ii) $b \equiv -1$ (mod 4),

(iii) $\left(\dfrac{b}{a'}\right) = -1$,

where $\left(\dfrac{*}{*}\right)$ denotes the Jacobi symbol and $a = ma'$.

Then equation (1) has only the positive integral solution $(x, y, z) = (2, 2, r)$.

In Theorem 1, we suppose that $2 \| m$ and $m \geq 6$. When $m = 2$, we also prove the following theorem. We note that we need not suppose b is an odd prime in Theorem 2.

Theorem 2. *Let r be an odd prime. Let a, b, c be positive integers satisfying* (2) *with $m = 2$. Suppose that b satisfies at least one of the following three conditions:*

(i) $b \equiv -1$ (mod 3), (ii) $b \equiv -1$ (mod 4),

(iii) $\left(\dfrac{b}{a'}\right) = -1$,

where $a = 2a'$.

Then equation (1) has only the positive integral solution $(x, y, z) = (2, 2, r)$.

Since $b = 3m^2 - 1 \equiv -1$ (mod 4) when $r = 3$, Theorems 1 and 2 give a generalization of Le's theorem.

§ 2. Lemmas. In this section, we prepare some lemmas used in the proof of Theorems 1 and 2.

Lemma 2. *Let r be odd ≥ 3. Let a, b, c be positive integers satisfying* (2). *Let m be a positive integer with $2 \| m$ and $m \geq 6$. Suppose that b satis-*

*) Division of General Education, Ashikaga Institute of Technology.

**) Department of Mathematics, Faculty of Science, Gakushuin University.

fies at least one of the following three conditions:
(i) $b \equiv -1 \pmod{m}$, (ii) $b \equiv -1 \pmod{4}$,
(iii) $\left(\frac{b}{a'}\right) = -1$,

where $a = ma'$.

If equation (1) *has positive integral solutions* (x, y, z), *then* x *and* y *are even.*

Proof. Let (x, y, z) be a solution of (1). We first show that y is even.

Case (i): $b \equiv -1 \pmod{m}$. From (1) and (2), we have $a^x + b^y \equiv (-1)^y \equiv 1 \equiv c^z \pmod{m}$. Since $m \geq 6$, y must be even.

Case (ii): $b \equiv -1 \pmod{4}$. If $x = 1$, then $\pm rm \pm 1 \equiv 1 \pmod{m^2}$ from (1) and (2). Thus $rm \equiv \pm 2 \pmod{m^2}$ and so $m = 2$, which is a contradiction. Hence $x \geq 2$. Then from (1) and (2), we obtain $(-1)^y \equiv 1 \pmod{4}$, which implies that y must be even.

Case (iii): $\left(\frac{b}{a'}\right) = -1$. Since $a^2 + b^2 = c^r$, we have $1 = \left(\frac{c}{a'}\right)^r = \left(\frac{c}{a'}\right)$. Thus from (1), we have $\left(\frac{b}{a'}\right)^y = \left(\frac{c}{a'}\right)^z = 1$, which implies that y must be even. Hence in all cases, it follows that y is even.

We next show that x is even (using that y is even). Note that $c \equiv 5 \pmod{8}$, since $c = m^2 + 1$ and $2 \| m$. From (2), we see that $\left(\frac{a}{c}\right) = \left(\frac{2}{c}\right) \left(\frac{m/2}{c}\right)\left(\frac{a'}{c}\right) = -\left(\frac{m^2+1}{m/2}\right)\left(\frac{c}{a'}\right) = (-1)\cdot 1 \cdot 1 = -1$. Then from (1), we have $\left(\frac{a}{c}\right)^x = \left(\frac{-b^y}{c}\right) = \left(\frac{b}{c}\right)^y = 1$, since y is even. Thus x must be even.

Lemma 3. (1) (Störmer [5], Ljunggren[4]). *The Diophantine equation*

$$x^2 + 1 = 2y^n$$

has only the positive integral solution $(x, y, n) = (239, 13, 4)$ *with* $x > 1$ *and* $n > 2$.

(2) (Ko [1]). *The Diophantine equation*

$$x^2 - 1 = y^n$$

has only the positive integral solution $(x, y, n) = (3, 2, 3)$ *with* $n > 1$.

Lemma 4. (Lehmer [2]). *Let* $\alpha = u + vi$ *and* $\beta = u - vi$, *where* u, v *are nonzero integers with* $(u, v) = 1$. *Define the sequence* $\{U_n\}$ *by*

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for } n \geq 1.$$

Let p *be a given odd prime, and let* m_0 *be the least positive integer such that* $p \mid U_{m_0}$. *If* $p^{t_0} \| U_{m_0}$ *and* $p^{t_0+t} \mid U_m$ *for some positive integers* t_0, t, m, *then we have* $m_0 p^t \mid m$.

§ 3. Proof of Theorem 1. Suppose that our assumptions are all satisfied. Let (x, y, z) be a solution of (1).

Then it follows from Lemma 2 that x and y are even.

We show that z is odd (using that b is an odd prime). Suppose, on the contrary, that z were even. Then equation (1) yields

$$c^{z/2} + a^{x/2} = b^y \text{ and } c^{z/2} - a^{x/2} = 1,$$

so

$$(b^{y/2})^2 + 1 = 2c^{z/2}.$$

Now Lemma 3, (1) implies that $z/2 \leq 2$. Thus

$$c^3 \leq c^r = a^2 + b^2 \leq a^x + b^y = c^z \leq c^4.$$

Since z is even, we have $z = 4$. Hence we obtain

$$c^2 - a^{x/2} = 1.$$

Lemma 3, (2) implies that $x = 2$. Then $c^2 = a + 1$ and so $1 \equiv \pm rm + 1 \pmod{m^2}$, which is impossible. Hence z is odd. Then since y is even and $c \equiv 5 \pmod{8}$, equation (1) implies that $a^x + 1 \equiv 5^z \equiv 5 \pmod{8}$. Since $2 \| a$, we have $x = 2$. Hence if $y = 2$, then from (1) we have $z = r$.

Suppose that $y > 2$ and so $z \geq 3$. It follows from Lemma 1 that

$$b^{y/2} = \pm v \sum_{j=0}^{(z-1)/2} (-1)^j \binom{z}{2j+1} u^{z-(2j+1)} v^{2j}, \quad c = u^2 + v^2,$$

where u, v are integers such that $(u, v) = 1$ and $u \not\equiv v \pmod{2}$. Since b is an odd prime, we see that $v = \pm b^k$, where k is an integer with $0 \leq k \leq y/2$. If $k > 0$, then we have

$$m^2 + 1 = c = u^2 + v^2 > b^2 = \left(m^2 \sum_{j=0}^{(r-3)/2} (-1)^j \binom{r}{2j+1} m^{r-(2j+3)} + (-1)^{(r-1)/2}\right)^2 > m^4,$$

which is a contradiction. Thus $k = 0$ and $v = \pm 1$. Hence by $c = m^2 + 1 = u^2 + v^2$, we have $u = \pm m$. Clearly we may suppose that $u = m$ and $v = 1$.

Now let $\alpha = m + i$ and $\beta = m - i$. Put $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ for $n \geq 1$. Then

$$U_1 = 1, \quad U_r = \frac{\alpha^r - \beta^r}{\alpha - \beta} = \pm b,$$

$$U_z = \frac{\alpha^z - \beta^z}{\alpha - \beta} = \pm b^{\frac{y}{2}}.$$

Let m_0 be the least positive integer such that

$b|U_{m_0}$. Then $m_0|r$. Since r is an odd prime and $m_0 \neq 1$, we have $m_0 = r$. Hence Lemma 4 implies that we have $rb^{\frac{y}{2}-1}|z$, since $y > 2$. Therefore we obtain

$$2b^y > a^2 + b^y = c^z \geq c^{rb^{\frac{y}{2}-1}} > e^{rb^{\frac{y}{2}-1}}$$
$$= \sum_{j=0}^{\infty} (rb^{\frac{y}{2}-1})^j / (j!) > \frac{1}{4!} (rb^{\frac{y}{2}-1})^4 > 3b^{2y-4},$$

so

$$2b^{2y} \geq 2b^{y+4} > 3b^{2y},$$

which is a contradiction. This completes the proof of Theorem 1.

Remark. We checked that at least one of the three conditions of Theorem 1 holds for a, b, c which are positive integers satisfying (2) when $r = 3, 5, 7, 11$, respectively. In the Tables I and II below, we give some examples of m, a, b, c satisfying the conditions of Theorem 1, when $r = 5, 7$. respectively. When $r = 3, 5, 7$, the positive integers a, b, c satisfying (2) can be expressed as follows:

$$r = 3: a = m(m^2 - 3),\quad b = 3m^2 - 1,\quad c = m^2 + 1.$$
$$r = 5: a = \pm m(m^4 - 10m^2 + 5),\quad b = 5m^4 - 10m^2 + 1,\quad c = m^2 + 1.$$
$$r = 7: a = \pm m(m^6 - 21m^4 + 35m^2 - 7),\quad b = \pm (7m^6 - 35m^4 + 21m^2 - 1),\quad c = m^2 + 1.$$

Table I. The case of $r = 5$ ($6 \leq m \leq 150$)

m	a	b	c
6	5646	6121	37
14	510454	190121	197
18	1831338	521641	325
22	5047262	1166441	485
26	11705746	2278121	677
46	204989846	22366121	2117
58	654405938	56548841	3365
62	913749862	73843241	3845
70	1677270350	120001001	4901
146	66307170346	2271646121	21317

§ 4. Proof of Theorem 2.

Note that when $m = 2$, we have $c = 2^2 + 1 = 5$.

We first show that x is even. Since $\sum_{j=0}^{(r-1)/2} \binom{r}{2j} = \sum_{j=0}^{(r-1)/2} \binom{r}{2j+1} = 2^{r-1}$, Lemma 1 now implies that

Table II. The case of $r = 7$ ($6 \leq m \leq 250$)

m	a	b	c
26	7782916258	2146430467	677
86	34694014809358	2830056272707	7397
102	114636746937822	7879348640771	10405
162	2925886463919882	126504326730851	26245
226	30100969389341258	932623079719267	51077
238	43239201522888518	1272100565359651	56645
242	48590549245358362	1405895873027491	58565

$$a \equiv \pm (-1)^{\frac{r-1}{2}} 2^r \pmod 5,$$
$$b \equiv \pm (-1)^{\frac{r-1}{2}} 2^{r-1} \pmod 5.$$

In fact, putting $u = 2$ and $v = 1$ in Lemma 1, we have

$$a = \pm 2 \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j} 4^{\frac{r-1}{2}-j} \equiv \pm 2$$
$$(-1)^{\frac{r-1}{2}} \sum_{j=0}^{(r-1)/2} \binom{r}{2j} = \pm (-1)^{\frac{r-1}{2}} 2^r \pmod 5.$$

Similarly, we have $b \equiv \pm (-1)^{\frac{r-1}{2}} 2^{r-1} \pmod 5$. Thus we see that

$$\left(\frac{a}{5}\right) = -1, \quad \left(\frac{b}{5}\right) = 1.$$

Therefore (1) leads to $(-1)^x = 1$ and so x is even.

We next show that y is even (using that x is even).

Case (i): $b \equiv -1 \pmod 3$. From $a^2 + b^2 = 5^r$, we see that $a \not\equiv 0 \pmod 3$. Thus since x is even, equation (1) leads to $1 + (-1)^y \equiv (-1)^z \pmod 3$ and so y is even. (Hence z is odd.)

Case (ii): $b \equiv -1 \pmod 4$. Since x is even, especially $x \geq 2$, equation (1) leads to $(-1)^y \equiv 1 \pmod 4$ and so y is even.

Case (iii): $\left(\frac{b}{a'}\right) = -1$. In the same way as in the proof of Lemma 2, Case (iii), we see that y is even. Hence in all cases, it follows that y is even.

From $a^2 + b^2 = 5^r$, we see that $ab \not\equiv 0 \pmod 3$. Thus since x and y are even, equation (1) implies that $1 + 1 \equiv (-1)^z \pmod 3$ and so z is odd. Then from (1), we have $a^x + 1 \equiv 5^z \equiv 5 \pmod 8$. Since $2 \| a$, we have $x = 2$. Hence if $y = 2$, then from (1) we have $z = r$.

Suppose that $y > 2$ and so $z \geq 3$. If follows from Lemma 1 that

$$b^{y/2} = \pm v \sum_{j=0}^{(z-1)/2} (-1)^j \binom{z}{2j+1} u^{z-(2j+1)} v^{2j},$$
$$5 = u^2 + v^2,$$

where u, v are integers such that $(u, v) = 1$ and $u \not\equiv v \pmod 2$. Since b is odd, v is odd and so u is even. Thus from $5 = u^2 + v^2$, we have $u = \pm 2$ and $v = \pm 1$. Cearly we may suppose that $u = 2$ and $v = 1$.

Now let $\alpha = 2 + i$ and $\beta = 2 - i$. Put $U_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ for $n \geq 1$. Then

$$U_1 = 1,\ U_r = \frac{\alpha^r - \beta^r}{\alpha - \beta} = \pm b,$$

$$U_z = \frac{\alpha^z - \beta^z}{\alpha - \beta} = \pm b^{\frac{y}{2}}.$$

Let $b = \Pi_{j=1}^{n} p_j^{ej}$ and $m_0(p_j)$ be the least positive integer such that $p_j \mid U_{m_0(pj)}$. Then $m_0(p_j) | r$. Since

Table III. a, b satisfying $a^2 + b^2 = 5^r$ $(3 \leq r < 30)$

r	a	b
3	2	11
5	38	41
7	278	29
11	2642	6469
13	33802	8839
17	24478	873121
19	3565918	2521451
23	35553398	103232189
29	8701963882	10513816601

r is an odd prime and $m_0(p_j) \neq 1$, we have $m_0(p_j) = r$. Hence Lemma 4 implies that since $y > 2$, we have $rp_j^{e_j(\frac{y}{2}-1)} | z$ for $1 \leq j \leq n$. By $b = \Pi_{j=1}^{n} p_j^{e_j}$, we have $rb^{\frac{y}{2}-1} | z$. Therefore as in Theorem 1, we also have a contradiction. This completes the proof of Theorem 2.

Remark. We checked that if r is an odd prime with $r < 100$, then at least one of the three conditions of Theorem 2 holds for a, b which are positive integers satisfying $a^2 + b^2 = 5^r$. In the table III above, we give some examples of a, b satisfying $a^2 + b^2 = 5^r$ with $3 \leq r < 30$.

References

[1] C. Ko: On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$. Scientia Sinica (Notes), **14**, 457–460 (1964).

[2] D. H. Lehmer: An extended theory of Lucas' functions. Ann. of Math., **31**, 419–448 (1930).

[3] M. Le: A note on the Diophantine equation $(m^3 - 3m)^x + (3m^2 - 1)^y = (m^2 + 1)^z$. Proc. Japan Acad., **73A**, 148–149 (1997).

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

[5] C. Störmer: Solution complète en nombres entiers de l'équation m arc tan $\frac{1}{x}$ + n arc tan $\frac{1}{y} = k\frac{\pi}{4}$. Bull. Soc. Math. France, **27**, 160–170 (1899).

[6] N. Terai: The Diophantine equation $a^x + b^y = c^z$. Proc. Japan Acad., **70A**, 22–26 (1994).

[7] N. Terai: The Diophantine equation $a^x + b^y = c^z$. II. Proc. Japan Acad., **71A**, 109–110 (1995).

[8] N. Terai: The Diophantine equation $a^x + b^y = c^z$. III. Proc. Japan Acad., **72A**, 20–22 (1996).